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

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувачка випускової кафедри
_____ Ніна РЖЕВСЬКА
« ____» _____ 2022 р.

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧКИ ВИЩОЇ ОСВІТИ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА
СПЕЦІАЛЬНОСТІ 291 « МІЖНАРОДНІ ВІДНОСИНИ,
СУСПІЛЬНІ КОМУНІКАЦІЇ ТА РЕГІОНАЛЬНІ СТУДІЇ»
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«МІЖНАРОДНА ІНФОРМАЦІЯ»

Тема: «КІБЕРТЕРОРИЗМ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ»

Виконавець: здобувачка вищої освіти 4 курсу, 409 Б групи, Маренич Єлизавета Олександрівна
Керівник: старший викладач кафедри міжнародних відносин, інформації та регіональних студій Ємець Валентина Олександрівна

Нормоконтролер _____ Валентина ЄМЕЦЬ
(підпис)

КИЇВ 2022

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АТО – Антитерористична операція на сході України

ДНР – Донецька народна республіка

ЕОМ – Електронна обчислювальна машина

ЄС – Європейський Союз

ЗМІ – Засоби масової інформації

ІКТ – Інформаційно-комунікаційні технології

ІТ – Інформаційні технології

ЛНР – Луганська народна республіка

МЗС – Міністерство закордонних справ

МОУ – Міністерство оборони України

МСЕ – Міжнародна спілка електрозв'язку

НАТО – Організація Північноатлантичного договору

ОБСЄ – Організація з безпеки і співробітництва в Європі

ООН – Організація Об'єднаних Націй

ОРДЛО – Окремі райони Донецької і Луганської областей

РНБО – Рада національної безпеки і оборони України

РФ – Російська Федерація

СБУ – Служба безпеки України

СНД – Співдружність Незалежних Держав

ТОВ – Товариство з обмеженою відповідальністю

CERT – Computer emergency response team

NCSC – National Cyber Security Centre

NCSI – National Cyber Security Index

ВСТУП

Актуальність. На сучасному етапі становлення міжнародних відносин та формування світового суспільства все більшого значення набуває розвиток науково-технічного прогресу, складовим елементом якого є високі комп'ютерні технології. Розвиток інформаційних технологій призвів до широкого використання мережі Інтернет у всьому світі. Мережа Інтернет є не лише важливою сполучною ланкою між різними світовими культурами, а й важливим інструментом для обміну політичною, економічною, торговельною та споживчою інформацією.

Кількість користувачів Інтернету зростає надзвичайно швидко, чим користуються різні злочинні елементи задля розширення свого впливу на суспільну свідомість, поширення насильницької інформації та різноманітних провокаційних заяв. Внаслідок зростання популярності мережі Інтернет виник один з найнебезпечніших видів кіберзлочинності – кібертероризм.

Проблема кібертероризму носить глобальний характер та є особливо актуальною в сучасному інформаційному суспільстві. За відносно короткий проміжок часу кібератаки перетворилися з окремого випадку на одну з головних загроз інформаційній безпеці держави. У глобальному контексті великі держави світу приділяють все більше уваги захисту критично важливих інформаційних ресурсів і можливості впливу на інформаційні ресурси інших держав. Більшість країн проводить активну роботу з аналізу потенційних можливостей подібних загроз та розробки засобів для боротьби з ними. Однак, незважаючи на це, все ще існує низка проблем, які країнам слід вирішити як у національних сегментах, так і в усьому кіберпросторі.

Небезпека кібертероризму полягає в тому, що він не має меж. Він існує у віртуальному світі та не має належного правового врегулювання як у вітчизняному, так і в міжнародному законодавстві. Саме тому сьогодні головним завданням є пошук шляхів та методів боротьби з кібертероризмом, щоб не допустити його поширення та захоплення інформаційного простору.

Метою роботи є визначення особливостей кібертероризму як загрози інформаційній безпеці держави та заходів протидії кібертероризму на міжнародному та національному рівні.

Для досягнення поставленої мети необхідно вирішити наступні **завдання:**

– дослідити кібертероризм як явище;

– проаналізувати міжнародно-правове регулювання кібертероризму;

– дослідити поняття інформаційної безпеки держави;

– здійснити аналіз українського та зарубіжного досвіду протидії кібертероризму;

– надати практичні рекомендації щодо попередження кібертероризму.

Об`єктом дослідження є кібертероризм як загроза інформаційній безпеці держави

Предметом дослідження є засоби та інструменти кібертероризму.

Методи дослідження, які використовувалися у кваліфікаційній роботі, ґрунтуються на особливостях об’єкту, предмету, мети й завдань дослідження. Було використано такі формально-логічні методи як опис і пояснення, аналогія та порівняння, аналіз і синтез, формалізація та інші, емпіричні методи дослідження. Також у процесі дослідження використовувався системний метод дослідження.

Практичне значення кваліфікаційної роботи полягає в тому, що результати дослідження можуть бути використані при підготовці лекційних та практичних занять, а також як науковий матеріал для написання наукових статей та доповідей.

Структура. Робота складається зі вступу, трьох розділів, висновків, списку використаних інформаційних джерел та додатків. Загальний обсяг роботи – 75 сторінок, з них основного матеріалу – 57 сторінок.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ КІБЕРТЕРОРИЗМУ

1.1. Сутність та зміст кібертероризму, основні його види

У сучасному світі існує багато способів маніпулювання інформацією. Маніпулятивні технології все частіше використовуються для ведення інформаційних війн, знищення конкурентів, впливу на маси та багатьох інших дій. Останнім часом інформаційний тероризм став ще більш популярним [4].

Розуміння поняття інформаційного тероризму є необхідною умовою для формування більш чіткого уявлення про природу сучасного міжнародного тероризму, запобігання загрозам, які можуть зруйнувати державні інститути, основи стабільності держави та основи національної безпеки в цілому.

Інформаційний тероризм – це не лише кіберзлочинність, хоча, безперечно, вона є його частиною. Інформаційним тероризмом також вважається маніпулювання або фальсифікація інформації, а в деяких випадках – подання завідомо неправдивих фактів, що призводить до залякування населення та виникнення параноїдальних ідей. Інформаційні правопорушення суттєво впливають на інформаційну безпеку держави не лише тому, що ці правопорушення завдають значної економічної шкоди, а насамперед тому, що наслідками цих правопорушень є порушення нормальної роботи інформаційно-комунікаційних систем, а також поширення інформації, яка має протиправний характер [2].

Щодо природи інформаційного тероризму, то слід зазначити, що він відрізняється від загального уявлення про те, що політичні цілі досягаються опосередковано. Принципова відмінність тероризму від інших видів жорстокої політичної боротьби полягає в тому, що він знаходиться на межі досягнення політичних цілей, які все ще використовують насильство проти цивільного населення [7 с. 291].

Міжнародні фахівці у сфері боротьби та протидії інформаційним загрозам, зазначають, що інформаційний тероризм – це поєднання фізичного насильства та злочинного використання інформаційних систем, а також навмисне зловживання

цифровими інформаційними системами, мережами чи їх компонентами для сприяння терористичним операціям чи діям [8, с. 74].

Сучасний інформаційний тероризм характеризують як сукупність інформаційних воєн і спеціальних операцій, пов’язаних із національними чи транснаціональними злочинними структурами та спецслужбами іноземних держав. Наявність інформаційних технологій значно підвищує ризики інформаційного тероризму. Розвиток інформаційної інфраструктури суспільства сприяє створенню додаткових ризиків інформаційного тероризму.

Науковці поділяють інформаційний тероризм на:

1. Інформаційно-психологічний тероризм (контроль над ЗМІ з метою поширення дезінформації, чуток, демонстрації сили терористичних організацій).

2. Медіа-тероризм або «зловживання ЗМІ» означає «зловживання інформаційними системами, мережами та їх компонентами для терористичних актів та дій».

3. Інформаційно-технічний тероризм (пошкодження окремих елементів і всього інформаційного середовища противника в цілому: руйнування елементної бази, активне придушення ліній зв'язку, штучне перезавантаження вузлів зв'язку тощо).

4. Кібертероризм – сукупність дій, що передбачають інформаційні атаки на комп’ютерні системи, обладнання для передачі даних, інші компоненти інформаційної інфраструктури, що здійснюються злочинними групами чи окремими особами [8, с. 68].

Важливо відзначити, що на сучасному етапі широко використовується інформаційний тероризм і новітні засоби зв’язку для полегшення процесу планування операцій, проведення зборів, спілкування, прийому та передачі оперативної інформації тощо.

Під впливом медіа-тероризму людина не в змозі зорієнтуватися в необмеженому інформаційному просторі доступних даних, тому що ЗМІ тепер представлені у вигляді інструментів для конструювання недостовірної реальності. Метою цієї реальності є не відображення істини, а приховування її за допомогою

«м’якої сили», яка прагне підкорити людину за допомогою характерних для неї суджень.

Тому сьогодні не можна говорити про перехід великої кількості інформації в її якість. Особливо це стосується засобів масової інформації, зокрема Інтернету, оскільки вони служать платформою для політичних ігор, спрямованих на спотворення реального стану речей [7 с. 287].

Сьогодні кібертероризм є загрозою розвитку сучасного глобального інформаційного суспільства. Однак для визначення терміну «кібертероризм» необхідно вирішити відносно складне завдання, оскільки непросто провести чітку межу між його відмінністю від інформаційної війни та інформаційної злочинності.

Кібернетика – наука про управління, комунікацію та обробку інформації. Основним предметом вивчення кібернетики є абстрактні кібернетичні системи, від комп’ютерів до людського мозку та людського суспільства [19].

Говорячи про кібертероризм, не можна не відзначити і кіберзлочинність.

Кіберзлочинність – це незаконні діяння, які вчиняють люди, які використовують інформаційні технології у злочинних цілях. Основними видами кіберзлочинності є поширення шкідливого програмного забезпечення, злом паролів, крадіжка номерів кредитних карток та інших банківських даних, а також поширення протиправної інформації через Інтернет [21].

Відомий дослідник Д. Деннінг розумів кібертероризм як незаконну атаку або загрозу атаки на комп’ютери, мережі чи інформацію, що у них накопичується, щоб змусити владу сприяти досягненню певних політичних чи соціальних цілей.

Визначення цьому терміну дав також український учений В. Голубєв. За його словами, кібертероризм – це навмисна атака на інформацію, оброблену комп’ютером, комп’ютерну систему та мережі, яка загрожує життю чи здоров’ю людей або передбачає інші серйозні наслідки, якщо такі дії спрямовані на порушення громадської безпеки, залякування населення чи провокації військового конфлікту [12].

Інше визначення терміну було введено К. Вілсоном: кібертероризм – використання комп'ютерів як зброї або об'єкта атаки політично мотивованими

міжнаціональними або міжнародними групами, або таємними агентами, які погрожують насильством або викликають страх, щоб вплинути на уряд або змусити його змінювати політику [48 с. 106].

Дослідники М. Дж. Девост, Б. Х. Х'ютон і Н. А. Поллард визначають кібертероризм як навмисне зловживання цифровими інформаційними системами, мережами або компонентами цих систем або мереж з метою сприяння здійснення терористичних операцій або актів [47].

Види кібертероризму включають три рівні за версією «Monterey»:

1. Простий – неструктурований. Використання хаків проти інформаційних систем, як правило, використання програм, створених кимось іншим (не самими кібертерористами). Зазвичай це найпростіший вид атаки, втрати від нього мінімальні або незначні.

2. Розширений – структурований. Він дозволяє здійснювати більш складні атаки проти кількох систем або мереж і, якщо необхідно, змінювати або створювати основні інструменти злому. Організація має певну структуру, управління та інші функції повноцінних компаній. Члени таких груп також навчають нових хакерів.

3. Комплексний – координований. Дає можливість скоординованої атаки, яка може спричинити серйозні порушення в системі безпеки країни. Можливе створення складних інструментів злому. Цей вид кібертероризму має жорстку структуру, часто являє собою організацію, яка вміє тверезо аналізувати свої дії, виробляти плани атак тощо.

Виходячи з основних понять кібертероризму, можна вивести наступне визначення, яке буде вважатися основним.

Кібертероризм – це складний акт навмисної, політично вмотивованої атаки на інформацію, що обробляється комп'ютерами та комп'ютерними системами, що створює загрозу життю чи здоров'ю людей або спричиняє інші тяжкі наслідки, якщо такі дії були вчинені з метою підриву громадської безпеки, залякування населення, провокації воєнного конфлікту [24 с. 94].

Також необхідно відзначити об'єкти кібертероризму. Об'єктом кібертероризму є безпека людей і різних матеріальних об'єктів; життя, здоров'я, свобода окремих

осіб або їх груп; нормальне функціонування та фізична цілісність тих чи інших предметів і споруд (наприклад, майна, що належить тероризованим особам, установам тощо). Це об'єкти прямого насильницького впливу. Застосовуючи насильство різними способами або погрожуючи його застосуванням проти окремих осіб чи конкретних матеріальних об’єктів, терористичні організації в кінцевому підсумку розраховують на досягнення своїх цілей і завдань, послаблюючи та підриваючи загальні об’єкти тероризму [8 с. 71].

Мета кібертероризму – підірвати громадську безпеку, залякати людей та спровокувати військові конфлікти.

Для досягнення своїх цілей кібертероризм використовує електронні мережі, сучасні інформаційно-комунікаційні технології та радіоелектроніку. Особливо небезпечними є втручання в інформаційну безпеку критично важливих інфраструктур: комп'ютерних систем управління банківської сфери, оборони, промисловості та ін. Реалізація таких загроз може призвести до небезпечних наслідків для суспільства та держави [30 с. 86].

Отже, кіберзлочинність – це сукупність комп’ютерних злочинів, у яких комп’ютерна інформація є предметом злочинних посягань, а також злочинів, вчинених шляхом суспільно небезпечних діянь, предметом яких є комп’ютерна інформація.

1.2. Класифікація кіберзагроз

Комп’ютерними злочинами вважаються протиправні, суспільно небезпечні, кримінальні правопорушення, що завдають шкоди інформаційним відносинам, засоби яких забезпечують належне функціонування ЕОМ, автоматизованих систем, комп’ютерних мереж або мереж електронного зв’язку.

Об'єктами втручань можуть бути технічні засоби (комп'ютери та периферійні пристрої) як матеріальні об'єкти, програмне забезпечення та бази даних.

Відповідно до розділу XVI Кримінального кодексу «Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та

комп’ютерних мереж і мереж електрозв’язку», родовим об’єктом злочинів є частина інформаційних відносин, які можна визначити як інформаційні відносини, засобом забезпечення яких є електронно-обчислювальні машини, системи, комп’ютерні мережі та мережі електрозв’язку. Тобто зазначені у цьому розділі правопорушення, посягають на певну частину інформаційних відносин – інформаційні відносини, пов’язані із застосуванням спеціальних технічних засобів. Кримінальний кодекс перераховує кілька видів таких засобів, зокрема:

– ЕОМ (комп’ютер) – пристрій, що складається з декількох або одного взаємопов’язаного центрального процесору і периферійних пристроїв і може виконувати обчислення без участі людини [4];

– автоматизована система – організаційно-технічна система, що складається із засобів автоматизації певного виду (або кількох видів) діяльності людей і персоналу, що здійснюють цю діяльність [2];

– комп’ютерна мережа – сукупність територіально розосереджених систем обробки даних, засобів і/або систем зв’язку та передачі даних, що забезпечує користувачам віддалений доступ і колективне використання її ресурсів [5];

– телекомунікаційна мережа (мережа електрозв’язку) – сукупність технічних засобів телекомунікацій та обладнання, призначених для маршрутизації, комутації, передачі та/або отримання символів, сигналів, письмового тексту, зображень і звуків або повідомлень будь-якого роду за допомогою радіо, кабельних, оптичних або інших електромагнітних систем між кінцевим обладнанням [7 с. 193].

Залежно від цих засобів інформаційні відносини, які є загальним об’єктом досліджуваних злочинів, можна поділити на чотири види:

1. Інформаційні відносини, засобом забезпечення яких є комп’ютери.

2. Інформаційні відносини, засобом забезпечення яких є комп’ютерні системи.

3. Інформаційні відносини, засобом забезпечення яких є комп’ютерні мережі.

4. Інформаційні відносини, засобом забезпечення яких є мережі електрозв’язку [37].

Методи кіберзлочинності спрямовані, зазвичай, на отримання несанкціонованого доступу до будь-якої комп'ютерної інформації, захищеної

законом. Застосування особливих прийомів лежить в основі таких способів. Їх можна розділити на наступні групи:

– отримання доступу шляхом використання вразливостей і помилок, допущених при розробці програмного забезпечення (наприклад шляхом прихованого запуску шкідливого програмного забезпечення, замаскованого під аудіо-, графічний або відеофайл);

– отримання доступу в результаті недбалості, шляхом підбору паролів, розсилки шкідливого програмного забезпечення на поштові скриньки і т.д;

– отримання доступу за допомогою спеціального, в тому числі шкідливого, програмного забезпечення (використання цих прийомів дозволяє отримати повний або частковий контроль над комп'ютерним обладнанням, перехоплювати певну інформацію, а також передавати її за призначенням, а шкідливі програми можуть бути завантажені на комп'ютер жертви за допомогою певних прийомів з першої або другої групи методів несанкціонованого доступу до комп'ютерної інформації).

Високотехнологічні способи вчинення кіберзлочинів характеризуються можливістю одержання високих доходів від злочинів та використанням новітніх інформаційних технологій. До цієї групи включають також наступні ознаки:

– ці способи використовуються професіоналами, часто об'єднаними в злочинні угрупування, які ретельно готуються до кожного злочину;

– зловмисники використовують програмні або програмно-апаратні засоби спеціально розроблені або модифіковані для злочинних цілей;

– особлива роль відводиться пошуку можливостей знищення і приховування слідів злочину;

– досконалі комп'ютерні злочини передбачають використання мережевих телекомунікаційних технологій, що забезпечують віддалений доступ до інформації;

– як правило, вчинення комп'ютерних злочинів завдає значної шкоди чиїмось інтересам або становить реальну загрозу заподіяння такої шкоди.

Класифікація способів вчинення посягань за Шумиловим М. І.:

– незаконне вилучення носіїв інформації;

– несанкціоноване отримання інформації;

– неправомірне маніпулювання інформацією.

У загальному вигляді виходячи із способів здійснення злочинних дій, спрямованих на отримання доступу до засобів комп'ютерної техніки, Вехов В. Б. запропонував виділити п’ять головних способів здійснення кіберзлочинності. До них належать:

– вилучення коштів комп'ютерної техніки;

– перехоплення інформації;

– несанкціонований доступ до засобів комп'ютерної техніки;

– маніпуляція даними та керуючими командами;

– комплексні методи.

Традиційні способи вчинення некомп'ютерних злочинів складають першу групу. Відповідно до даної групи, метою дій злочинця є заволодіння чужим майном у вигляді засобів комп'ютерної техніки. Особливістю даної групи способів здійснення комп'ютерних злочинів буде те, що засоби комп'ютерної техніки завжди виступатимуть лише як предмет злочину, а інші інструменти, технічні засоби та обладнання будуть використовуватися як знаряддя злочину.

Способи вчинення кіберзлочинів, засновані на діях злочинця, задля отримання даних і машинної інформації за допомогою аудіовізуального і електромагнітного перехоплення належать до другої групи. Комп’ютерна техніка тут виступатиме як предмет, так і як інструмент злочинного втручання.

Дії зловмисника, спрямовані на отримання несанкціонованого доступу до засобів комп'ютерної техніки – наприклад, шляхом випадкового підбору коду відносять до третьої групи. Іноді злочинці використовують спеціально створену саморобну або заводську програму для автоматичного отримання пароля для досягнення цієї мети.

Дії злочинців, пов'язані з використанням методів маніпулювання даними і керуючими командами засобів комп'ютерної техніки належать до четвертої групи способів скоєння комп’ютерних злочинів. Найпростішим з цих методів є підміна

даних, яка здійснюється при введенні та виведенні інформації, і часто використовується злочинцями для здійснення різних протиправних дій.

До п'ятої групи способів вчинення кіберзлочинів відносяться комплексні методи. Вони передбачають використанні двох і більше «традиційних» способів та їх різноманітні комбінації.

На сьогодні відсутня єдина класифікація способів вчинення злочинів, в роботах фахівців у сфері кримінального права і криміналістики мало спільного з питання про види способів вчинення кіберзлочинів. Зважаючи на це, питання, пов’язані з розробкою кваліфікації кримінальних правопорушень у літературі залишаються дискусійними.

Підводячи підсумок, слід зазначити, що сьогодні існує прямий зв’язок між ступенем розвитку інформаційної інфраструктури, комп'ютеризацією країн і кількістю подібних терактів.

Нині проблема кібертероризму та кіберзлочинності особливо актуальна для країн, які є лідерами у використанні супутникового зв'язку та глобальних мереж. На думку науковців, кібертероризм та кіберзлочинність становлять серйозну загрозу для людства, яку можна порівнювати по ефективності зі зброєю масового знищення, адже у світі немає держави, яка повністю була б захищена від кібертерористичних атак.

1.3. Міжнародно-правове регулювання кібертероризму

Перші закони стосовно комп’ютерних злочинів були прийняті ще у 70-80 роках більшістю промислово розвинутих країн. Таким, наприклад, є Computer Fraud and Abuse Act 1984, який був прийнятий у Сполучених Штатах Америки, адже саме вони зазнають найбільших втрат від кібертероризму. На цьому процес вдосконалення законів у галузі кібербезпеки не припиняється й досі, враховуючи стрімкий розвиток ІТ.

З 1991 року при Генеральному секретаріаті Інтерполу функціонує робоча група з питань кіберзлочинності, яка вивчає даний різновид правопорушень у різних

країнах світу, дає рекомендації, допомагає стандартизувати національне законодавство та розвиває методологічний досвід у сфері запобігання та розслідування кіберзлочинності [40].

У квітні 1995 року відбулася Перша міжнародна конференція Інтерполу з кіберзлочинності. У конференції взяли участь представники правоохоронних органів, співробітники різних спецслужб, співробітники великих банків та різні ІТ-спеціалісти з 49 країн світу.

У 2000 році 10-й Конгрес із запобігання злочинності та поводження з правопорушниками, проведений в рамках ООН, підкреслив постійне зростання глобальної кіберзлочинності та появу нових видів злочинів у сфері високих технологій. Відзначалася також неспроможність держав і організацій впоратися з кількістю правових проблем, що зростає на національному та міжнародному рівнях.

У березні 2001 року Комісія ООН із запобігання злочинності та кримінального правосуддя представила спеціальну доповідь, підготовлену відповідно до Резолюції 1999/23 від 28 липня 1999 року. У цій доповіді експерти з питань боротьби з кіберзлочинністю надали класифікацію кіберзлочинів [70].

Саме ця класифікація лягла в основу першого міжнародно-правового акту про форми та види кіберзлочинності. 23 листопада 2001 року в Будапешті (Угорщина) було підписано Конвенцію про кіберзлочинність, до якої приєдналися 30 країн. Ця Конвенція встановлює найбільш загальні та водночас визначальні принципи забезпечення заходів боротьби з кіберзлочинністю на національному та міжнародному рівнях. Відповідно до статті 23 сторони співпрацюють між собою шляхом застосування відповідних міжнародних документів про міжнародне співробітництво у кримінальних справах, угод, укладених відповідно до єдиного або взаємного законодавства та внутрішньодержавного законодавства для розслідування або переслідування злочинів, пов’язаних із комп’ютерними системами та даними або для збору доказів в електронній формі, що стосуються кримінальних правопорушень.

Конвенція визначає чотири категорії злочинів проти конфіденційності, цілісності та доступності комп'ютерних даних і систем: злочини, пов'язані з

незаконним доступом до інформації: неправомірне перехоплення (стаття 3), втручання у дані (стаття 4), втручання у систему (стаття 5), зловживання пристроями (стаття 6), злочини, пов’язані з протиправним використанням комп'ютерів: комп'ютерна підробка (стаття 7), комп'ютерне шахрайство (стаття 8); злочини, пов’язані зі змістом, включаючи створення, поширення та зберігання дитячої порнографії (стаття 9), злочини, пов'язані з порушенням авторського та суміжного права (стаття 10) [39].

Важливим аспектом, на якому акцентується увага при вивченні Конвенції, є той факт, що вона приділяє особливу увагу співучасті в кіберзлочинності, підкреслюючи відповідальність за спробу та допомогу (стаття 11) та корпоративну відповідальність (стаття 12). Щодо санкцій за вчинення цих правопорушень, то в статті 13 зазначається, що кожна країна, яка ратифікувала Конвенцію, вживає таких законодавчих та інших заходів, які можуть бути необхідними для забезпечення того, щоб злочини, встановлені відповідно до статей 2-11, каралися ефективними, пропорційними та переконливими санкціями, включаючи позбавлення свободи. Також вказується на необхідність забезпечення відповідальності юридичних осіб на принципах ефективних, пропорційних і переконливих кримінальних або некримінальних санкцій або заходів, у тому числі фінансових.

Відповідно до статті 15 Конвенції кожна країна, яка її ратифікувала, забезпечує, щоб встановлення, імплементація та здійснення повноважень і процедур, передбачених Конвенцією, регулювалися умовами та запобіжними заходами, передбаченими внутрішньодержавним правом для забезпечення належного захисту прав і свобод людини. Конвенція передбачає такі види запобіжних заходів:

– заходи загального характеру, до яких відносяться невідкладне збереження комп'ютерних даних, що зберігаються (стаття 16) та термінове збереження та часткове розкриття даних про рух інформації (стаття 17);

– заходи представлення (стаття 18), які регулюють порядок та межі видачі відповідних ордерів для здійснення необхідних процесуальних дій на національній території правоохоронними органами інших країн;

– обшук і арешт комп’ютерних даних, які зберігаються (стаття 19);

– збирання комп’ютерних даних у режимі реального часу, що включає збір даних про рух інформації в реальному часі (стаття 20) та перехоплення даних змісту інформації (стаття 21).

Щодо процесу міжнародного співробітництва у сфері безпосередньої боротьби (оперативної діяльності правоохоронних органів) з кіберзлочинцями, то Конвенція, зокрема, застосовує такі заходи:

– екстрадиція (стаття 24);

– взаємна допомога (стаття 25), коли сторони надають одна одній якомога ширшу допомогу з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами та даними, або з метою збору доказів у електронній формі щодо кримінального правопорушення;

– добровільна допомога (стаття 26), коли сторона в рамках свого законодавства може надіслати інформацію, отриману в ході її власного розслідування, іншій стороні без попереднього запиту, якщо вона вважає, що розкриття такої інформації може допомогти стороні, яка отримує інформацію, відкрити або провести розслідування або переслідування, яке стосується кіберзлочинів;

– взаємодопомога щодо тимчасових заходів, що включає термінове збереження збережених комп'ютерних даних (стаття 29) та термінове розкриття інформації про рух інформації (стаття 30);

– взаємодопомога щодо повноважень на розслідування, зокрема: взаємодопомога у доступі до збережених комп’ютерних даних (стаття 31); транскордонний доступ до збережених комп’ютерних даних за згодою або якщо вони є загальнодоступними (стаття 32); взаємодопомога у зборі даних про рух інформації в режимі реального часу (стаття 33); взаємодопомога у перехопленні даних про зміст інформації (стаття 34);

– цілодобова мережа, тобто створення та підтримка в актуальному стані мережі в рамках якої відбувається обмін різною інформацією щодо запобігання кіберзлочинності (стаття 35) [39].

Особливо важливим документом в рамках ООН є Резолюція «Про боротьбу із злочинним використанням інформаційних технологій» 2001 року. У ній наголошується на необхідності співпраці між державами та приватним сектором у боротьбі зі злочинним використанням інформаційних технологій, що має бути досягнуто шляхом: введення в законодавство відповідальності за інформаційні злочини; транснаціональне співробітництво між правоохоронними органами; міжнародний обмін інформацією з проблем злочинного використання інформаційних технологій; навчання співробітників правоохоронних органів в умовах інформаційного суспільства; захист комп'ютерних систем від несанкціонованого втручання тощо [70].

Окремо слід відзначити п. 1 Резолюції, в якому зазначено, що інформаційні технології мають бути розроблені для запобігання та виявлення злочинів, моніторингу злочинців та збору доказів. Теоретично цей пункт дає правоохоронним органам певної країни можливість у короткі терміни та з більшою ефективністю виявляти та організовувати заходи із затримання злочинців.

Однак існує можливість незаконного доступу зловмисників до цих технологій та використання прихованих можливостей систем для вчинення інформаційних злочинів, наприклад, крадіжки персональних даних. У рамках співробітництва держав-учасниць СНД у 2001 році було укладено Угоду про боротьбу з комп'ютерною інформаційною злочинністю, згідно з якою сторони співпрацюють у формі обміну інформацією, розслідувань комп'ютерної інформації, сприяння в підготовці кадрів, проведенні спільних наукових досліджень, створенні інформаційних систем, обміну нормативно-правовими актами та науково-технічною літературою з питань боротьби з кіберзлочинністю.

Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 року не містить чіткого визначення «кібертероризму», але її положень випливає, що кібертероризм – це навмисне використання протиправних повноважень, насильства,

руйнування або вторгнення в кіберсистеми, якщо такі дії можуть призвести до смерті або спричинити заподіяння шкоди особі або особам, матеріальної шкоди майну, громадських заворушень або значної економічної шкоди. Ця конвенція є відповіддю Сполучених Штатів на терористичні атаки 11 вересня 2001 року [42].

Закон «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року законодавчо закріплює доктринальні принципи кібербезпеки нашої країни, а також встановлює правову основу діяльності Національного координаційного центру кібербезпеки. Відповідно до положень цього Закону Національний координаційний центр кібербезпеки є робочим органом Ради національної безпеки і оборони України, який координує та контролює діяльність суб’єктів сектору безпеки та оборони, що забезпечують кібербезпеку, вносить пропозиції Президентові України щодо формування та уточнення Стратегії кібербезпеки України.

Набрав чинності Указ Президента України «Про Рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» від 26 серпня 2021 року № 447/2021» [66] .

Відповідно до затвердженої Стратегії, Україна створить найбільш відкритий, вільний, стабільний і безпечний кіберпростір в інтересах прав і свобод людини, соціального, політичного та економічного розвитку держави.

Національний координаційний центр кібербезпеки відіграватиме ключову об'єднувальну та координуючу роль у цьому процесі [49].

РОЗДІЛ 2. КІБЕРТЕРОРИЗМ ЯК ЕЛЕМЕНТ ДЕСТАБІЛІЗАЦІЇ СИСТЕМИ МІЖНАРОДНИХ ВІДНОСИН

2.1. Особливості інформаційної безпеки держави

Відповідно до положень Закону України «Про національну безпеку України», національна безпека України – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [61].

З даного визначення стає зрозумілим, що подолати будь-яку систему безпеки, зокрема національну, можливо трьома основними способами:

– посилити тиск за напрямами, проти яких спрямована система безпеки;

– знайти та створити такі загрози, проти яких система безпеки не спрацює;

– змінити систему інтересів, а відповідно і комплекс загроз, щоб нейтралізувати дії системи безпеки.

Ю.О. Бондар з цього приводу слушно зазначає, що система забезпечення національної безпеки не є самостійним об'єктом інтересу з боку зовнішніх або внутрішніх загроз. Потужність системи національної безпеки у спроможності протистояти загрозам [11].

Національна безпека і її складова – інформаційна безпека, являють собою складний суспільний процес, що постійно розвивається, залежно від стану і характеру суспільства, суспільних відносин, діючих концепцій, існування протилежних точок зору. Однак, чітко прослідковується взаємозалежність: чим більш розвиненим є суспільство, тим стабільнішою, стійкішою до загроз є система національної безпеки в інформаційній сфері.

Особливості національної безпеки держави розкривають зміст функціонування суспільства і держави, визначають сучасний стан і тенденції до змін суспільства.

Питання інформаційної безпеки як складової національної безпеки викликано розвитком інформаційних технологій, техніки та збільшенням кількості конфліктів

між державами. Ще за часів так званої «холодної війни» інформація та інформаційні системи залишилися дієвим інструментом впливу одних держав і народів на інші.

Найбільш цілісним, з нашої точки зору, є розуміння безпеки як стану, при якому суб'єкт не піддається дії зовнішніх та внутрішніх загроз, що можуть мати негативний вплив на нього, це надійний захист від небезпечних чинників.

Якщо розглядати категорію національної безпеки, то в сучасних умовах доцільно виділяти три цілісних підходи щодо визначення національної безпеки держави. Представники першого підходу акцентують увагу на розумінні національної безпеки як системи захисту цінностей суспільства. Серед базових суспільних цінностей вони виділяють суверенітет, сталий економічний розвиток, дотримання прав людини та громадянина, справедливість тощо. Більше того, безпека розглядається не тільки як стан захищеності цінностей, але і як процес їх поширення.

Другий підхід полягає у вивченні національної безпеки у розрізі захисту національних інтересів.

Третій підхід вказує на стійкий взаємозв'язок між категоріями суспільних цінностей та національних інтересів, потребі розуміння їх взаємообумовленості у вивченні сутності та природи національної безпеки держави [18, с. 45-46].

Вважаємо доцільним брати за основу третій підхід, так як національні інтереси як базова категорія в системі національної безпеки держави і захист суспільних цінностей є взаємодоповнюючими елементами загального концепту безпекової політики держави. Забезпечення національних інтересів (воєнно-політичний суверенітет, сталий соціально-економічний розвиток, економічний розвиток, збереження конституційного ладу) та збереження цінностей соціуму (які власне і зберігають його цілісність та можливість розвиватися в подальшому) є ключовою метою державного керівництва в модерному глобалізованому світі.

Розгляд основних підходів дав змогу провести групування наявних визначень інформаційної безпеки.

Перш за все слід чітко визначити основні ракурси з яких варто розглядати дане поняття:

По-перше, інформаційна безпека сприймається як захист інформаційного простору країни від зовнішніх негативних чинників на всіх рівнях (індивідуальному, суспільному, державному).

По-друге, як стан не тільки інформаційного, а й соціально-політичного простору, коли дотримується безпека індивіда, соціальних груп та країни у цілому. В даному контексті мова йде в основному про захист суспільства від пропаганди, маніпуляцій громадською думкою, поширення агресивних та провокаційних гасел / ідей / лозунгів і т.д.

По-третє, як право на отримання необхідних інформаційних ресурсів [17].

Сьогодні, в наукових колах умовно сформовані три підходи до трактування сутності інформаційної безпеки:

1. Правовий – визначає сутнісну природу інформаційної безпеки з точки зору її позиціонування в законодавчих актах та нормативних документах.

2. Доктринальний – аналізує сутність інформаційної безпеки, зважаючи на наявні в науковій думці теоретичні концепти та дослідницький доробок вітчизняних та зарубіжних вчених.

3. Енциклопедичний – грунтується на формалізованому розумінні інформаційної безпеки зважаючи на її трактування в енциклопедичних матеріалах та словниках [65, с. 97].

Тим не менш, вважаємо за доцільне констатувати, що, з нашої точки зору, даний комплекс підходів до визначення не відображає усіх аспектів поняття «інформаційна безпека». З цієї причини, в свою чергу, слід представити комплексну дефініцію, що дасть змогу відобразити увесь спектр елементів, які включає дане поняття.

Згідно з законодавством України інформаційна безпека – це стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому попереджається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через

негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій.

Спираючись на усе вище викладене, під інформаційною безпекою слід розуміти комплекс умов, при яких можлива захищеність життєво важливих інтересів держави, суспільства та окремого індивіда в інформаційній сфері, яка відображається в чотирьох аспектах: ціннісному (відсутність негативного впливу на громадську думку), технологічному (кібербезпека), правовому (розвиненість законодавства, що регулює правовідносини в інформаційній сфері), соціально-політичному (відсутність політичної цензури, вільний доступ до публічної інформації).

Україна усвідомлює нагальну необхідність у вдосконаленні національного законодавства у сфері інформаційної безпеки та ключову роль, яку вона відіграє на міжнародному та регіональному рівні щодо протистояння загрозам в інформаційному просторі, особливо з огляду на агресію Російської Федерації щодо України. Тому, за останні кілька років Україна розробила ряд принципових документа в сфері забезпечення інформаційної безпеки.

А саме, необхідно почати з того, що у Законі України «Про інформацію» від 2 жовтня 1992 року № 2657-XII представлений перелік головних напрямків впровадження інформаційної політики, серед яких визначено «забезпечення інформаційної безпеки України» (стаття 3) [58].

Більш розширеними, у розрізі безпекових цілей, є положення Концепції Національної програми інформатизації, схвалена Законом України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 року № 5/98-ВР, мета якої визначається синтез двох стратегічних завдань: забезпечення прав та свобод громадян України у доступі до своєчасної та достовірної інформації (при використанні інформаційних технологій), досягнення цілей інформаційної безпеки [59].

Базовими елементами корекції профільного Закону «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII є: визначення напрямків та форм державно-громадської взаємодії в межах цілей національної безпеки, зокрема в

інформаційній сфері; визначення сфер реалізації політики національної безпеки (за зразком Закону «Про основи національної безпеки України» 2003 року), а також визначення цілей безпекової політики відповідно до наявних сфер, класифікації існуючих та потенційних загроз у визначених сферах [41].

Відповідно до чинного законодавства основні принципи, напрямки та методи реалізації безпекової політики в інформаційній сфері базуються на ключових нормах «Стратегії національної безпеки України», а державно-громадська взаємодія розглядається з точки зору забезпечення ефективної конфігурації системи протидії існуючим та потенційним інформаційним загрозам національній безпеці [65]. Проте, в документі відсутній комплексний підхід до розробки способів протидії цим загрозам. Також, використовуючи термін «кібербезпека» документ фактично звужує сферу його дії лише до комунікаційного аспекту трьох елементів інформаційної безпеки, виключаючи їх змістовний компонент, що в контексті агресії Російської Федерації проти України має найпринциповіше значення.

У 2016 році рішенням Ради національної безпеки і оборони України було затверджено Доктрину інформаційної безпеки України. В документі визначено актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері [42], однак про це більш детально піде мова у наступному розділі даної роботи. Важливо наголосити, що при цьому документ не містить визначення понять: «інформаційна безпека» та «інформаційний простір», а також не розмежовує загрози на воєнно-політичні, терористичні та кримінальні, що суттєво звужує предмет її регулювання.

Крім того, наразі існує Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. Закон чітко визначає, що його положення не поширюються на відносини та послуги, пов’язані зі змістом інформації, тобто змістовний аспект інформаційної безпеки знову залишається поза межами регулювання зазначеного нормативно-правового акту [63].

Постановою Правління Національного Банку України від 26 листопада 2015 року № 829 було затверджено Постанову «Про затвердження нормативно-правових актів з питань інформаційної безпеки» [56].

Проаналізувавши основні документи у сфері забезпечення інформаційної безпеки, можна прийти до висновку, що усі ці документи мають суттєві недоліки в контексті використаної у них термінології та її змістовного наповнення, а також з позиції логіки і побудови, а тому потребують суттєвого доопрацювання.

Попри це, варто зазначити, що Україна впевнено крокує до створення повноцінної системи інформаційної безпеки держави, як з правової, так і з технічної точки зору, беручи активну участь у міжнародних ініціативах на міжнародному і національному рівні та робить свій вклад у розбудову глобальної системи міжнародної інформаційної безпеки [20, с. 204-206].

У рамках співробітництва з ООН щодо досягнень в сфері інформатизації та телекомунікацій в контексті міжнародної безпеки Україною було підготовлено та направлено три доповіді Генеральному Секретарю у відповідь на однойменну резолюцію.

Україною було запропоновано розглянути можливість реалізації таких заходів міжнародного співробітництва: введення в практику консультативних механізмів співробітництва у сфері кіберзахисту; створення системи обміну інформацією щодо моніторингу кіберпростору та системи оперативного оповіщення про початок кібератак; співробітництво з метою усунення негативних наслідків кібератак, напрацювання технічних рішень та організаційних рекомендації з цього питання. Важливо наголосити, що крім зазначених заходів, Україна виступила з ініціативою розробки міжнародно-правових актів щодо погодження єдиної термінології та правил, наприклад, Кодексу поведінки в Інтернеті [87, с. 20-21].

Крім того, в рамках ООН Україна бере участь у роботі групи експертів всебічного дослідження проблеми кіберзлочинності, що проводяться з 2011 року. Під час останнього засідання групою експертів розглядались пропозиції та зауваження до проекту всебічного дослідження проблем кібербезпеки, державами було здійснено обмін інформацією та думками щодо національного законодавства, практики, технічної допомоги та міжнародного співробітництва. Під час засідання також порушувалось питання створення нового міжнародно-правового документа з

питань кібербезпеки, проте експертам не вдалось дійти консенсусу в цьому питанні [88 с. 10].

Україна бере активну участь у роботі МСЕ, вносить пропозиції до рекомендацій МСЕ та активно захищає національні інтереси, зокрема, під час проведення у 2015 році Всесвітньої конференції радіозв'язку Україна виступила із заявою щодо порушення Російською Федерацією правил експлуатації передавальних засобів у межах офіційних кордонів України та незаконного використання українських радіочастот. Україною було також запропоновано провести в Україні тематичні заходи щодо забезпечення кібербезпеки та правомірного використання радіочастот [29 с. 249].

Активну позицію Україна займає щодо поглиблення співпраці в рамках Ради Європи. Наразі імплементуються положення Конвенції про кіберзлочинність щодо забезпечення строків збереження комп'ютерних даних, збирання і вилучення доказів в електронній формі в кримінальних справах. Україні надається постійна експертна підтримка в рамках спільного проекту Ради Європи та ЄС «Кіберзлочинність та Східне партнерство III», що спрямований на вдосконалення правових методів співробітництва публічного та приватного сектору у сфері боротьби з кіберзлочинністю та електронних доказів [27, с. 3]. Також, Україна є членом Комітету з питань Конвенції РЄ про кіберзлочинність, а тому бере участь в обговоренні підготовки проекту другого додаткового протоколу до Конвенції РЄ з метою погодження питань розмежування юрисдикцій та сприяння захисту електронних доказів.

Необхідно зауважити, що з метою реалізації курсу України на вступ до НАТО, однією з найрозгорнутіших сфер співробітництва є співпраця України з Альянсом. Так, у 2020 році було розроблено Річну національну програму співробітництва Україна – НАТО [64].

Таким чином, доцільно наголосити, що для ефективної реалізації національної політики у сфері забезпечення інформаційної безпеки необхідно:

1. Привести у відповідність існуючі правові норми у сфері забезпечення інформаційної безпеки сучасним досягненням.

2. Сформувати єдиний підхід до розуміння інформаційної безпеки з огляду на її триелементну структуру та наявність технічного та змістовного компоненту кожного з них; привести законодавство України у відповідність до цього підходу.

3. Гармонізувати існуючі правові норми у сфері забезпечення інформаційної безпеки з метою уникнення дублювання різними нормативними актами функцій органів державної влади держави в сфері забезпечення інформаційної безпеки, а також ліквідації прогалин щодо регулювання окремих її аспектів.

4. Створити технічний потенціал для протидії загрозам в інформаційному просторі.

5. Заохочувати розробку програмного забезпечення національного виробництва з метою мінімізації ризиків використання програмного забезпечення з вбудованими шкідливими програмами.

6. Сприяти впровадженню національної культури інформаційної безпеки та підвищенню обізнаності громадян і всіх зацікавлених сторін у цій сфері.

7. Заохочувати розвиток державно-приватного партнерства у сфері інформаційної безпеки.

2.2. Основні напрямки забезпечення національної безпеки в інформаційній сфері в Україні

З розвитком технологій інформаційна безпека стала ще більш складною і високозабезпечуваною. Держави мають постійно удосконалювати концепцію інформаційної безпеки, адже інформаційні загрози національним інтересам значно динамічніші, ніж економічні чи політичні, так як щодня виникають нові технологій, механізми та засоби. Кожна держава на сучасному етапі свого розвитку стає перед викликом у пошуку нових шляхів та засобів протидії інформаційним загрозам.

Серед управлінських та організаційних орієнтирів державної політики, визначених «Стратегією національної безпеки України», з огляду на предметну специфіку роботи, можна умовно виокремити два напрямки: протидію операціям проти України, які спираються на інформаційні технології, а також боротьбу із

застосуванням технік для маніпулювання суспільною думкою та кампаніями дезінформації; реалізація спільно із представниками приватного бізнесу та організацій громадянського суспільства програм із медійної культури на загальнонаціональному рівні.

Відповідні орієнтири наявні також в «Концепції розвитку сектору безпеки і оборони України», затвердженій Указом Президента України від 14 березня 2016 року № 92/2016, що на правовому рівні передбачає формування необхідних умов для залучення неурядових рухів та об'єднань до роботи з досягнення цілей безпеки та обороноздатності української держави [60].

Відповідно до положень Стратегії національної безпеки, держава зобов'язується активно та ефективно протидіяти розвідувально-підривній діяльності, спеціальним інформаційним операціям та кібератакам, російській та іншій підривній пропаганді, а також гарантує дотримання кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації [65].

На нашу думку, для забезпечення інформаційної безпеки як складової національної безпеки України ефективним є здійснення державою наступних дій:

– визначення державної політики та створення необхідної інфраструктури в інформаційній сфері;

– розробка національної електронної стратегії;

– створення інформаційної та комунікаційної інфраструктури (забезпечення доступу усім групам населення, включаючи людей з особливими потребами та людей похилого віку до інформаційних технологій);

– розробка ефективних заходів підвищення грамотності у сфері інформаційно-комунікаційних технологій.

Проаналізувавши ряд основоположних документів в забезпеченні інформаційної безпеки України, можна прийти до висновку, що важлива частина стратегії національної безпеки країни, крім захисту інформаційних систем і розвитку інформаційної структури, полягає в реалізації інформаційних протиборств у засобах мережі Інтернет.

Оскільки Інтернет розвивається надзвичайно динамічно, інформаційно-психологічний вплив здійснюється сьогодні переважно за його допомогою.

З метою протидії використанню мережі Інтернет терористами, експерти пропонують п’ять напрямків діяльності:

1. Постійне вдосконалення захисту мереж з метою унеможливлення доступу до його вразливих компонентів зловмисників на скільки це можливо.

2. Встановлення жорсткої правової відповідальності в якості стримуючого фактору для осіб, які приймають участь у агресивних терористичних актах, використовуючи мережу Інтернет.

3. Проведення постійного аналізу кіберпростору задля кращого розуміння існуючих та можливих загроз та вразливих місць.

4. Обмін розвідувальними даними між відповідними органами щодо протидії загрозам використання кіберпростору в терористичних цілях.

5. Обмеження публічного висвітлення успішно проведених кібертерористичних атак з метою позбавлення терористичних угрупувань досягнення ними політичних цілей [1, с. 23].

На нашу думку, для того, щоб ефективно протистояти реальній загрозі використання мережі Інтернет терористичними угрупуваннями необхідно прийняти відповідні заходи як на міжнародному, так і на національному рівнях.

На національному рівні рекомендується:

1. Застосовувати існуючі норми законодавства, передбачені Конвенцією Ради Європи про кіберзлочинність щодо процедури направлення запитів про взаємну допомогу за відсутності відповідних міжнародних угод.

2. Застосовувати існуючі норми законодавства про боротьбу з тероризмом до випадків кібертероризму, зокрема положення Конвенції Ради Європи про запобігання тероризму, що стосуються публічного підбурювання до вчинення терористичного злочину, а також прийняти спеціальні правові норми, спрямовані на боротьбу із використанням Інтернету в терористичних цілях.

Наступним важливим кроком є подолання проблеми організаційної та інституційної слабкості взаємодії між громадянським суспільством та державою в

питаннях інформаційної безпеки. Тут чітко простежується необхідність своєчасних системних змін у роботі виконавчих структур, наприклад у принципах діяльності Міноборони. В першу чергу на базі Директиви Міністра оборони України «Про вдосконалення співпраці органів військового управління з громадськими організаціями» [53] та Наказу Міністра оборони України «Про забезпечення участі громадськості у формуванні та реалізації державної політики у військовій сфері» [55] необхідним є формування нових принципів роботи міністерства, які будуть передбачати, по-перше, аналітичний та експертний супровід з боку громадянського суспільства, по-друге, створення умов для постійного залучення експертів провідних «think tanks» України (таких як Центр Разумкова та інші), до спільної інформаційно-аналітичної роботи із Департаментом воєнної політики та стратегічного планування МОУ.

Зважаючи на інституційну неоформленість взаємодії між громадянським суспільством та державою, важливим кроком є створення консультативного органу, який би забезпечував існування комунікації між двома суб'єктами (наприклад, Державна служба забезпечення інформаційної безпеки України). При чому важливо розмежувати компетенцію даного органу із компетенцією громадських рад, що включають в свій склад громадські організації та спілки. Досвід зарубіжних країн, зокрема США, показує, що такі органи на відміну від громадських об'єднань надають більш фахову та професійну допомогу державним структурам особливо в сфері національної безпеки.

Разом з тим, вважаємо за доцільне відзначити необхідність створення структури, діяльність якої буде направлена на включення представників такого органу в управлінський процес, використання їх «інтелектуального та експертного ресурсу» для досягнення безпекових цілей в інформаційній сфері, аналітичний супровід політики уряду. Це, в свою чергу, передбачає розробку нормативних та програмних підстав для створення даної структури шляхом:

1. Внесення змін в Положення «Про Міністерство інформаційної політики України».

2. Внесення змін в Доктрини інформаційної безпеки України (а саме до розділу 6 «Механізм реалізації Доктрини»).

3. Включення пункту про створення такого органу в План діяльності Міністерства інформаційної політики України.

Структурно такий орган має включати у складі дві групи учасників: не менше половини членів мають складати вітчизняні експерти, науково-дослідних інститутів, університетів, а також експерти у сфері інформаційної безпеки; іншу частину повинні складати представники державних інституцій (державних аналітичних центрів та науково-дослідних інститутів).

До основних напрямків роботи запропонованого органу слід віднести наступне:

1. Розробку стратегічної програми контрпропагандистських заходів, зокрема у аспекті «розвінчання міфів» про так звані злочини української влади проти мирного населення Донбасу, які поширює офіційна російська пропаганда.

2. Формування стандартів та рекомендацій по забезпеченню кібербезпеки інформаційних ресурсів Кабміну та інших центральних органів виконавчої влади і т.д.

3. Аналітичну роботу в сфері інформаційної безпеки, її моніторинг з метою виявлення ймовірних ризиків та проблем, а також формування пропозицій щодо вдосконалення стратегічної політики в сфері безпеки та оборони України.

4. Реалізацію науково-дослідних ініціатив та проектів спільно із державними аналітичними центрами, науково-дослідними інститутами при університетах, науковцями та фахівцями у сфері інформаційної безпеки.

5. Формування аналітичних доповідей та звітів із актуальних проблем в сфері інформаційної безпеки.

Загалом, ефективність аналітичної та експертної підтримки, яку вітчизняні «мозкові центри» мають можливість надавати уряду і безпековим структурам, може бути підвищена тільки шляхом відповідних змін у діючому механізмі співпраці між громадянським суспільством та державою. Мова йде не про окремі локальні кроки, а про комплексні реформи, що створять умови для підвищення продуктивності

спільної роботи обох суб'єктів. Тому вважаємо запропоновані варіанти доцільними та ефективними.

2.3. Сучасний стан та особливості інформаційної агресії РФ у вигляді кібертероризму проти України

На даний момент найбільша кібертерористична загроза для України виникає не через тенденції розвитку міжнародного кібертероризму, а через агресивну політику Російської Федерації, спрямовану на дестабілізацію і дезінтеграцію нашої держави та пов'язані з цим організації та підтримку диверсійно-терористичної діяльності квазідержавних утворень «ДНР» і «ЛНР», а також організацій сепаратистського спрямування.

У 2014 році Україна, з початком російської агресії, з 163 країн Глобального індексу тероризму перемістилася з 51 на 12 місце, а у 2015 році – на 11 місце. У 2017 році Україна зайняла 17 місце в рейтингу глобального тероризму, а у 2021 – 24, піднявшись на одне місце вгору з минулого року [90].

У 2016 році Служба безпеки України попередила вчинення 30 терористичних актів, затримала 56 учасників терористичних та диверсійно-розвідувальних груп. У 2017 СБУ попередила 17 терористичних актів і при цьому затримала 25 осіб [26]. У 2018 році кількість попереджених СБУ терористичних актів на території України становила 8, а у 2019 – 28.

Упродовж 2020 року суди винесли 192 обвинувальних вироки злочинцям, яких викрила і затримала Служба безпеки України за посягання на територіальну цілісність і недоторканність країни, а також за терористичну діяльність. Такі результати роботи СБУ за напрямом захисту національної державності, у рамках якого було розпочато загалом 335 кримінальних проваджень. Зокрема, за цей період спецслужба запобігла 7 терористичним актам і затримала 10 осіб, причетних до їх підготовки та вчинення.

У 2021 році, за матеріалами СБУ, суд покарав понад 320 осіб за тероризм і посягання на українську державність і при цьому було затримано 17 осіб, причетних

до міжнародних терористичних та релігійно-екстремістських організацій. Ще 45 іноземців, які мають відношення до тероризму, примусово повернуто до країн-походження.

Терористична активність в Україні у період з 2014 року по 2022 рік має такі характерні прояви: використання «класичної» тактики терору (вибухи, залякування, диверсії тощо) не тільки в районі проведення антитерористичної операції, а й в інших регіонах України; застосування важкої зброї, у т.ч. проти мирного населення; використання цивільного населення як «живого щита», наприклад, ведення вогню з житлових кварталів населених пунктів, розміщення зброї біля шкіл, лікарень, дитячих садків тощо; переслідування громадян за інші політичні або релігійні переконання; жорстоке поводження із захопленими українськими військовослужбовцями, проукраїнські налаштованими мешканцями Донбасу тощо; перешкоджання діяльності міжнародних, у т.ч. гуманітарних, організацій: недопущення гуманітарних конвоїв ООН, погрози та обстріли Спеціальної моніторингової місії ОБСЄ, виведення з ладу та викрадення спостережного обладнання ОБСЄ; активний пропагандистсько-психологічний маніпулятивний вплив на молодь, яка проживає в ОРДЛО; активне використання мережі Інтернет (пропаганда, вербування тощо).

Нині стає очевидним, що багатьом сучасним війнам передують інформаційні війни. Україна, на жаль, не стала винятком зазначеного ходу подій, перетворившись на об’єкт політичних маніпулювань з боку Російської Федерації за допомогою інформації. Так війна на теренах нашої держави розпочалася задовго до відкритого військового конфлікту. Ще від початку незалежності України російські канали супутникового мовлення, радіомовлення транслювали передачі, кінопродукцію із своєю викривленою ідеологією, спрямованою на підрив європейських цінностей та нагнітання міжетнічної ворожості, у тому числі маніпулювання мовними, релігійними, економічними питаннями. Нині латентна форма війни за допомогою інформації переросла у відкритий збройний конфлікт.

Україна виявилася досить вразливою до російської інформаційної агресії. Саме на зламі 2013-2014 років пропагандистська антиукраїнська кампанія

Російської Федерації показала недостатній рівень розробленості наукових та методологічних напрацювань у сфері інформаційної безпеки України та виявила слабку координацію діяльності державних органів, науковців та суспільства для протидії інформаційній агресії, яка справила значний вплив на свідомість українського суспільства.

Революція Гідності була кваліфікована Російською Федерацією як «фашистський переворот», а у російській громадськості, успішно навіювалася думка, що в Україні до влади прийшли «сили ультра-націоналістичного і фашистського характеру». Такі підміни понять, у свою чергу, вписуються у категорію загроз Російської Федерації, які декларує Стратегія національної безпеки Російської Федерації, а саме: «діяльність радикальних суспільних об'єднань і угруповань, які використовують націоналістичну і релігійно-екстремістську ідеологію, іноземних і міжнародних неурядових організацій, фінансових і економічних структур, а також приватних осіб, спрямована на порушення єдності і територіальної цілісності Російської Федерації, дестабілізацію внутрішньополітичної та соціальної ситуації в країні, включаючи інспірування «кольорових революцій», руйнування традиційних російських духовно-моральних цінностей» [50].

Подібні інсинуації, поширені на міжнародному рівні, стали сурогатом морального виправдання анексії Криму, підтримки сепаратистів і відкритої агресії, поданих як захист місцевого населення, зокрема у фразеології про «каральні заходи київської хунти». Вони також спрямовані, з одного боку, на дискредитацію політики Заходу щодо підтримки України і стримування Російської Федерації, а з іншого – мають на меті розколоти демократичний світ, граючи на геополітичних нюансах західних країн та їх лідерів. Саме тому активно використовується проросійське лобі в окремих країнах і міжнародних організаціях [44].

Ситуація, яка склалася на Сході нашої держави та в Криму, була зумовлена залежністю інформаційного простору від Російської Федерації, яка ще з початкуне незалежності здійснювала інформаційний вплив та інформаційно-психологічні операції, направлені на підрив національних інтересів та безпеки України. На цих

територіях було створено потужний медійний ґрунт: телеканали, друковані видання, FM-радіостанції, Інтернет-ресурси. Населення Донбасу та Криму знаходилося під постійним кремлівським ідеологічним впливом ЗМІ. Проте українська влада, володіючи реальною ситуацією, не забезпечила розвиток проукраїнських ЗМІ у цих регіонах на противагу російським.

Ефективність «обробки» Донбасу забезпечується мотивованими російськими журналістами. У травні 2014 року 300 співробітників галузі («Первый канал», «Russia Today» и холдинг Life News, жодного з «Дождя» чи «Эхо Москвы») В. Путін нагородив різними орденами та медалями «за високий професіоналізм та об'єктивність у висвітленні подій у Республіці Крим» [38, с. 169].

Українські ЗМІ фактично не мають жодного впливу на російські медіа. Спроби підвищити ефективність роботи української преси у протидії інформаційній агресії в умовах війни доводиться робити на тлі економії коштів, диверсифікації підходів до роботи ЗМІ. Відтак українські ЗМІ зіштовхуються з викликами, які мінімізують їх вплив у подоланні російської дезінформації.

Проблемою ефективної діяльності українських ЗМІ стала олігархізована система медіа-власності. Це стало на заваді розвитку незаангажованої і правдивої журналістики. Провідні телеканали країни з найбільшим охопленням аудиторії перетворилися в руках власників-олігархів на інструменти політичного впливу та захисту власних інтересів. Для прикладу, в розпал війни на сході новини телеканалів «Інтер» (у власності Дмитра Фірташа та Сергія Льовочкіна, вихідців із команди Віктора Януковича) та «1+1» (у власності Ігоря Коломойського) використовувалися в корпоративних війнах двох олігархічних груп. Щодо телеканалу «Україна», то у новинах традиційно висвітлюється благодійна діяльність його власника Ріната Ахметова [29, с. 260]. Далеко не всі медіа, які позиціонують себе як незалежні, насправді такими є. Російський інформаційний вплив прослідковується і через такий український канал як «ТВІ».

Російські радіостанції мали широку аудиторію в Україні. До прикладу «Наше радіо» – 27,7% слухачів, «LuxFM» – 20,6%, «Русское радио» – 15,3%, HitFM – 15,2%, «Мелодія» – 9,5%. Також Національна рада з питань телебачення і

радіомовлення (з причин недостатньої кількості україномовних програм в ефірі) не продовжила ліцензію для «Радио Вести» у Харкові [31].

За результатами опитування, проведеного Київським міжнародним інститутом соціології на замовлення ГО «Детектор медіа», що проводилося з 3 по 12 грудня 2016 року, українці продовжували дізнаватись інформацію про стан справ у країні переважно з українських загальнонаціональних телеканалів – 87,1% віддавало перевагу цьому виду ЗМІ. 40,7% опитаних отримувало інформацію з онлайн-ЗМІ. Загальнонаціональні газети та радіо суттєво відставали – 17% та 16,5% відповідно. Водночас з російських телеканалів отримували інформацію 7,9% українських громадян. У той же час майже половина опитаних (47,7%) отримувало інформацію про події з неофіційних джерел – від родичів, друзів, сусідів, колег по роботі. Сьогодні ж, українським ЗМІ довіряють найбільше як джерелу інформації про збройне протистояння, а довіра до російських телеканалів майже на нулі.

На запитання «Яким з перерахованих джерел інформації про збройне протистояння на Донбасі Ви довіряєте?» у 2016 році 40,4% опитаних громадян України відповіли, що це українські загальнонаціональні телеканали. На Сході довіра до центральних телеканалів значно нижча, і становила 22,2%. На другому місці, зі значним відривом, за довірою – родичі, друзі, сусіди, колеги по роботі (18,8%), на Сході ця цифра складала 13,4%. На третьому – Інтернет-ЗМІ – 17,5% (на Сході – 14,2%). Іншим видам ЗМІ довіряло вкрай мало: радіо – 5,3% (Схід – 0,5%), газети – 3,8% (Схід – 1,4%), соцмережі – 7,1% (Схід – 1,9%).

Російським телеканалам як джерелу інформації про збройне протистояння на Донбасі довіряло лише 1,3% респондентів по всій Україні (на Сході – 0,8%).

Основними телеканалами, з яких черпалася інформація про збройне протистояння в Україні були: «1+1» – 43,1%, «Інтер» – 34%, «Україна» – 20,1%, СТБ – 15,7%, ICTV – 15,3%. Російські канали значно відставали: «Россия» – 1,7%, «Первый канал» – 1,1%, НТВ – 0,9%, «Дождь» – 0,2%.

Громадянам недостатньо інформації про державну стратегію щодо окупованих та непідконтрольних територій. 41,7% опитаних вважають, що мають недостатньо інформації про стратегію та цілі держави щодо Криму, 29,1% відповіли, що взагалі

не отримують її. Також 44,9% громадян вважають, що недостатньо інформації про стратегію та цілі держави щодо територій на Сході, непідконтрольних сьогодні Україні, 22 % зазначили, що взагалі не отримують її.

Громадянам було запропоновано відповісти на питання: «Якою мірою Ви згодні чи не згодні з наступними твердженнями, які поширюються засобами масової інформації», серед цих тверджень були такі: «Події, що відбулися взимку 2014 року в Києві – це незаконний збройний переворот» – за результатами опитування 34,3% респондентів по всій Україні погоджуються з цим. Найбільше погодилися з такою тезою на Півдні (51,1%) та Сході (57,3%) країни [77].

Україна опинилася на передовій інформаційної війни, тримаючи оборону від потужного дезінформаційного пресингу з боку Російської Федерації. Виклики інформаційній безпеці, з якими стикнувся демократичний світ після 2014 року (як-от: фейкові новини, антидемократична пропаганда через соціальні мережі та фейкові медіа, які розповсюджують ксенофобні та анти-західні повідомлення), в Україні є набагато гострішими.

Фактично війна Кремля проти України почалася з масованої пропагандистської атаки взимку 2013-2014 років. Російська медійна машина (російські телеканали, Інтернет-видання, соціальні мережі, пов’язані з Кремлем українські медіа) на повну потужність працювала для дезінформування українських громадян стосовно подій на Майдані (відомих тепер як Революція гідності). Для мобілізації потенційних прихильників подальшої інтервенції культивувалися різні страхи і стереотипи. Зокрема, громадянам говорили про нацистів, які йдуть із Західної України вбивати російськомовний схід і південь України, про підступний Захід, який привів цих нацистів до влади в Києві й тепер нацьковує їх проти Російської Федерації. Це значною мірою зробило свій внесок у дестабілізацію ситуації на сході та півдні на початку 2014 року і створило сприятливі умови для подальшої військової інтервенції.

Сьогодні значна частина антиукраїнської пропаганди фінансується та курується спецслужбами країни-агресора. В Україні російські наративи просуваються в маси через лідерів суспільної думки та відомих «експертів», які

інтерпретують факти і події у вигідному для противника світлі. Ворожа пропаганда маскується під «свободу слова», «альтернативну точку зору» або «політичну агітацію» під час виборів.

Завдання сучасної антиукраїнської пропаганди – підірвати довіру, дискредитувати українську владу, політику, економіку, культуру та інше через навмисне та масове поширення неправдивих, упереджених новин з ворожою політичною метою.

Крім цього, внести хаос у суспільну свідомість закликами до порушення державного суверенітету, територіальної цілісності України. Для сучасної пропаганди в засобах масової інформації властиві такі ознаки: зумисне свідоме поширення викривленої інформації з деструктивними намірами, спрямованими на дестабілізацію ситуації в Україні та дискредитацію її міжнародного авторитету.

Протягом 2014-2016 років було прийнято низку урядових рішень, спрямованих на обмеження можливостей Кремля впливати на інформаційний простір українців та посилення інформаційної безпеки [22, с. 17]:

– заборонено трансляцію російських телеканалів, що містять пропагандистський контент. Ідеться про заборону їх трансляції в ефірі та через кабельні мережі: громадяни мають вільний доступ до них через супутник та Інтернет. Перші канали були заборонені рішенням суду в березні 2014 року, тепер число заборонених російських телеканалів перевищило вісімдесят. При цьому український уряд зробив усе, щоб дотриматися норм міжнародного законодавства, тож протести російської сторони не мали успіху;

– заборонено показ російських фільмів, виготовлених після 1 січня 2013 року, а також усіх російських фільмів, що містять елементи пропаганди. Ідеться про обмеження їх демонстрації по телебаченню та в кінотеатрах; люди можуть вільно дивитися ці фільми з будь-яких носіїв, а також онлайн;

– обмежено імпорт книгопродукції з Російської Федерації;

– створено Міністерство інформаційної політики – спеціальний урядовий орган, відповідальний, зокрема, за інформаційну безпеку;

– прийнято закон про прозорість медіавласності, який дозволив суспільству краще розуміти вплив проросійських бізнесових груп на медійний простір;

– розпочато низку важливих медійних реформ (зокрема, створення суспільного мовлення та роздержавлення преси), спрямованих на демократизацію медійного середовища та покращення доступу громадян до якісних, збалансованих новин.

Незалежно від існуючої думки, що Україна програє інформаційну війну з Російською Федерацією, позитивним є те, що міжнародна думка стосовно подій у нашій державі чітко та однозначно ідентифікує Російську Федерацію як країну-агресора, а ключові гравці світової політики активно долучилися до інформаційної протидії пропаганді Російської Федерації. Крім того, в умовах українсько-російської кризи, бюрократична система державного управління України, що традиційно є консервативною й негнучкою, засвідчила достатній рівень адаптивної спроможності до умов, що склалися. До позитивних результатів роботи українського уряду у сфері державної інформаційної політики, протягом українсько-російської кризи (2014-2016 років), можна віднести наступні здобутки:

Україні довелося в стислий термін вжити досить радикальних заходів у власному внутрішньому інформаційному просторі щодо мінімізації найбільш агресивних ворожих інформаційних впливів. Водночас, зазначені заходи не можуть претендувати на цілісне вирішення проблеми, а є лише ситуативним реагуванням. Так, Україна вдалася до тимчасових заходів, пов'язаних із обмеженням мовлення чи поширення контенту, який створюється державою-агресором. Зокрема, за неодноразові порушення діючого українського законодавства в інформаційній сфері та на підставі судових рішень тимчасово припинено ретрансляцію в Україні таких російських телеканалів: «Первый канал. Всемирная Сеть», «РТР-Планета», «НТВ-Мир», «Россия-24», TVCI, «Россия-1», «НТВ», «ТНТ», «Петербург-5», «Звезда», «РЕН-ТВ», Life News, Russia Today, «РБК-ТВ», «История» (ВГТРК), «365 дней», «Мир 24».

Через офіційні механізми Державної міграційної служби, Міністерства закордонних справ, а також органів сектору безпеки і оборони України деякі з

працівників російських ЗМІ видворено з території нашої держави за відверту проросійську пропаганду та підготовку антиукраїнських постановочних сюжетів. Низку видань було позбавлено акредитації при органах державної влади. Впроваджено Державний реєстр засобів масової комунікації (зокрема, Інтернет-видань). Налагоджено контроль за дотриманням засобами масової інформації, незалежно від їх форми власності, Конституції України, законів та інших нормативних документів, тощо.

З метою забезпечення прозорості у питаннях власності Мас-медіа, недопущення російською стороною деструктивного використання українських комерційних ЗМІ проти України, започатковані процеси деолігархізації в інформаційній сфері. Зміна правил гри зумовлена необхідністю вжиття певних заходів, що їх переважною мірою спрямовано на представників Російської Федерації або контрагентів, яких вона фінансує. З метою підтримання балансу в медіа-сфері вжиті заходи щодо зміцнення засад демократичного й прозорого функціонування ЗМІ, створення для журналістів кращих можливостей реалізовувати свою професійну діяльність.

Зосереджено зусилля на повноцінному відновленні українського кіновиробництва, створенні необхідних законодавчих передумов для кіно- й телевиробництва, оптимізації діяльності Держкомкіно відповідно до потреб часу.

Вжито заходів із забезпечення інформаційної присутності України на окупованому Донбасі та Криму. У грудні 2014 року затверджено та зареєстровано нові редакції статутів Донецької та Луганської ОДТРК з новими адресами розташування організацій та оновленими колективами. За погодженням із Національною радою з питань телебачення і радіомовлення на 9 телевізійних передавачах Луганської ОДТРК, розташованих на підконтрольній державі території, транслювалася українська програма «Донбас+Україна». Зазначена програма сформувалася на базі Сєвєродонецької телерадіокомпанії недержавної форми власності – ТОВ Незалежна ТРК «ІРТА» [71, с. 76].

Посилено діяльність офіційних прес-служб Міністерства оборони України, в зоні АТО поширювалася газета «Народна армія» (як у середовищі

військовослужбовців, так і серед населення), вживалися заходи щодо інформаційно-психологічної протидії ворожій пропаганді, розпочали роботу групи цивільно-військових відносин. Проводилися інформаційні кампанії, спрямовані на профілактику сепаратизму та зорієнтовані на фіксацію доказів присутності військовослужбовців Російської Федерації на території України. Значно активнішою стала робота військових журналістів, які залучаються до роботи штабів секторів Антитерористичної операції та груп цивільно-військового співробітництва. Активніше почали використовуватися соціальні мережі для належного інформування громадян про ситуацію в зоні АТО. На регулярній основі було організоване відвідування населених пунктів на території Донецької області представниками ЗМІ держав-членів НАТО та інших закордонних ЗМІ. Проводилися прес-тури цивільних журналістів до місць дислокації військ, спільно з Міністерством інформаційної політики був підготовлений проект Embedded journalism (прикріплення журналістів до військових підрозділів у зоні АТО).

Створені структури, завданням яких є надавати об'єктивну інформацію про події в Україні, протидіяти негативним інформаційним впливам на українських громадян і міжнародний імідж держави. До них відносяться Об'єднаний інформаційно-аналітичний центр «Єдина Країна», Єдиний прес-центр з висвітлення АТО на базі СБУ, Український кризовий медіа-центр (УКМЦ), Рада з питань комунікацій при Кабінеті міністрів України, Міністерство інформаційної політики України тощо.

Налагоджена тісна співпраця органів державної влади України з представниками громадянського суспільства щодо протидії російській пропаганді. Зокрема при Міністерстві інформаційної політики України створені так звані «Інтернет-війська», що за координації Міністерства виконують контрпропагандистські завдання [71, с. 123].

Разом з тим, державна інформаційна політика України потребує адаптації до сучасних умов інформаційного протиборства з Російською Федерацією.

2017 року в Україні було розпочато масштабну хакерську атаку, в результаті якої постраждали десятки українських банків, ЗМІ, державних установ та приватних

компаній, було вражено понад 13 000 комп'ютерів та понад 200 установ. Такі кібератаки, які, крім пропаганди та шантажу, мають на меті підірвати економіку, вважаються ефективною російською зброєю в гібридному нападі на Україну [73].

З цієї причини РНБО у 2019 році вирішила ретельніше вивчити ефективність кіберзахисту електронних державних інформаційних ресурсів, після чого почала готуватися нова стратегія кібербезпеки для України.

З січня 2022 року кількість масштабних кібератак на українські державні сайти помітно зросла.

Першою з них стала кібератака 14 січня на близько 70 українських державних сайтів побудованих на CMS October компанією Kitsoft. Внаслідок цієї атаки постраждала велика кількість державних сайтів, зокрема сайт Міністерства оборони, Міністерства закордонних справ, Державної служби України з надзвичайних ситуацій, портал Дія та інші. Внаслідок кібератаки витоку даних не відбулося. Наразі Кіберполіцією України ведеться розслідування щодо причетності до кібератаки російських служб [68].

На сайті МЗС та деяких інших можна було побачити таке повідомлення: «Українець! Всі ваші особисті дані були завантажені в загальну мережу. Всі дані на комп'ютері знищуються, відновити їх неможливо. Вся інформація про вас стала публічною, бійтеся і чекайте гіршого. Це вам за ваше минуле, сьогодення і майбутнє. За Волинь, за ОУН УПА, за Галичину, за Полісся і за історичні землі».

Його опублікували українською, російською та польською мовами.

Такий вид нападу називають дефейс-атакою, під час якої зловмисники отримують доступ до сервера, на якому розміщений сайт, і замінюють чи публікують там провокативні повідомлення.

Другою була кібератка на державні та банківські сайти України 15-16 лютого 2022 року, яка тривала більше ніж п’ять годин. Кібератака вразила близько 15 українських банків, зокрема «Приватбанк», «Ощадбанк» та сайти домену gov.ua. Вартість такої атаки становила мильйони доларів, однак злочинцям не вдалося досягти своєї мети через швидку реакцію відповідальних за кібербезпеку органів та

допомогу США. На думку українських посадовців, до цього також причетна Російська Федерація, однак там цей факт заперечують [33].

Третьою масштабною кібератакою була атака на державні ресурси та банки 23 лютого 2022 року, за день до відкритого вторгнення Російської Федерації на територію України. Внаслідок неї постраждали такі державні сайти, як портали Кабміну, Верховної ради, МЗС та інші. На зламаних сайтах почали працювати шкідливі програмні засоби HermeticWiper, метою яких є знищення інформації з баз даних [74].

Під час нападу Російської Федерації на Україну 24 лютого 2022 року був атакований сайт Київської ОДА. На сайтах meta.ua та i.ua були виявлені e-mail листи з фішинговими посиланнями на приватні адреси українських військових та пов'язаних осіб [16]. За даними Державної служби спеціального зв'язку та захисту інформації за цим стоять білоруські хакери з групи UNC1151, які працюють в Мінську.

Атаки у мережі часто координуються з операціями на полі бою. Так, наприклад, наприкінці лютого 2022 року російські хакери атакували один із великих українських радіотелецентрів. Того ж дня російські військові повідомили про наміри знищити українські «центри дезінформації». Одночасно було завдано ракетного удару по телевежі у Києві.

Мета цих скоординованих нападів – порушити роботу уряду та військових України та підірвати довіру громадськості до цих державних інститутів.

Реакція світової спільноти була швидкою та потужною. 18 лютого український уряд звернувся до ЄС з проханням про допомогу у захисті державних сайтів від кібератак у листі до лідерів ЄС, яке побачило POLITICO. У відповідь країни ЄС, зокрема Хорватія, Естонія, Литва, Нідерланди, Польща та Румунія, мобілізували Кіберкомандування швидкого реагування, щоб допомогти Україні боротися з російськими кібератаками [81].

Міжнародне угруповання хактивістів Anonymous, яке було засноване у 2003 році, 24 лютого 2022 року проголосило «кібервійну» проти російської влади та президента Російської Федерації В. Путіна. Про це група заявила у Twitter. Спершу

під хакерську атаку потрапив російський сайт новин Russia Today, наступним став сайт Міноборони Російської Федерації. Хакери опублікували дані співробітників у вільний доступ.

25 лютого 2022 року кіберпідрозділи України отримали доступ до системи бухгалтерії та документообігу ДСК (для службового користування) ВЧ 6762, Ставропольський край, Залізноводськ. Там були паспорти, військові квитки, особисті дані, список кредитних карток військовослужбовців, які були відправлені в Україну [36].

26 лютого міністр цифрової трансформації України Михайло Федоров оголосив про створення ІТ-армії з кіберфахівців, копірайтерів, дизайнерів, маркетологів і таргетологів. Вони атакували російські урядові сайти та банки. Зокрема, у відкритому доступі були оприлюднені номери російських зірок і чиновників, на деяких російських телеканалах звучали українські пісні, зокрема «Молитви за Україну».

У реаліях українсько-російського конфлікту наша держава не в змозі відмовитися від моделі інформаційного протиборства «пропаганда – контрпропаганда». Дана модель є ефективною в умовах війни, але, на жаль, має свої недоліки. Зокрема:

– недосконалість галузевої нормативно-правової бази, необхідність її подальшої адаптації до вимог внутрішнього розвитку, з одного боку, і до вимог Європейського Союзу та Ради Європи – з іншого;

– гострий брак системної, комплексної та ефективної державної політики розвитку інформаційного суспільства, громіздка й непродуктивна система державного управління та регулювання, відсутність кореляції між стратегічними проектними документами і реальною адміністративно-політичною та регуляторною практикою держави, хронічне недофінансування сфери з Державного бюджету, недосконалі й непрозорі механізми її фінансування;

– недостатня розвиненість національної інформаційно-комунікаційної інфраструктури: неподолана цифрова нерівність між регіонами України, значна кількість застарілих телекомунікаційних мереж, низькі показники проникнення

широкосмугового доступу до мережі Інтернет та мобільного зв'язку стандарту 3G та 4G, надто повільний розвиток сегментів е-урядування, е-освіти, е-медицини, е-комерції, ІТ-послуг.

Виходячи з усього вищесказаного, пріоритетними напрямами вдосконалення державної політики інформаційної безпеки в умовах протидії гуманітарній експансії Російської Федерації проти України повинні стати:

1. Зосередження на ефективному впровадженні у національний інформаційний простір суспільного мовлення, відновлення довіри населення до українських ЗМІ, впровадження прозорості медіа-ринку та проведення його демонополізації, що створить умови для розвитку незалежних ЗМІ.

2. Контроль за діяльністю Інтернет-ресурсів України, що в умовах інформаційної війни можуть створюватися російськими спецслужбами в соціальних мережах з метою координації і організації дестабілізаційних процесів в українському суспільстві.

3. Концентрування уваги на роботі з представниками регіональних ЗМІ (областей, районів, міст тощо).

4. Вжити заходи щодо налагодження ефективної політ-інформаційної роботи у військах із залученням представників ЗМІ.

5. У протидії російському пропагандистському впливу доцільно займати наступальну позицію, а не вживати «оборонні» заходи, так як у психологічному сенсі, виправдання об'єкта атаки породжують у населення асоціації його винуватості.

РОЗДІЛ 3. ВДОСКОНАЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ ЩОДО ПРОТИДІЇ КІБЕРТЕРОРИЗМУ

3.1. Зарубіжний досвід боротьби з кібертероризмом та можливості його імплементації в Україні

За оцінками експертів, у сфері кібернетичної безпеки переважна більшість провідних країн світу має стійку тенденцію до значного збільшення кількості та розширення спектру кібератак з метою порушення конфіденційності, цілісності та доступності державних інформаційних ресурсів, у тому числі тих, що циркулюють на об'єктах критичної інформаційної інфраструктури [62].

Сьогодні немає сумнівів у тому, що чинний в Україні механізм забезпечення кібербезпеки є недосконалим та потребує удосконалення. У цьому контексті відмітимо, що визначення шляхів удосконалення такого механізму є неможливим без вивчення зарубіжного досвіду, що особливо є актуальним у прагненні України адаптувати вітчизняне законодавство до європейських стандартів. Саме тому в контексті представленого наукового дослідження ми приділимо увагу досвіду найуспішніших країн Європи.

Розглядаючи країни Європи, слід приділити увагу досвіду Великобританії, адже сьогодні в цій країні питання кібербезпеки виходять на перші місця, що підтверджується тим, що у листопаді 2016 року Уряд Великої Британії оприлюднив 5-річний план реалізації Стратегії національної кібербезпеки [86] і виділив на це рекордні 1,9 млрд. фунтів. Основними законодавчими актами у сфері забезпечення кібербезпеки у Великобританії є Конституція – як Основний Закон, та Закони «Про боротьбу з комп'ютерними злочинами» (1990); «Про захист даних» (1998); «Про шахрайство» (2006), тощо.

Основним документом, що спрямований на забезпечення кібербезпеки у Великобританії, є Стратегія національної кібербезпеки 2016-2021 років, яку було прийнято замість аналогічної стратегії 2011-2015 років. Основна мета Стратегії

полягає в тому, щоб зробити Великобританію безпечною і стійкою до кіберзагроз, процвітаючою і впевненою в цифровому плані державою.

Слід також відмітити, що ця Стратегія стосується кіберзлочинності в контексті двох взаємопов'язаних форм злочинної діяльності:

– злочини, пов'язані з використанням кібератаки – традиційні злочини, які можуть бути збільшені в масштабі або охоплені за допомогою комп'ютерів, комп'ютерних мереж або інших видів ІКТ (таких як шахрайство з використанням кібертехнологій і крадіжка даних).

– кіберзалежні злочини, тобто злочини, які можуть бути здійснені тільки з використанням пристроїв інформаційно-комунікаційних технологій (наприклад, розробка та поширення шкідливого програмного забезпечення для фінансової вигоди, злому з метою викрадення, пошкодження, спотворення або знищення даних).

Відповідно до положень чинного законодавства, основний обов'язок уряду Великобританії полягає в тому, щоб захистити країну від нападів інших держав, захистити громадян і економіку від шкоди і встановити внутрішні і міжнародні рамки для захисту інтересів країни. Будучи власником значних даних і постачальником послуг, уряд приймає суворі заходи для забезпечення гарантій для своїх інформаційних активів. Уряд також несе відповідальність за консультування та інформування громадян про стан виконання Національної стратегії кібербезпеки. Крім того, уряд інформує громадян про те, що потрібно зробити, щоб захистити себе в Інтернеті та встановлює стандарти, дотримання яких Великобританія очікує від ключових компаній і організацій.

У Стратегії підкреслюється: незважаючи на те, що ключові сектори економіки країни знаходяться в приватних руках, уряд в кінцевому рахунку несе відповідальність за забезпечення національної безпеки.

Особливу увагу слід звернути на те, що з метою реалізації Стратегії від 1 жовтня 2016 року було створено Національний центр кібербезпеки (NCSC) [89]. NCSC надає унікальну можливість для створення ефективних партнерських

відносин в області кібербезпеки між урядом, промисловістю і громадськістю для забезпечення безпеки Великобританії в Інтернеті.

Ключові сектори зможуть безпосередньо взаємодіяти з Центром для отримання рекомендацій і підтримки щодо захисту мереж і систем від кіберзагроз. NCSC забезпечує:

– єдине джерело консультацій для попередження загрози кібербезпеки і забезпечення інформації;

– ефективну та прозору роботу уряду по боротьбі з кіберзагрозами, співпрацюючи з промисловістю, науковими колами та міжнародними партнерами, щоб захистити Великобританію від кібератак.

Наступна європейська країна, досвіду якої слід приділити увагу – Німеччина, адже саме ця країна є однією з найважливіших країн, державно-приватне партнерство якої є одним із головних інструментів ефективної системи кіберзахисту в країні. Однак в останні роки в Німеччині кіберзлочинність різко зросла.

У 2016 році у зв'язку із використанням Інтернет-технологій було скоєно 82 649 злочинів, тоді як у 2015 році поліція зафіксувала 45 793 кібер-злочини. Загалом кількість виявлених злочинів подібного роду зросла з 5,9% до 38,7%. І ця тенденція в державі досі зберігається [72]. В результаті Федеральний канцлер Німеччини з 2005 до 2021 року А. Меркель підкреслила, що кібербезпека є «надзвичайно важливою». Вона зазначила, що федеральний уряд оновив свою стратегію кібербезпеки. Крім того, федеральний уряд готовий працювати з містами та муніципалітетами. Вона також закликала представників місцевих органів влади та компаній у разі підозри скоєння кіберзлочинів звернутися до Федерального управління з питань захисту інформації.

Як і у Великобританії, у 2011 році в Німеччині було прийнято Стратегію кібербезпеки Німеччини, відповідно до якої федеральний уряд застосовує заходи на основі вже створених структур за наступними стратегічними напрямками [80].

У липні 2015 року в Німеччині було прийнято Закон про інформаційну безпеку з метою запобігання нападам на важливі інформаційні системи. Закон встановлює стандарти кібербезпеки для більш ніж 2000 компаній з критичною

інфраструктурою. Ці стандарти безпеки мають бути досягнуті шляхом покращення доступності, достовірності, конфіденційності та цілісності безпеки ІТ по всій Німеччині, підвищення безпеки Інтернету для громадян; поліпшення захисту критичної інфраструктури загальнодержавного значення.

Таким чином, в Німеччині досить багато уваги приділяється питанню забезпеченню кібербезпеки, про що яскраво свідчить розгалужена система органів державної влади у досліджуваній сфері. Крім того, в державі активно застосовується міжнародне співробітництво, що, в свою чергу, дозволяє більш ефективно та оперативно виявляти загрози у досліджуваній сфері та розвивати вітчизняне законодавство і технології. Із позитивного також слід вказати те, що в країні постійно відбувається розширення заходів, спрямованих на реалізацію державної політики у сфері забезпечення кібербезпеки.

Розглядаючи досвід Франції, слід відзначити, що базовими нормативними актами, в яких визначаються стратегічні напрями політики національної безпеки Франції, є Біла книга про оборону та національну безпеку 2008 року [84] та Національна стратегія цифрової безпеки 2015 року [83].

Біла книга представляє найбільш ймовірні загрози територіям Франції та Європейського співтовариства: тероризм, використання балістичних ракет, організована злочинність, природні небезпеки та ускладнення епідеміологічної ситуації у великих містах, прихована імміграція, далекосяжні напади на інформацію, шпигунство та стратегічний вплив.

Що ж стосується Стратегії, то вона покликана супроводжувати цифровий перехід французького суспільства і відповідає новим викликам, які пов’язані зі зміною використання цифрових технологій і пов'язаними з ними загрозами.

Міністерство Європи і закордонних справ координує роботу Франції в сфері «кібердипломатії». Франція особливо активна в рамках ООН, де обговорюються правила відповідальної поведінки в кіберпросторі. Франція брала участь в останніх п’яти групах урядових експертів ООН (GGE) з кібербезпеки, чия робота допомогла розмістити кіберпростір в міжнародній системі, створеній Статутом Організації

Об’єднаних Націй, і направляти держави до запобігання, співпраці і нерозповсюдження злочинності в кіберпросторі.

Відповідно до національної Стратегії кібербезпеки, французька держава працює над забезпеченням безпеки ІТ-систем в напрямку колективного реагування, цифрової довіри, що є необхідним для стабільності держави, економічного розвитку і захисту громадян. Таким чином, зміцнення стратегічної стабільності і міжнародної безпеки в кіберпросторі є однією з ключових цілей Франції. Тому вона відіграє активну роль в просуванні безпечного, стабільного і відкритого кіберпростору.

Таким чином, узагальнюючи весь наведений матеріал у представленому підрозділі дипломного дослідження, можемо із впевненістю констатувати, що досі глобальні тенденції розвитку інформаційного суспільства спонукали всі країни світу до вжиття заходів з кібербезпеки. Не є новиною, що Україна знаходиться лише на перших етапах розвитку цього інституту.

Аналіз досвіду вищезазначених країн дозволяє нам визначити такі напрямки розвитку Інституту кібербезпеки в Україні:

1. Необхідно збільшити фінансування компаній, діяльність яких спрямована на забезпечення кібербезпеки в країні.

2. Слід покращити якість підготовки кібер-поліцейських.

3. Стратегію кібербезпеки України необхідно повністю оновити. Можна з упевненістю сказати, що вона повинна бути більш всебічною і охоплювати більше, ніж просто основні теми. У цьому контексті досвід Великобританії та Німеччини є цікавим, оскільки стратегії кібербезпеки охоплюють практично кожну тему та усі ключові документи у цій галузі.

4. Міжнародне співробітництво в галузі кібербезпеки потрібно посилити, не обмежуючи співпрацю лише з певними країнами.

5. Контроль в Інтернеті потрібно посилити (наприклад, у Німеччині). Ця пропозиція виправдана, перш за все, тим, що нині в мережі з’являється стільки так званих «помилкових» повідомлень, які лише вводять в оману населення та підривають довіру до певних державних органів (найчастіше правоохоронних органів) та держави загалом.

Позитивним моментом є те, що Закон України «Про основні засади кібербезпеки України» закріпив концепцію кіберзагроз як існуючі та потенційні явища та фактори, які загрожують життєво важливим національним інтересам України в кіберпросторі та негативно впливають на кібербезпеку в державі. Однак, надаючи визначення даному терміну, поза увагою залишилося те, що все ж таки існує велика кількість конкретних видів кіберзагроз.

3.2. Проблемні аспекти протидії кібертероризму в Україні

У сучасному глобальному інформаційному суспільстві кіберзлочинність загрожує зростанню світової економіки та особистої безпеки громадян. Підвищення культури поведінки людей в Інтернеті, медіаграмотність та просування глобальних правил проти кіберзлочинності можуть забезпечити захист міжнародної спільноти. З цієї причини інформаційна безпека та управління критичною інфраструктурою обговорюються на різних зустрічах світових лідерів так часто.

В Україні діє команда реагування на комп'ютерні надзвичайні події України (CERT-UA) [79]. Команда постійно вживає заходів щодо взаємодії з іншими командами CERT держав-членів, а також з розвідувальною групою Cisco Talos з питань подолання наслідків кібератак на критичну інформаційну інфраструктуру та виявлення причин та обставин кібер-інцидентів. Крім того, враховуючи своє членство в міжнародних інституціях, беручи до уваги взяті на себе зобов’язання та важливість державно-приватного партнерства у сфері кібербезпеки, CERT-UA допомагає усунути загрози для приватного сектору України, а також для іноземного державного та приватного секторів.

Варто зазначити, що Закон України «Про основні засади кібербезпеки України», серед іншого, визначає завдання CERT-UA на законодавчому рівні.

Відповідно до цього закону, CERT-UA та Центр реагування на кіберзлочинність відіграватимуть координуючу роль у заходах, спрямованих на оперативну реакцію на кібератаки та кібер-інциденти та запровадження контрзаходів, скерованих мінімізувати вразливість систем зв'язку [40]. Державна

служба зв'язку бере участь у роботі Агентства кібербезпеки ЄС та Європейського центру досліджень і компетенцій в галузі кібербезпеки, а також у запланованих ЄС навчаннях щодо впровадження Оперативної спільної схеми реагування ЄС та держав-членів на кібератаки великих масштабів [63].

З метою розвитку глобальної культури кібербезпеки та мотивації держав щодо вдосконалення національного законодавства у сфері забезпечення кібербезпеки МСЕ було розроблено Глобальний індекс кібербезпеки (NCSI) [85], що являє собою комплексне дослідження показників рівня розвитку кібербезпеки окремих країн відповідно до п'яти сфер: юридичної, технічної, організаційної, розвитку потенціалу та міжнародного співробітництва [78].

Глобальний індекс кібербезпеки забезпечує аналіз безпеки мережевого простору країн-членів ООН. Створюючи рейтинг, експерти досліджують у країнах:

– правові системи та структури, що стосуються кібербезпеки та кіберзлочинності;

– установи, що координують політику та стратегію кібербезпеки на державному рівні;

– програми досліджень, освіти та навчання, сертифікування фахівців та державних установ, що сприяють зміцненню потенціалу в галузі інформаційної безпеки;

– механізми співпраці з іншими країнами, партнерські програми та системи обміну інформацією;

– також оцінюють функції кібербезпеки.

У рейтингу Глобальної кібербезпеки (NCSI) 2021 року Україна посіла 24 місце із 160 країн, піднявшись на одне місце вгору порівняно з 2020 роком. Лідером списку є Греція.

Лідер рейтингу – Греція, яка набрала 96,10 балів. Друге місце дісталося Литві з показником у 93,51 балів, третє – Бельгії, яка має також має 93,51 балів, однак нижчий рівень цифрового розвитку. У першій п'ятірці останнє місце посіли – Чеська Республіка та Естонія з 92,21 та 90,91 відповідно.

Україна зайняла 24 позицію, залишивши позаду країни СНД - Азербайджан (85), Білорусь (60), Вірменія (90), Таджикистан (143), Киргизстан (110) та Туркменістан (152).

«Глобальний індекс кібербезпеки» також вказує на те, що з кожним роком доступ до Інтернету має все більший відсоток населення. Ця тенденція є важливим кроком у майбутнє глобального інформаційного суспільства, одночасно вказуючи на необхідність посилення кібербезпеки національного рівня.

Також Україна бере участь у роботі Агентства з кібербезпеки ЄС, Європейського центру досліджень та компетенції з кібербезпеки задля виконання Спільної оперативної схеми щодо реагування держав-членів ЄС на кібератаки.

Жовтень вважається місяцем кібербезпеки у всіх країнах ЄС [25]. Країнами проводяться заходи, присвячені підвищенню обізнаності громадськості про кіберзагрози та обмін досвідом у цій галузі.

Кампанія 2019 року фокусувалася на різних темах, що стосуються необхідності зміни поведінки та визначення можливостей, щоб допомогти користувачам визнати ризики нових технологій.

Перша тема охоплювала базову «Кібергігієну», використовуючи гігієнічну метафору для інформування про добрі звички до кібербезпеки, які є частиною щоденного розпорядку кожного. Наявність здорових практик кібербезпеки може забезпечити користувачам більше впевненості у використанні своїх пристроїв, будь то комп'ютер, смартфон чи будь-який інший гаджет, підключений до Інтернету. Основне повідомлення стосувалося того, що кібергігієна – це звичка, яку люди набувають з раннього віку та мають впроваджувати у свій розпорядок дня.

Друга тема була зосереджена на «новітніх технологіях» і наголошувала на важливості безпеки нових технологічних гаджетів та пристроїв. Технології швидко розвиваються, і важливо брати до уваги параметри безпеки та конфіденційності під час нових покупок. Розглянувши це питання, громадяни почали краще орієнтуватися у тому, що які слід знати, коли мова йде про новітні технології.

У таких проектах, як «Глобальний індекс кібербезпеки», фахівці намагаються представити кращі методики, для успішного застосовування іншими їх досвіду у

себе. Він сприяє гармонізації ІТ-практик та розвиває культуру кібербезпеки глобально.

Після випадків останніх років, а саме витоків інформації, кібератак та різноманітних вторгнень, світ почав дедалі частіше замислюватися саме про те, як запобігати таким проблемам, а не вирішити їх. І це є досить правильним, зважаючи на ситуацію у багатьох країнах світу.

З початком відкритого воєнного нападу Російської Федерації на Україну 24 лютого 2022 року число кібератак на сайти банків та державних установ України почало стрімко зростати, а їх масштаб став набагато більшим.

Лише у січні 2022 року було виявлено 6,8 млн підозрілих подій та 25,5 тис. потенційних кіберінцидентів. Крім того, фахівці зупинили 121 критичний кіберінцидент, тоді як у квітні 2021 року це число становило 53 [34].

У Microsoft вважають, що кібератаки продовжуватимуться надалі та страждатиме від них не тільки Україна, а й інші країни. «Пов'язаним із Російською Федерацією виконавцям можуть доручити розширити свої деструктивні дії за межі України, щоб помститися тим країнам, які вирішують надати більше військової допомоги Україні та вжити більш каральних заходів проти російського уряду у відповідь на агресію», – зауважив віцепрезидент компанії Microsoft з питань безпеки Том Берт [51].

Не можна не відзначити створення Центру протидії дезінформації (ЦПД) [76] . Орган був утворений відповідно до рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації», уведеного в дію Указом Президента України від 19 березня 2021 року № 106 [67].

Орган проводить аналіз та моніторинг подій і явищ у інформаційному просторі, досліджує стан інформаційної безпеки та присутність України у світовому інформаційному просторі.

Також ЦПД виявляє поточні й заплановані загрози інформаційній безпеці України, чинники, що впливають на їхнє формування, а також прогнозує наслідки для національних інтересів. Основний акцент робиться на боротьбі з поширенням неправдивої інформації в Інтернеті та фальсифікацією в ЗМІ [52].

3.3. Пропозиції щодо вдосконалення механізмів реалізації державної політики протидії кібертероризму в контексті забезпечення інформаційної безпеки України

Загальна оцінка проблем інформаційної безпеки, а також забезпечення безпеки телекомунікацій і протидія кіберзлочинності є ключовими напрямками забезпечення національної безпеки України, що, у свою чергу, сприяє зміцненню міжнародної безпеки в умовах глобалізації.

Світові процеси глобалізації, формування інформаційного співтовариства, впровадження нових інформаційних технологій підсилюють важливість такої складової національної безпеки держави, як інформаційна безпека, яка характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх і внутрішніх загроз [75].

Відповідно, до загроз інформаційній безпеці на міжнародному рівні можна віднести наступні:

– неправомірне використання інформаційних ресурсів;

– несанкціоновані дії, які мають деструктивний характер, в автоматизованих системах, в тому числі системах управління об'єктами національної критичної інфраструктури;

– використання інформаційної інфраструктури для поширення інформації, яка розпалює ворожнечу і ненависть в суспільстві або окремій країні;

– поширення інформації, яка суперечить чинному національному законодавству, а також нормам і принципам моралі;

– використання кіберпростору з метою дестабілізації суспільства, підриву економічної, політичної і соціальної системи іншої держави або дезінформація, спрямована на спотворення культурних та етнічних цінностей;

– протидія доступу до новітніх технологій, створення умов для технологічної залежності в сфері інформатизації з метою отримання переваги і контролю за кіберпростором інших держав.

В інформаційній сфері слід виділити наступні проблемні питання, які проявляються в умовах глобалізації. До них відносяться: інформаційно-психологічний вплив індивідуальної та масової спрямованості, обмеження доступу споживачів до послуг, заснованих на інформаційно-телекомунікаційних технологіях, кіберзлочинність.

Згідно з оцінками українських експертів, підвищенню рівня ймовірності реалізації зазначених вище загроз сприяють такі чинники:

– недостатній (низький) рівень комп'ютерної грамотності більшості користувачів інформаційних ресурсів і послуг кіберпростору;

– відсутність єдиного міжнародного понятійного апарату, пов'язаного з інформаційною безпекою;

– різні підходи в національному законодавстві, пов'язані з заходами щодо захисту інформації, спрямованими на створення і модернізацію (відновлення) інформаційної інфраструктури;

– різні рівні інформатизації та забезпечення безпеки інформації в інших країнах;

– потенційна небезпека, пов'язана з підключенням до інформаційно-телекомунікаційних систем коштів з деструктивними можливостями;

– відсутність визначеності в ідентифікації джерел несанкціонованих дій в кіберпросторі.

Транснаціональний характер комп'ютерної злочинності дає підставу вважати, що настав час розробки міжнародних принципів, спрямованих на зміцнення безпеки інформаційно-телекомунікаційних мереж, загальної міжнародної політики безпеки, вдосконалення форм, методів і засобів виявлення, оцінки та прогнозування загроз інформаційній безпеці.

Одним з основоположних напрямків забезпечення глобальної інформаційної безпеки є підготовка і прийняття міжнародно-правових актів, спрямованих на усунення термінологічної невизначеності в сфері інформаційної безпеки. При цьому важливим елементом є визначення міжнародно-правового статусу кіберпростору, а також нормативно-правове закріплення юрисдикції держав щодо національних

складових цього простору (за аналогією з повітряним, водним простором держав) і подальшим врегулюванням питань, пов'язаних з кібервійною, кіберагресіями, тощо.

Ключовим напрямком нормотворчої діяльності в даній сфері є також впровадження уніфікованого поняття кіберзлочинності, а також чіткої систематизації відповідних діянь.

Інші можливі заходи, які могли б бути прийняті міжнародним співтовариством для зміцнення інформаційної безпеки на глобальному рівні, можуть включати гармонізацію нормативно-правової бази в сфері захисту інформації, розробку узгоджених критеріїв і методів оцінки ефективності систем і засобів забезпечення інформаційної безпеки, взаємне визнання сертифікатів продукції в сфері захисту інформації, розширення взаємодії при вирішенні науково-технічних і правових питань забезпечення безпеки інформації. При цьому зміцнення взаємодії правоохоронних органів держав щодо запобігання комп'ютерним злочинам, застосування юридичної відповідальності є необхідною умовою успішної взаємодії на даному напрямку.

Правове регулювання формування єдиного інформаційного простору України має сприяти гармонійному розвитку інформаційних ресурсів, інформаційних послуг та інформаційного продукту в країні.

Важливість проблеми розвитку законодавства у галузі інформації та інформаційної безпеки, формування інформаційного суспільства визначається тим, що закони цієї сфери суттєво впливають на законодавче регулювання відносин у всіх сферах життя [54].

Враховуючи руйнівний інформаційний вплив країни-агресора на цільову аудиторію України та інших країн, можна виділити наступні основні напрямки заходів щодо захисту національного інформаційного простору та забезпечення національної системи інформаційної безпеки України:

1. Удосконалити правове регулювання в галузі інформаційної державної політики, яке визначало б взаємодію правоохоронних органів України з органами місцевого самоврядування, державними органами та державними установами.

2. Створити єдиний міжвідомчий координаційний орган, який би керував, координував та контролював заходи інформаційної безпеки (його можна, наприклад, створити у формі міжвідомчої комісії при РНБО).

3. Створити систему всебічного моніторингу популярних аудіовізуальних та друкованих ЗМІ, а також популярних Інтернет-ресурсів.

4. Заохочувати подальші комплексні дослідження у галузі інформаційної безпеки [2].

Слід зазначити, що пріоритетні заходи боротьби з пропагандою тероризму та забезпечення інформаційної безпеки України в цілому повинні включати:

– визначення складу, послідовності та процедури складання законопроектів та нормативно-правових актів з питань інформаційної безпеки, протидії екстремізму та тероризму, а також механізмів їх реалізації (правовий супровід);

– розробку державної цільової науково-технічної програми інформаційної безпеки, створення інформаційної бази, спрямованої на реалізацію концепції інформаційної безпеки України (науково-технічне забезпечення);

– розробку та створення організаційної структури системи інформаційної безпеки України (Міжвідомчий центр інформаційної безпеки);

– створення вітчизняної системи експертної оцінки інформації про наявність екстремістської складової (організаційна підтримка);

– забезпечення реальних потреб системи інформаційної безпеки в кадрових, матеріально-технічних та фінансових ресурсах (ресурсне забезпечення).

Врахування цих напрямків створить умови для розробки ефективної системи боротьби з пропагандою тероризму та допоможе запобігти появі загроз національній безпеці України.

ВИСНОВКИ

На основі проведеного дослідження можна зробити висновок про те, що в умовах глобальної інтеграції та жорсткої міжнародної конкуренції основною ареною зіткнень і боротьби різних національних інтересів держав стає інформаційний простір.

У кваліфікаційній роботі відповідно до поставлених завдань було визначено особливості кібертероризму як загрози інформаційній безпеці держави та заходи протидії кібертероризму на міжнародному та національному рівні. Отримані результати дозволили зробити певні висновки.

Сьогодні надзвичайно поширеним явищем є комп'ютерна злочинність, під якою прийнято розуміти сукупність комп'ютерних злочинів, де комп'ютерна інформація є предметом злочинних посягань, а також злочинів, які здійснюються за допомогою суспільно небезпечних діянь, предметом яких є комп'ютерна інформація.

Кібертероризмом є сукупність дій, що передбачають інформаційні атаки на комп’ютерні системи, обладнання для передачі даних, інші компоненти інформаційної інфраструктури, що здійснюються злочинними групами чи окремими особами. Метою таких дій є підрив громадської безпеки, залякування людей та провокація військових конфліктів.

Незважаючи на деякий розлад, непослідовність і несистематичність, українське законодавство в інформаційній сфері за останні роки було переглянуто та підлаштовано відповідно до нових викликів та загроз у військовій інформаційній галузі та відповідно агресії Російської Федерації.

Згідно з законодавством України інформаційна безпека – це стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому попереджається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій.

В Україні ключовими державними органами з питань інформаційної безпеки та її складових є Міністерство внутрішніх справ України, Служба безпеки України, а також Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку).

Правове регулювання формування єдиного інформаційного простору України має сприяти гармонійному розвитку інформаційних ресурсів, інформаційних послуг та інформаційних продуктів у країні.

Враховуючи руйнівний інформаційний вплив країни-агресора на населення України та інших країн, можна виділити наступні основні напрямки заходів щодо захисту національного інформаційного простору та забезпечення національної системи інформаційної безпеки України:

1. Удосконалити правове регулювання в галузі інформаційної державної політики, яке визначало б взаємодію правоохоронних органів України з органами місцевого самоврядування, державними органами та державними установами.

2. Створити єдиний міжвідомчий координаційний орган, який би керував, координував та контролював заходи інформаційної безпеки (його можна, наприклад, створити у формі міжвідомчої комісії при РНБО).

3. Створити систему всебічного моніторингу популярних аудіовізуальних та друкованих ЗМІ, а також популярних Інтернет-ресурсів.

4. Заохочувати подальші комплексні дослідження у галузі інформаційної безпеки.

Ці заходи в цілому повинні включати:

1. Визначення складу, послідовності та процедури складання законопроектів та нормативно-правових актів з питань інформаційної безпеки, протидії екстремізму та тероризму, а також механізмів їх реалізації (правовий супровід).

2. Розробка державної цільової науково-технічної програми інформаційної безпеки, створення інформаційної бази, спрямованої на реалізацію концепції інформаційної безпеки України (науково-технічне забезпечення).

3. Розробка та створення організаційної структури системи інформаційної безпеки України (Міжвідомчий центр інформаційної безпеки).

4. Створення вітчизняної системи експертної оцінки інформації про наявність екстремістської складової (організаційна підтримка).

5. Забезпечення реальних потреб системи інформаційної безпеки в кадрових, матеріально-технічних та фінансових ресурсах (ресурсне забезпечення).

Для захисту від дезінформації та боротьби з російською пропагандою важливо забезпечити обізнаність населення з цього питання. Перевірка отриманої інформації, уточнення відомостей через інші джерела, обізнаність у сфері методів пропагандистського впливу дають змогу виявити маніпулятивні прийоми та технології.

Врахування цих напрямків створить умови для розробки ефективної системи боротьби з кібертероризмом та допоможе запобігти появі загроз національній безпеці України.

СПИСОК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Актуальні питання протидії тероризму у світі та в Україні: аналіт. Доповідь. Резнікова О. О., Місюра А. О., Дрьомов С. В., Войтовський К. Є.; за ред. О. О. Резнікової. Київ: НІСД, 2017. 60 с.

2. Актуальні проблеми управління інформаційною безпекою держави: зб. матеріалів доп. учасн. XII Всеукр. наук.-практ. конф., 26 бер. 2021 р. Київ, НА СБУ, 2021. 346 с. URL: https://academy.ssu.gov.ua/uploads/p_57_53218641.pdf (дата звернення: 17.04.2022)

3. Актуальні проблеми управління інформаційною безпекою держави: зб. матеріалів доп. учасн. X Всеукр. наук.-практ. конф., 4 квіт. 2019 р. Київ, НА СБУ, 2019. 384 с. https://academy.ssu.gov.ua/uploads/p_57_54325835.pdf (дата звернення: 15.04.2022)

4. Антонов В. О. Конституційно правові засади національної безпеки України: монографія. Київ: ТАЛКОМ, 2017. 576 с. URL: http://idpnan.org.ua/files/antonov-v.o.-konstitutsiyno-pravovi-zasadi-natsionalnoyi-bezpeki-ukrayini-_d_.pdf (дата звернення: 12.05.2022)

5. Бабенко Ю. Інформаційна війна–зброя масового знищення! *Українська правда :* веб-сайт. URL: http://www.pravda.com.ua/rus/articles/2006/04/20/4399050/?attempt=1 (дата звернення: 07.05.2022)

6. Банк Р. О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект / *Інформація і право* 1.16. 2016 С.110-116 URL: http://ippi.org.ua/sites/default/files/17.pdf (дата звернення: 11.06.2022)

7. Бєлай С. В., Корнієнко Д. М. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки / *Актуальні проблеми управління інформаційною безпекою держави.* Київ : Національна академія Служби безпеки України, 2018. 408 с.

8. Боднар І. Р. Інформаційна безпека як основа національної безпеки / *Механізм регулювання економіки.* Суми. 2014. С. 68-75.

9. Бондар Ю. Зміцнення та захист національного інформаційного простору України: проблеми та шляхи забезпечення. Український науковий журнал: *Освіта регіону політологія психологія комунікації.* Київ. 2010. URL: http://enpuir.npu.edu.ua/bitstream/123456789/10206/1/Bondar.pdf (дата звернення: 19.06.2022)

10. Бондаренко Р. В., Михальчук В. М. Інформаційна безпека держави. Інвестиції: практика та досвід. 2021. С. 95-101. URL: http://www.investplan.com.ua/pdf/5_2021/17.pdf (дата звернення: 29.05.2022)

11. Бойко В. О. Державно-приватне партнерство у сфері кібербезпеки: кейс Німеччина: аналітична записка. Київ. Національний інститут стратегічних досліджень, Відділ інформаційної безпеки та розвитку інформаційного суспільства Національного інституту стратегічних досліджень. 2018. URL: https://niss.gov.ua/sites/default/files/2018-01/Germany-7f497.pdf (дата звернення: 06.06.2022)

12. Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України / Центр досліджень соціальних комунікацій НБУВ. 2017. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijnabezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350 (дата звернення: 29.05.2022)

13. Волох О. К. Питання кібернетичної безпеки в умовах розбудови інформаційного суспільства. Юридичний науковий електронний журнал. С. 104-107. URL: http://lsej.org.ua/4_2016/29.pdf (дата звернення: 28.04.2022)

14. Волошин Ю. О. Legal globalization and interstate integration as a leading factor of the formation of state security and sovereignty. Atlantic Press. 2nd International Conference on Social, Economic and Academic Leadership. 2018, № 11. P. 351- 358.

15. Волошин Ю. О., Замула А. Ю. The State as the Leader in Fighting International Terrorism in Globalized World. International Conference “Entrepreneurial and Sustainable Academic Leadership”. 2018. P. 491- 501.

16. Ворог атакує email-адреси українських військових на сервісах i.ua і meta.ua – Держспецзв'язку. *Економічна правда* : веб-сайт. URL: https://www.epravda.com.ua/news/2022/02/25/682770/ (дата звернення: 23.05.2022)

17. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. 2020. URL: http://dspace.lvduvs.edu.ua/bitstream/1234567890/2927/1/%d0%b3%d0%b0%d0%b2%d1%80%d0%b8%d0%bb%d1%8c%d1%86%d1%96%d0%b2.pdf (дата звернення: 18.05.2022)

18. Глазов О. В. Національна безпека: сутність, ознаки, концепція та геополітичні чинники. Науковий вісник Чорноморського державного університету імені Петра Могили «Наукові праці» Сер.: Політологія.Т. 155. Вип. 143. 2011. С. 42-46.

19. Головка А. А. Інститути громадянського суспільства в системі інформаційної безпеки України. ВІСНИК НТУУ «КПІ». Сер.: Політологія, соціологія, право. 2015. С. 13-16. URL: https://ela.kpi.ua/bitstream/123456789/22662/1/VPSP2015-3-4_13-16.pdf (дата звернення: 02.06.2022)

20. Грицун О. О. Україна на шляху до створення національної системи інформаційної безпеки: матеріали наук. конф. 204 с. URL: http://www.iir.edu.ua/uploads/files/Publikacii (дата звернення: 30.05.2022)

21. Джерела інформації, медіаграмотність і російська пропаганда: результати всеукраїнського опитування громадської думки. Аналітичний звіт. Київ. *Детектор Медіа* : веб-сайт. URL: https://detector.media/infospace/article/164308/2019-03-21-dzherela-informatsii-mediagramotnist-i-rosiyska-propaganda-rezultaty-vseukrainskogo-opytuvannya-gromadskoi-dumky/ (дата звернення: 29.05.2022)

22. Діяльність органів державної влади в сфері інформаційної політики та регуляції медіа за 1 півріччя 2017 року. Моніторинговий звіт. Київ. *Детектор Медіа*. 48 с. URL: https://ms.detector.media/content/files/dm_derjava_report_2017_internet.pdf (дата звернення: 28.04.2022)

23. Добржанська О. Л., Демцов А. А. Кібербезпека як феномен міжнародних відносин на прикладі Федеративної Республіки Німеччини. *Актуальні проблеми міжнародних відносин.* Вип. 102 (1). 2011. С. 111–116., 113–115.

24. Довгань О. Д., Ткачук Т. Ю. Система інформаційної безпеки України: онтологічні виміри / *Інформація і право № 1* (24). 2018 . С. 89-103

25. ЄС оголосив жовтень місяцем кібернетичної безпеки. *Укрінформ* : веб-сайт. URL: https://www.ukrinform.ua/rubric-technology/2790553-es-ogolosiv-zovten-misacem-kiberneticnoi-bezpeki.html (дата звернення: 11.06.2022)

26. За минулий рік СБУ попередила 30 терактів. *РБК-УКРАЇНА* : веб-сайт. URL: https://www.rbc.ua/ukr/news/proshlyy-god-sbu-predupredila-30-teraktov-1490350867.html (дата звернення: 19.06.2022)

27. Звіт щодо України від 3 листопада 2016 року / Підготовлено Офісом Програми з кіберзлочинності на основі експертної підтримки незалежних експертів Ради Європи пана Маркко Куннапу і пана Марка Юріча. 2016. UURL: https://rm.coe.int/16806f3743 (дата звернення: 06.06.2022)

28. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам / *Humanitarian vision 2. Num. 1.* 2016. С. 27-32. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf (дата звернення: 16.05.2022)

29. Інформаційна безпека (соціально-правові аспекти): підручник / Б. В. Остроухов, Б. М. Петрик, М. М. Присяжнюк та ін.; за ред. Є. Д. Скулиша. Київ, 2010. 776 с.

30. Інформаційні виклики гібридної війни: контент, канали, механізми протидії : аналіт. доп. / за заг. ред. А. Баровської. Київ : НІСД, 2016. 109 с.

31. Іщенко Н. В окопах «інформаційного фронту». Україна має знайти унікальний метод захисту від гібридної агресії. *Day.kyiv.ua* : веб-сайт. URL: https://day.kyiv.ua/uk/article/media/v-okopah-informaciynogo-frontu (дата звернення: 30.05.2022)

32. Карчевський М. В. Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Злочини в сфері використання IT. 2022. URL: http://it-crime.at.ua/index/tezi_lekcij/0-31 (дата звернення: 15.04.2022)

33. Кібератака в Україні 15 лютого була найбільшою в історії держави: в Кабміні назвали вартість. *УНІАН* : веб-сайт. URL: https://www.unian.ua/techno/communications/kiberataka-v-ukrajini-15-lyutogo-bula-naybilshoyu-v-istoriji-derzhavi-v-kabmini-nazvali-vartist-11706571.html (дата звернення: 18.06.2022)

34. Кібератаки на держоргани України: скільки інцидентів було заблоковано. *Слово і діло* : веб-сайт. URL: https://www.slovoidilo.ua/2022/02/15/infografika/bezpeka/kiberataky-derzhorhany-ukrayiny-skilky-incydentiv-bulo-zablokovano (дата звернення: 17.05.2022)

35. Кібербезпека в Україні: правові та організаційні питання: зб. матеріалів доп. учасн. Міжнародної наук.-практ. конф., 22 лист. 2019 р. Одеса: ОДУВС, 2019.108 с. URL: http://eportfolio.kubg.edu.ua/data/conference/5087/document.pdf (дата звернення: 19.05.2022)

36. Кібервійськами України отримано доступ до бухгалтерії російської військової частини. *Хрещатик* : веб-сайт. URL: https://khreschatyk.news/kibervijskamy-ukrayiny-otrymano-dostup-do-buhgalteriyi-rosijskoyi-vijskovoyi-chastyny/ (дата звернення: 10.06.2022)

37. Кіберсвіт у новому тисячолітті. Хто вони: кіберзлочинці, кібершахраї, кібертерористи? *LexInform* : веб-сайт. URL:https://lexinform.com.ua/dumka-eksperta/kibersvit-u-novomu-tysyacholitti-hto-vony-kiberzlochyntsi-kibershahrayi-kiberterorysty/ (дата звернення: 28.04.2022)

38. Конах В. К. Забезпечення безпекових імператив у медіапросторі України (контентний вимір): монографія. Київ: Видавництво «Фенікс», 2017. 540 с.

39. Конвенція про кіберзлочинність: Конвенція Ради Європи від 23 лист. 2001 р. №2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 07.05.2022)

40. Космічна й електронна кіберзлочинність: загрози і виклики нового тисячоліття. *LexInform* : веб-сайт. URL: https://lexinform.com.ua/dumka-eksperta/kosmichna-j-elektronna-kiberzlochynnist-zagrozy-i-vyklyky-novogo-tysyacholittya/ (дата звернення: 12.05.2022)

41. Кравцова М. О. Сучасний стан і напрями протидії кіберзлочинності в Україні. 2018. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/3848/Suchasnyi%20stan%20i%20napriamy%20protydii%20kiberzlochynnosti%20v%20Ukraini%20_Kravtsova_2018.pdf?sequence=1&isAllowed=y (дата звернення: 06.06.2022)

42. Крижна В. В. Історико-правовий аспект протидії кібертероризму. 2018. URL: http://elar.naiau.kiev.ua/bitstream/123456789/9442/1/%D0%90%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D1%96%20%D0%BF%D1%80%D0%BE%D0%B1%D0%BB.%20%D0%BA%D1%80%D0%B8%D0%BC%D1%96%D0%BD.%20%D0%BF%D1%80%D0%B0%D0%B2%D0%B0_p195-197.pdf (дата звернення: 16.05.2022)

43. Кубишкін О. В. Міжнародно-правові проблеми забезпечення інформаційної безпеки держави. URL: http://pravolib.pp.ua/mejdunarodno-pravovyie-problemyi-obespecheniya.html (дата звернення: 30.05.2022)

44. Литвиненко О. М. Виклики національній політиці пам'яті в часи «гібридної війни»: аналіт. записка. URL: http://www.niss.gov.ua/articles/1818/ (дата звернення: 02.06.2022)

45. Луцкий М. Г. Исследование программных средств анализа и оценки риска информационной безопасности / Луцкий М. Г., Корченко А. Г., Иванченко Е. В., Казмирчук С. В. // *Захист інформації.* 2011. №3. С. 97-108. (дата звернення: 10.06.2022)

46. Луцкий М. Г., Иванченко Е. В., Казмирчук С. В. Базовые понятия управления риском в сфере информационной безопасности // *Захист інформації.* 2011. №2. С. 86-94. (дата звернення: 10.06.2022)

47. Макеєва О. М., Загородній Д. Кіберзлочинність: теоретико-правові засади URL: https://core.ac.uk/download/pdf/286629373.pdf (дата звернення: 15.04.2022)

48. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ : Вид. дім «Гельветика», 2017. 168 с.

49. Нова Стратегія кібербезпеки України. *LexInform* : веб-сайт. URL: https://lexinform.com.ua/zakonodavstvo/nova-strategiya-kiberbezpeky-ukrayiny/ (дата звернення: 23.05.2022)

50. О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 31.12.2015 № 683 URL: http://www.consultant.ru/document/cons_doc_LAW_191669/ (дата звернення: 29.05.2022)

51. Пов'язані з РФ хакери ще до початку вторгнення здійснили 240 кібератак на Україну. *Укрінформ* : веб-сайт. URL: https://www.ukrinform.ua/rubric-technology/3469525-microsoft-povazani-z-rf-hakeri-se-do-pocatku-vtorgnenna-zdijsnili-240-kiberatak-na-ukrainu.html (дата звернення: 19.06.2022)

52. Президент затвердив Положення про Центр протидії дезінформації. *Офіційне інтернет-представництво Президента України* : веб-сайт. URL: https://www.president.gov.ua/news/prezident-zatverdiv-polozhennya-pro-centr-protidiyi-dezinfor-68317 (дата звернення: 23.05.2022)

53. Про вдосконалення співпраці органів військового управління з громадськими організаціями: Директива Міністерства оборони України від 27 квіт. 2009 р. № Д-13 URL: https://zakon.rada.gov.ua/rada/show/v0013322-09#Text (дата звернення: 13.06.2022)

54. Про Доктрину інформаційної безпеки України: Проект Указу Президента України від 1 трав. 2014 р. № 449 URL: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025 (дата звернення: 30.05.2022)

55. Про забезпечення участі громадськості у формуванні та реалізації державної політики у військовій сфері: Постанова Кабінету Міністрів України від 3

лист. 2010 р. № 996 URL: https://zakon.rada.gov.ua/laws/show/996-2010-%D0%BF#Text (дата звернення: 23.05.2022)

56. Про затвердження нормативно-правових актів з питань інформаційної безпеки: Постанова Правління Національного Банку України від 26 лист. 2015 р. № 829 URL: https://zakon.rada.gov.ua/laws/show/v0829500-15#Text (дата звернення: 02.06.2022)

57. Про затвердження плану заходів щодо реалізації Стратегії комунікації з питань євроатлантичної інтеграції України на період до 2025 року: Розпорядження Кабінету Міністрів України від 12 січ. 2022 р. № 41-р URL: https://zakon.rada.gov.ua/laws/show/41-2022-%D1%80#Text (дата звернення: 08.06.2022)

58. Про інформацію: Закон України від 2 жовт. 1992 р. № 2657-XII. С. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 29.04.2022)

59. Про Концепцію Національної програми інформатизації: Закон України від 4 лют. 1998 р. № 75/98-ВР. С.182. URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text (дата звернення: 04.05.2022)

60. Про Концепцію розвитку сектору безпеки і оборони України: Рішення Ради національної безпеки і оборони України від 4 бер. 2016 р. URL: https://zakon.rada.gov.ua/laws/show/n0002525-16#Text (дата звернення: 10.05.2022)

61. Про національну безпеку України: Закон України від 21 черв. 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 11.06.2022)

62. Про основні засади забезпечення кібербезпеки України: Пояснювальна записка до проекту Закону України від 19 черв. 2015 № 2126а. URL: https://ips.ligazakon.net/document/GH1N268A (дата звернення: 13.04.2022)

63. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовт. 2017 р. № 2163-VIII. С.403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 28.05.2022)

64. Про Річну національну програму під егідою Комісії Україна – НАТО на 2020 рік: Указ Президента України від 26 трав. 2020 р. № 203/2020. URL: https://www.president.gov.ua/documents/2032020-33861 (дата звернення: 23.05.2022)

65. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14 вер. 2020 р. № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037 (дата звернення: 06.05.2022)

66. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України №447/2021 від 14 трав. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 15.05.2022)

67. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації»: Указ Президента України №106/2021 від 19 бер. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/106/2021#Text (дата звернення: 22.05.2022)

68. Російські хакери атакували 70 державних сайтів, українські активи падають. *Економічна правда* : веб-сайт. URL: https://www.epravda.com.ua/news/2022/01/14/681463/ (дата звернення: 19.06.2022)

69. Світлична В. Ю. Інформаційна безпека: сутність та порядок реалізації / Інтернет–конференції ХНУМГ ім. ОМ Бекетова. 2015. С.97-100.

70. Скулиш Є. Д. Міжнародно-правове співробітництво у сфері подолання кіберзлочинності. *Інформація і право 1.* 2014. С.93-100. URL: http://ippi.org.ua/sites/default/files/14sydspk.pdf (дата звернення: 02.06.2022)

71. Тимчук Д., Карін Ю., Машовець К. Вторгнення в Україну: хроніка російської агресії. Київ: Брайт Букс, 2016. 240 с.

72. У Німеччині різко зросла кіберзлочинність. *Made for minds* : веб-сайт. URL: https://www.dw.com/uk/%D1%83-%D0%BD%D1%96%D0%BC%D0%B5%D1%87%D1%87%D0%B8%D0%BD%D1%96-%D1%80%D1%96%D0%B7%D0%BA%D0%BE-%D0%B7%D1%80%D0%BE%D1%81%D0%BB%D0%B0-

%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%BB%D0%BE%D1%87%D0%B8%D0%BD%D0%BD%D1%96%D1%81%D1%82%D1%8C/a-38555191 (дата звернення: 16.06.2022)

73. Україну вразила вірусна атака. *Financial club* : веб-сайт. URL: https://finclub.net/ua/analytics/ukrainu-vrazyla-virusna-ataka.html (дата звернення: 02.06.2022)

74. Федоров розповів подробиці чергової атаки хакерів проти України. *Слово і діло* : веб-сайт. URL: https://www.slovoidilo.ua/2022/02/23/novyna/polityka/fedorov-rozpoviv-podrobyczi-cherhovoyi-ataky-xakeriv-proty-ukrayiny (дата звернення: 23.05.2022)

75. Характеристика становища інформаційної безпеки України. *Vuzlit.com* : веб-сайт. URL: https://vuzlit.com/1137657/harakteristika_stanovischa_informatsiynoyi_bezpeki_ukrayini (дата звернення: 11.05.2022)

76. Центр протидії дезінформації при РНБО України : веб-сайт. URL: https://cpd.gov.ua/ (дата звернення: 22.05.2022)

77. Як російська пропаганда впливає на суспільну думку в Україні (дослідження). *Детектор Медіа* : веб-сайт. URL: https://ms.detector.media/mediadoslidzhennya/post/18384/2017-02-13-yak-rosiyska-propaganda-vplyvaie-na-suspilnu-dumku-v-ukraini-doslidzhennya/ (дата звернення: 02.05.2022)

78. Яцик Т. П. Особливості інформаційного тероризму як одного із способів інформаційної війни. Науковий вісник Національного університету державної податкової служби України. Сер. економіка, право. 2014. Вип. 2. С. 55-60. https://lib.nadpsu.edu.ua/eldocs/BooksShow8/Nvnudpsu_2014_2_10.pdf (дата звернення: 15.04.2022)

79. Computer Emergency Response Team of Ukraine : веб-сайт. URL: https://cert.gov.ua/ (дата звернення: 17.05.2022)

80. Cyber-Sicherheitsstrategie für Deutschland : веб-сайт. URL: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_download.pdf?__blob=publicationFile (дата звернення: 04.06.2022)

81. EU to mobilize cyber team to help Ukraine fight Russian cyberattacks. *Politico* : веб-сайт. URL: https://www.politico.eu/article/ukraine-russia-eu-cyber-attack-security-help/ (дата звернення: 23.05.2022)

82. Global Cybersecurity Index & Cyberwellness Profiles : report. Geneva : ITU, 2015. 516 p. URL: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf (дата звернення: 29.05.2022)

83. LA STRATÉGIE NATIONALE POUR LA SÉCURITÉ DU NUMÉRIQUE : UNE RÉPONSE AUX NOUVEAUX ENJEUX DES USAGES NUMÉRIQUES : веб-сайт. URL: https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/ (дата звернення: 04.06.2022)

84. LE LIVRE BLANC 2008 SUR LA DEFENSE ET LA SECURITE NATIONALE : веб-сайт. URL: https://www.afri-ct.org/wp-content/uploads/2010/07/Article_Buffotot.pdf (дата звернення: 04.06.2022)

85. National Cyber Security Index : веб-сайт. URL: https://ncsi.ega.ee/ncsi-index/?order=-ncsi (дата звернення: 29.05.2022)

86. NATIONAL CYBER SECURITY STRATEGY 2016-2021 : веб-сайт. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (дата звернення: 05.06.2022)

87. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/075/86/PDF/N2107586.pdf?OpenElement (дата звернення: 30.05.2022)

88. Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 6 to 8 April 2021. URL:

https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Report/V2102595.pdf (дата звернення: 11.06.2022)

89. The National Cyber Security Centre : веб-сайт. URL: https://www.ncsc.gov.uk/ (дата звернення: 04.06.2022)

90. Ukraine ranks 17th in Global Terrorism Index 2017. *Уніан* : веб-сайт. URL: https://www.unian.info/society/2244364-ukraine-ranks-17th-in-global-terrorism-index-2017.html (дата звернення: 27.05.2022)

ДОДАТКИ

Стратегії із забезпечення кібербезпеки

	Великобританія	Німеччина	Франція
Зміст Стратегії кібербезпеки	– Виділяти достатньо коштів для захисту Великобританії від кіберзагроз; – ефективно реагувати на інциденти, забезпечувати захист і стійкість мереж і даних у Великобританії.	– В центрі уваги кібербезпеки лежить захист найважливіших інформаційних структур, адже безпека має важливе значення в майже всіх постійно зростаючих найважливіших інфраструктурах.	– Гарантувати національний суверенітет.
	– Виявляти та розслідувати ворожі дії, що вживаються проти Британії.	– ІТ-системи безпеки ФРН. Захист інфраструктур потребує більшої надійності ІТ-систем громадян, а також малих та середніх підприємств.	– Забезпечити сильну відповідь на акти кіберзлочинності.
	– Розробляти та сприяти розвитку інноваційних технологій та індустрії кібербезпеки.	– Посилення ІТ-безпеки в публічному управлінні.	– Інформувати громадськість в цілому.
	– Сприяти розвитку кадрового потенціалу.	– Для оптимізації оперативної співпраці усіх державних установ і покращення координації заходів щодо захисту від кібертероризму було створено Національний центр кіберзахисту.	– Забезпечити цифрову безпеку, адже це є конкурентною перевагою для французьких підприємств.

		– Створено Національну раду кібербезпеки, діяльність якої спрямована на виявлення і усунення конструктивних причин криз.	– Посилити позиції Франції на міжнародній арені.
		– Ефективна боротьба зі злочинністю у кіберпросторі; – ефективна співпраця у кібербезпеці в Європі та у світі.	

Складено на основі [16; 72]