Міністерство освіти і науки України
Національний університет «Острозька академія»
Навчально-науковий інститут міжнародних відносин та національної безпеки
Кафедра національної безпеки та політології

Кваліфікаційна робота
на здобуття освітнього ступеня магістра
на тему: **«Кіберзлочинність як виклик державній інформаційній політиці»**

Виконала студентка ІІ курсу, групи МНб-21
спеціальності 256 Національна безпека
(за окремими сферами забезпечення і видами діяльності)
Швець Тетяна Анатоліївна
Керівник – кандидат технічних наук, старший викладач
Назарук Віталій Дмитрович
Рецензент – кандидат технічних наук, доцент кафедри обчислювальної техніки НУВГП
Сидор Андрій Іванович

Острог, 2022

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ

НАТО– Організація Північноатлантичного договору, також Північноатлантичний альянс або НАТО (англ. North Atlantic Treaty Organization)

ІТ – Інформаці́йні технолóгії, IT information and communication technologies.

ПДФО – Податок на прибуток або на доходи.

СБУ – Служба безпеки України.

ЄС – Європейський союз.

ООН – Організація Об'єднаних Націй.

ESET – (англ. Essential Security against Evolving Threats) міжнародний розробник антивірусного програмного забезпечення і рішень в області комп'ютерної безпеки для корпоративних і домашніх користувачів.

DDoS-атаки (англ. Distributed Denial of Service) – напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам.

МВС РФ – Міністерство внутрішніх справ Російської Федерації.

ЦНАП – Центр надання адміністративних послуг.

НБУ – Національний банк України.

НКЦК – Національний координаційний центр кібербезпеки.

RT – (Russia Today) Росія сьогодні.

ФСБ – Федеральна служба безпеки.

ВСТУП

Актуальність дослідження. Сьогодні у світі дослідженню проблем боротьби з кіберзлочинністю приділяється значна увага, що обумовлено об'єктивними процесами розвитку інформаційно-телекомунікаційних технологій.

За останні роки, кіберпростір усе більше розглядається державами світу як один з найважливіших безпекових пріоритетів, оскільки захист інформації стає визначальним чинником розвитку економіки, соціального, військового та інших секторів.

Кіберзлочинність стала одним із п’яти найпоширеніших економічних злочинів в Україні. Нині боротьба з кіберзлочинністю є однією з найбільш актуальних проблем у світі. Постійне вдосконалення інформаційних технологій є одним із факторів появи нових можливостей для вчинення таких злочинів. Після чого вони створюють загрозу для глобальних інформаційних мереж і суспільства загалом.

Варто зазначити, що актуальність даного дослідження зумовлена необхідністю подолати суперечності між наявним станом швидкого зростання важливості кібербезпекової проблематики в Україні на час військового стану.

Вдосконалення законодавства, яке регламентує сферу боротьби з кіберзлочинністю, та організаційно-правовий статус суб’єктів, які протидіють цьому негативному та руйнівному явищу, є досить актуальним. Впровадження ефективного механізму правового регулювання протидії правопорушенням у кіберпросторі - це пріоритетне та першочергове завдання України.

Актуальність дослідження зумовлена тим, що з кожним роком все більш поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення персональних даних, незаконних фінансових операцій, крадіжок і шахрайства в мережі Інтернет. Кіберзлочинність здатна завдати значної шкоди інтересам особи, суспільства і держави.

Провівши аналіз наукових праць вітчизняних науковців щодо досліджень кіберзлочинності та сучасного стану законодавства України по боротьбі з кібератаками, можна сказати про те, що ми знаходимось лише на початковому етапі вивчення даного питання.

Стан наукової розробки теми. За оцінками експертів, десятки тисяч злочинів із використанням інформаційних технологій, програмного забезпечення, апаратного та спеціального технологічного обладнання здійснюється в Україні щорічно. В даний час ці проблеми ускладнюються тим фактом, що відсутня всеосяжна система управління загальнодержавної кібербезпеки в Україні [1,7].

Проаналізувавши існуючі визначення кіберпростору, науковець О.В. Манжай дійшов висновку, що кіберпростір ідентифікується з певним єдиним простором – це інформаційне середовище, яке виникає за допомогою технічних систем під час взаємодії людей між собою, взаємодії технічних систем та управління людьми цими технічними (комп'ютерними) системами [27, с.215-219]

Проте Кравцова М. О. дає більш розширене поняття і зазначає, що під кіберзлочинністю слід розуміти соціально-правовий феномен, що проявляється в забороненій законом про кримінальну відповідальність предметній діяльності (кримінальній активності) частини населення з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку [20, с.14].

Проблему кіберзлочинності в Україні розглядали багато дослідників, зокрема особливу увагу кібертероризму та кібербезпеці розглядали В.К.Харченко, О.М.Климчук, О.Г.Корченко, Ю.П.Травніков; організаційно-правові засади організації систем захисту критичної інфраструктури від кібератак вивчають І.О.Чернухін, О.Д.Довгань, В.М.Богуш.

Деякі аспекти нормативної бази по боротьбі з кіберзлочинності вивчали та обговорювали в своїх публікаціях К. Бєляков, В. Бутузов, А. Волеводз,Д. Гавловський, В. Голубєв, В. Гуславський Д. С. Кльоцкін, М. Литвинов, Е. Рижков, В. Розовський Т. Тропина, В. Цимбалюк, О. Юхно та інші.

Предметом роботи є специфіка впливу кіберзлочинів на державну інформаційну політику з точки зору оцінки наявних небезпек і загроз.

Мета роботи полягає в аналізі особливостей атак на державні інформаційні ресурси до та на початку повномасштабного вторгнення Росії в Україну, розробка практичних рекомендацій.

Завдання:

- ✓ дослідити кіберзлочинність як явище та його передумови виникнення, розвиток;
- ✓ виокремити особливості комп'ютерних злочинів;
- ✓ вивчити світовий та вітчизняний досвід державної політики у протидії кіберзлочинності;
- ✓ визначити ключові аспекти розвитку інформаційної політики України;
- ✓ охарактеризувати інформаційну політику в Україні та її нормативно-правове регулювання;
- ✓ охарактеризувати особливості атак на державні інформаційні ресурси до та на початку повномасштабного вторгнення Росії в Україну;
- ✓ дослідити стан державної інформаційної політики до та після повномасштабного вторгнення Росії в Україну;
- ✓ надати практичні рекомендації щодо моделі попередження кіберзлочинності;

Хронологічні рамки: у кваліфікаційній роботі розглядається період з 2019 по 2022 роки, де нижньою межею є створення Міністерства цифрової трансформації України 2 вересня 2019 шляхом перетворення Державного агентства з питань електронного урядування України, а верхньою межею є Російське вторгнення в Україну 2022 року.

Методологія і методика дослідження. Методологічна база дослідження зумовлена поставленою метою і особливостями його предмету. Зміст поставлених завдань визначив необхідність застосування таких методів, як порівняльно-правовий, порівняльно-історичний та метод системного аналізу, а також метод описової статистики. Це дасть нам можливість дослідити стан державної інформаційної політики до та після повномасштабного вторгнення Росії на територію України.

Аналіз джерельної бази: в основу наукової роботи покладено велику кількість матеріалів, що стосуються кіберзлочинності та кіберзахисту держави. Зокрема, нами були проаналізовані такі нормативно-правові документи: Закон України "Про основні засади забезпечення кібербезпеки України", 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",Закон України «Про Державну службу спеціального зв'язку та захисту інформації України», Закон України «Про телекомунікації», Стратегія кібербезпеки України (2021 – 2025 роки). До того ж у роботі розглядаються матеріали різних експертів щодо інформаційної політики в Україні та її нормативно-правового регулювання. Джерельна база є досить репрезентативною та сприяє реалізації нашого дослідження. Велика кількість матеріалів українських та міжнародних експертів, звіти аналітичних центрів з забезпечення кібербезпеки, були опрацьовані і використані в роботі, це дозволило розкрити основні досліджувані аспекти теми та дало ґрунтовні відповіді на поставленні питання.

Практичне значення: роботи полягає у тому, що результати дослідження можна використовувати під час розробки навчальних програм; для підготовки фахівців у галузі кібербезпеки. Теоретичні напрацювання автора, висновки та практичні рекомендації можуть бути використані у навчальному процесі для читання курсів у галузі кібербезпеки.

Наукова новизна отриманих результатів та особистий внесок дослідника полягають у тому, що на основі застосування сучасної методики наукового пізнання, використання комплексного міждисциплінарного підходу у вивченні питання кіберзлочинності, розроблено авторське бачення впливу кібератак Російської Федерації на інформаційну політику України. Наукова новизна конкретизується у теоретичних висновках та практичних рекомендаціях попередження кіберзлочинності в Україні.

Структура роботи визначається метою, предметом та завданнями дослідження. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи – 88 сторінок, з них основного матеріалу – 76 сторінок.

РОЗДІЛ 1. КІБЕРЗЛОЧИННІСТЬ - ЯК ЗАГРОЗА ДЕРЖАВНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРУ

1.1. Виникнення та розвиток кіберзлочинності

Кіберзлочинність є об’єктивним наслідком глобалізації інформаційних процесів і появи глобальних комп’ютерних мереж. Зі збільшенням використання інформаційних технологій у різних сферах людської діяльності зростає і їх використання з метою вчинення кримінальних правопорушень [6, с.52].

Концепція «Кіберзлочинність» охоплює весь спектр злочинів у сфері інформаційних технологій, будь то злочини, вчинені за допомогою комп’ютерів, або злочини, предметом яких є комп’ютери, комп’ютерні мережі та інформація, що в них зберігається [65, с.36].

Кіберзлочинність – це злочинність у так званому кіберпросторі. Автори «Модельного закону» Міжнародного союзу електрозв’язку про кіберзлочинність (2009) визначають кіберпростір як «фізичний і фізичний простір, створений та сформований таким чином: комп’ютери, комп’ютерні системи, мережі, їхні комп’ютерні програми, комп’ютерні дані, дані контенту, трафік і користувачі».

Законодавством України визначено поняття кіберпростору як середовища, (віртуального простору), яке надає можливості для здійснення комунікацій або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [67].

Кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння в кіберпросторі або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність або яке визнано злочином міжнародними договорами України [61].

Кіберзлочинність має свою класифікацію та поділяється на види за об’єктом, предметом злочину, видом вчинення тощо. За об’єктом атаки виділяють наступні групи кіберзлочинів: злочини проти конфіденційності, цілісності та доступності комп’ютерних даних і комп’ютерних мереж, комп’ютерні злочини у сфері підприємницької діяльності, комп’ютерні злочини проти особистих прав і недоторканності приватного життя, комп’ютерні злочини проти суспільних і державних інтересів (рис.1.1).

Проте варто зазначити, що багато кіберзлочинів включають посягання на кілька об’єктів одночасно: незаконне перехоплення приватних електронних комунікацій, порушення недоторканності приватного життя та конфіденційності комп’ютерних даних, комп’ютерне шахрайство – власність та цілісність комп’ютерних даних тощо.

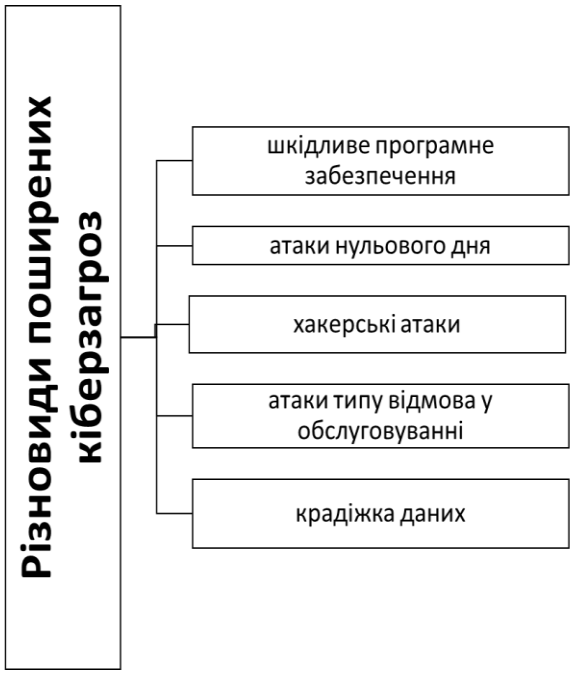


Рис.1.1 Різновиди поширених кіберзагроз

На даний момент найпоширеніша класифікація кіберзлочинності базується на структурі Конвенції Ради Європи про кіберзлочинність, яка спочатку поділяла кіберзлочинність на чотири групи (потім був прийнятий додатковий протокол, а зараз — п’ять груп). Ця класифікація є актуальною як

«стандарт», відповідно міжнародних та регіональних документів, наукової практики.

Класифікація комп’ютерних злочинів складається з п’яти груп;

- до першої групи належать такі злочини проти конфіденційності, цілісності та доступності комп’ютерних даних і систем, як незаконний доступ, незаконне перехоплення, вторгнення в дані, вторгнення в систему;
- до другої групи належать злочини, пов'язані з використнням комп’ютеру як засобу вчинення кримінальних правопорушень – а саме як засобу маніпулювання інформацією. До цієї групи належать комп'ютерне шахрайство та комп'ютерна підробка;
- третю групу складають складові злочини (вміст даних). До цієї групи належать злочини, пов'язані з контентом, тобто вмістом даних, що зберігаються в комп'ютерних мережах.
- до четвертої групи належать правопорушення, пов'язані з порушенням авторських право та суміжних прав;
- п’ята група злочинів обліковується в окремому журналі – це расистські та ксенофобські дії, вчинені через комп’ютерні мережі. Конвенція Ради Європи не виділяє на окремі групи правові акти, які є предметом багатьох дискусій, але все ще є технічно суперечливими [65].

Криміналізація та необхідність гармонізації законодавства на міжнародному рівні сприяла появі нових понять, що стосуються кібербезпеки. Одним із них є так званий «кібертероризм» і використання кіберпростору в терористичних цілях (наприклад, участь у скоєнні терористичних злочинів або інше сприяння їм). Відсутність єдиного визначення тероризму на міжнародному рівні наразі ускладнює дискусію щодо кібертероризму як явища, криміналізація якого необхідна як універсальна для всієї міжнародної спільноти, але це не заважає державам і міжнародним організаціям докладати зусиль для протидії кібертероризму. терористичними організаціями - наприклад, існує проект Clean IT на рівні Європейського Союзу [66].

Ще одна категорія правопорушень, конкретно не включена до Конвенції Ради Європи (і яка набула більшого поширення після прийняття Конвенції), – це викрадення особистих даних, викрадення, передача та використання персональних даних з метою вчинення кримінальних правопорушень. Деякі країни виділяють ці злочини в окрему категорію, інші вважають, що ці діяння підпадають під дію кількох статей кримінального законодавства. Зважаючи на те, що ці злочини набули поширення порівняно недавно, наразі точаться дискусії щодо виділення цього злочину в окрему групу та необхідності гармонізації законодавства у цій сфері на міжнародному рівні [15].

Історію кіберзлочинності можна простежити в історії хакерства. Хакер – це висококваліфікований ІТ-фахівець, людина, яка розбирається в тонкощах комп'ютерів. Є два типи ІТ-хакерів: «білий капелюх» і «чорний капелюх». «Чорний капелюх» відноситься до кіберзлочинців, тоді як «білий капелюх» відноситься до інших фахівців з інформаційної безпеки (включаючи експертів, які працюють у великих ІТ-компаніях) або дослідників ІТ, які не порушують закон [29, с.200-202].

На ранніх етапах розвитку кіберзлочинності термін «злом» використовується дуже часто, хоча пізніший злом визначається як один із злочинів, включених до поняття кіберзлочинності. Саме хакерство характеризує протиправні дії хакерів.

Кіберзлочинність – це не лише техніко-правова, а й соціальна проблема, ефективне вирішення якої потребує, перш за все, системного підходу до вироблення рамкових умов забезпечення безпеки життєво важливих інтересів громадян, суспільства та держави у кіберпросторі.

Через механізми та способи вчинення злочину у сфері обчислювальної техніки вони мають високу затримку. Найбільшу загрозу для населення становлять злочини, пов'язані з незаконним доступом до комп'ютерної інформації.

Проаналізовані злочини мають дуже високу латентність, яка за різними даними становить близько 85-90%. Причому факти виявлення незаконного доступу до інформаційних ресурсів на 90% є випадковими [40, с.55].

Ці дані говорять про те, що правоохоронці часто просто не розуміють, як розслідувати та доводити ці злочини в суді. Через неможливість якісного проведення розслідувань традиційні методи організації та планування розслідувань у цих умовах не працюють. Необхідно підвищити ефективність правоохоронної діяльності, підвищити вимоги до професіоналізму працівників правоохоронних органів, а також до їх морально-ділових якостей. Не слід допускати їх формального ставлення до звітності про результати боротьби з кіберзлочинністю.

Ще одна проблема, з якою найчастіше стикаються слідчі, розслідуючи злочини, пов’язані з комп’ютерними технологіями, – встановлення фактів. Це тому, що комп’ютерні злочини часто здійснюються в так званому «кіберпросторі», вони не знають кордонів, дуже часто злочини вчиняються не виходячи з дому за допомогою персонального комп’ютера. Крім того, незаконне копіювання інформації часто залишається непоміченим, введення вірусу в комп’ютер найчастіше пов'язане з ненавмисною помилкою з боку користувача, який не зміг «зловити» його на контакті із зовнішнім комп’ютерним світом. Ставлення потерпілих до нападів на них також не завжди відповідне. Замість того, щоб інформувати правоохоронні органи про незаконне проникнення в комп’ютерну систему, потерпілі не поспішають робити це, боячись підірвати свою ділову репутацію. Зазвичай жертвами комп’ютерних злочинів стають локальні мережі, сервери та окремі особи [29, с.10].

Слід підкреслити, що професійні комп’ютерні злочинці обирають в якості об’єктів злочинності локальні мережі та сервери великих компаній, «аматори», у свою чергу, проникають в інформацію комп’ютерів окремих осіб, а провайдери рідше «зламують», як правило, безкоштовно.

Також варто зазначити , що потерпілі в особі великих корпорацій, які володіють системою, неохоче (якщо взагалі повідомляють) повідомляють про факти комп'ютерного злочину в правоохоронні органи. А оскільки вони складають більшість, це може пояснити високу латентність кіберзлочинності.

Крім того, чиновники, в обов'язки яких входить забезпечення комп'ютерної безпеки, часто не зацікавлені в розкритті факту злочину. Визнання несанкціонованого доступу до їхньої юрисдикції ставить під сумнів їх професійну кваліфікацію, а недотримання заходів комп'ютерної безпеки керівництвом може спричинити серйозні внутрішні ускладнення.

Як правило, працівники банку ретельно приховують злочини, скоєні проти комп'ютерів банку, оскільки це може зашкодити репутації банку та призвести до втрати клієнтів. Деякі жертви бояться серйозного компетентного розслідування, оскільки воно може виявити непристойні або навіть незаконні механізми бізнесу [40, с.89].

Існує ще одна проблема з ефективністю розслідування та переслідування комп'ютерних злочинів. У суспільстві є думка, що кіберзлочинність не вважається серйозним злочином, тому що навіть після завершення розслідування та винесення вироку кіберзлочинців відпускають з легкими вироками, часто умовними.

Отже – правовий нігілізм, з одного боку злочинці, які відчувають безкарність, а з іншого – жертви, які не хочуть звертатися із запитом про несанкціонований доступ до правоохоронних органів, бо розуміють, що досі не отримують належного покарання для злочинців.

1.2. Проблема кіберзлочинності у контексті трансформації безпекових викликів

Питання кіберзлочинності є надзвичайно актуальним на державному рівні. У більшості випадків кібератакам піддаються об'єкти критичної інфраструктури: енергетичні, транспортні та банківські. Захист від

кіберзлочинів зазвичай коштує в 10 разів дорожче, ніж сама атака. Таким чином, кібербезпека є пріоритетною сферою в багатьох національних політиках.

За даними аналізу, проведеного компанією «FireEye», у країнах Близького Сходу, Європи та Африки від кібератак найбільше страждають урядові веб-сайти, веб-сайти фінансових організацій та сайти операторів зв'язку (див. Додаток А).

Кожна кібератака не проходить непоміченою та має економічні наслідки. Наприклад, влітку 2014 року хакери отримали доступ до даних 83 мільйонів клієнтів одного з найбільших американських банків JPMORGAN CHASE [66].

Метою таких атак є отримання довільних даних з метою продажу їх третім особам. У результаті банки були змушені витрачати кошти на відновлення даних, вдосконалювати сервери, на яких зберігається інформація, реорганізовувати спеціальні відділи для боротьби з кібератаками.

Популярність кіберзлочинності супроводжується високими винагородами. Проте нерідкі випадки, коли кіберзлочинці здійснюють атаки з метою помсти чи відновлення справедливості, а не лише за винагороду. Наприклад, хакерська група «Анонімі» влаштувала масштабну кампанію «Розплата» за підтримку скандального сайту WikiLeaks. Після арешту Джуліана Ассанжа (засновника сайту) у грудні 2010 р. платіжні системи PayPal, MasterCard і Visa заблокували грошові рахунки WikiLeaks, у відповідь «Анонімі» здійснили серію кібератак, в результаті яких сайти сервісу були заблоковані, а системи електронних платежів на деякий час були відключені [66].

Цьогорічний огляд глобальної економічної злочинності підкреслює зростаючу загрозу кіберзлочинності. Сьогодні багато людей і організацій використовують різні технології, в тому числі і Інтернет. Таким чином, вони наражаються на потенційний ризик атак шахраїв з усіх куточків світу. На тлі таких проблем, як викрадення даних і витік інформації, комп'ютерні віруси та

хакерські атаки, наша робота зосереджується на важливості цього виду злочинності і його впливу на організації в усьому світі.

Поширення комп’ютерних вірусів, шахрайство з пластиковими платіжними картками, викрадення коштів з банківських рахунків, викрадення комп’ютерної інформації та порушення правил роботи автоматизованих електронно-обчислювальних систем – це далеко не вичерпний перелік подібних злочинів. Цю категорію злочинів називають по-різному: кіберзлочини, комп’ютерні злочини, злочини, пов’язані з комп’ютерними технологіями, злочини, пов’язані з комп’ютерною інформацією. У літературі найчастіше зустрічаються два терміни: кіберзлочинність і комп’ютерна злочинність. Оскільки вони використовуються для найменування одних і тих же суспільно небезпечних діянь, їх можна вважати синонімами та рівнозначними.

Кожен день комп'ютерні системи піддаються хакерським атакам з негативними наслідками для користувачів. Але найбільшою проблемою є хакерські атаки на комп’ютери великих корпорацій та органів влади. Такі атаки кіберзлочинців несуть загрозу не тільки функціональності компанії чи державної установи, а й економіці країни в цілому [12].

Проблема комп'ютерної злочинності привернула увагу кримінологів провідних зарубіжних країн з моменту широкого впровадження комп'ютерних технологій, що мало низку негативних наслідків і погіршило ситуацію із захистом інформації в комп'ютерних базах даних і комп'ютерних системах. Статистика таких злочинів ведеться з 1958 року. Тоді під ними малися на увазі: випадки пошкодження та крадіжки комп'ютерної техніки; викрадення інформації; шахрайство або крадіжка грошей за допомогою комп'ютера; несанкціоноване використання комп'ютерів [16].

Сьогодні кіберзлочинність в Україні регулюється такими нормативно-правовими актами: Конвенція про кіберзлочинність, Закон України «Про ратифікацію Конвенції про кіберзлочинність», Кримінальний кодекс України,

Закон України «Про основні засади забезпечення кібербезпеки України» [17, 18, 22].

Першою причиною розвитку кіберзлочинності, як і будь-якого іншого бізнесу, є прибутковість. Друга причина зростання кіберзлочинності як бізнесу полягає в тому, що успіх справи не супроводжується великим ризиком. У реальному світі психологічний аспект злочинності передбачає наявність певних засобів стримування. У віртуальному світі злочинці не бачать своїх жертв, незалежно від того, чи є вони окремими особами чи цілими організаціями, на які вони хочуть напасти [13, с.38].

Кожне покоління злочинців має свої інструменти. Однією з програм, яку використовують сучасні кіберзлочинці є троянська. Вони застосовують її як зброю, використовують для створення ботнетів для крадіжки паролів і конфіденційної інформації, запуску DDoS-атак і шифрування даних для шантажу жертв.

Ще одна поширена техніка, яка використовується зі зловмисним програмним забезпеченням, – це переривання роботи антивірусних програм, щоб запобігти виявленню та збереженню шкідливого програмного забезпечення на комп'ютері. Такі дії часто спрямовані на відключення безпеки, видалення коду або зміну файлу хостів Windows, щоб запобігти відновленню антивірусних програм.

Кіберзлочинність – це явище сучасної цифрової епохи. Для сучасних «технарів» це часто ідеальна можливість заробити та реалізуватись. Злочинці не стоять на місці. Їх методи вдосконалюються і стають все більш і більш складними.

Незважаючи на віртуальний характер злочинів, збитки, які вони завдають, цілком реальні. За деякими оцінками, світова економіка щорічно втрачає через кіберзлочинців 114 мільярдів доларів, передає РБК. А США оцінили свої збитки за всі роки існування глобальної мережі в $400 млрд, що втричі перевищує річну вартість освіти [66].

Профілактичні заходи вже не допомагають, з кожним роком збитки зростають, а злочини стають все більш «витонченими». Найпоширенішими із них є злом баз даних компаній і державних організацій. До цього призвела, наприклад, вірусна атака на іранську атомну електростанцію в Бушері. Також широко відомі крадіжки інновацій чи технологій і, нарешті, банальна крадіжка грошей [7].

Водночас у 2017 році відбулося особливо суттєве зростання кіберзлочинності (порівняно з 2013 роком більш ніж у чотири рази), що свідчить про наявність специфічних ознак досліджуваного виду злочинів, пов’язаних із низкою факторів, що його визначають, як от:

- швидкий розвиток процесу інформатизації суспільства (впровадження мережі мобільного зв'язку третього покоління (4G);
- розвиток кібертехнологій як засобу злочинної діяльності;
- об’єктивна затримка технічної складової правоохоронної системи тощо.

Статистичний аналіз географічного поширення кіберзлочинності в Україні за останні роки показав залежність від фактора урбанізації. Найвищий рівень активності кіберзлочинності за рангом зафіксований у Дніпропетровській, Київській, Харківській, Запорізькій та Черкаській областях; найнижчий – у Чернівцях, Херсоні, Сумах та Кіровограді [3].

Відповідні географічні особливості кіберзлочинності в Україні не варто розглядати стільки через призму домінування кіберзлочинності у східних регіонах порівняно із заходом (що традиційно пояснюється низкою факторів, наприклад, щільністю населення на сході нашої країни), оскільки розглядати його через призму домінування промислово та економічно розвинутих районів (центрів).

Це технічний (а відповідно і фінансовий) розвиток, який неможливий без використання сучасних, переважно інформаційних технологій, середовищем яких є середовище кіберзлочинності. Таким чином, аналіз «географічних» особливостей окремих видів кіберзлочинності дозволив з’ясувати такі ознаки.

На думку деяких авторів, сферою кіберзлочинності є так званий віртуальний простір, який можна визначити як інформаційний простір за допомогою комп'ютерного моделювання, який містить дані про людей, об'єкти, факти, події, явища та процеси, подані математичній, символьній чи в будь-якій іншій формі, і переміщується через локальні та глобальні комп'ютерні мережі.

1.3. Особливості комп'ютерних злочинів

Сліди кіберзлочинів досліджуються за допомогою комп'ютерних та технічних досліджень, а також дослідження відео- та аудіозаписів. Що стосується наукової кваліфікації, то вона повністю залежить від рівня професійної підготовки фахівців, і близько 3% з них мають наукові ступені.

При безпосередньому доступі до комп'ютерної інформації приховування слідів кримінального правопорушення зводиться до відтворення обстановки, що передувала його вчиненню, тобто знищення залишених слідів (наприклад, слідів пальців рук на клавіатурі, кнопках дисководів та інших поверхнях, яких торкався злочинець; слідів взуття; мікрочастинок та ін.) [4].

При опосередкованому (віддаленому) доступі приховування полягає в самому способі вчинення злочину, що ускладнює виявлення неправомірного доступу. Так, використання універсальних програм, призначених для застосування в аварійних ситуаціях дозволяє не тільки здійснити несанкціонований доступ до комп'ютера, минаючи всі засоби захисту і контролю, а й довільно змінювати будь-які атрибути файлів, не залишаючи при цьому ніяких слідів (робота цих програм не протоколюється).

Нижче описано список різних типів комп'ютерних злочинів які є актуальними сьогодні, а саме:

- дитяча порнографія – виготовлення, розповсюдження, зберігання або перегляд дитячої порнографії;
- шахрайство з кліками – шахрайські клацання по рекламі в інтернеті;

- порушення авторських прав – викрадення або використання захищеного авторським правом матеріалу іншої особи без дозволу;
- злом – злам або розшифровка кодів, призначених для захисту даних;
- кібертероризм – хакерство, погрози та шантаж щодо компанії чи особи;
- кіберзалякування або кіберпереслідування – переслідування в інтернеті;
- кіберсквотінг – створення домену іншої особи чи компанії з єдиним наміром продати його їм пізніше за вищою ціною;
- створення зловмисного програмного забезпечення – написання, створення або розповсюдження шкідливого програмного забезпечення (наприклад, вірусів і шпигунського пз);
- data doddling – комп'ютерне шахрайство, пов'язане з навмисною фальсифікацією чисел під час введення даних;
- атака на відмову в обслуговуванні – перевантаження системи такою кількістю запитів, що вона не може обслуговувати звичайні запити;
- крадіжка даних – викрадення чужої особистої чи конфіденційної інформації;
- doxing – розголошення особистої інформації іншої особи без її дозволу;
- шпигунство – шпигунство за особою чи бізнесом;
- підробка – продукти чи послуги, які не є справжніми або підробленими. наприклад, фейковий антивірус і фейкова техпідтримка;
- шахрайство – маніпулювання даними, наприклад зміна банківських записів для переказу грошей на рахунок або участь у шахрайстві з кредитними картками;
- зелене графіті – тип графіті, у якому використовуються проектори або лазери для проектування зображення чи повідомлення загрозливого характеру на будівлю;
- збирання врожаю – зловмисник збирає облікові записи або пов'язану з ними інформацію про інших людей;

- торгівля людьми – участь у незаконному акті купівлі або продажу інших людей;
- крадіжка особистих даних – прикидатися кимось, ким ви не є;
- незаконний продаж – купівля або продаж незаконних товарів в інтернеті, зокрема наркотиків, зброї та психотропних речовин;
- крадіжка інтелектуальної власності – викрадення практичної чи концептуальної інформації, розробленої іншою особою чи компанією;
- порушення прав інтелектуальної власності – порушення прав інтелектуальної власності – це будь-яке порушення авторських прав, патентів або торгових марок іншої особи;
- фішинг або вішинг – обман осіб з метою отримання приватної або особистої інформації про цю особу;
- програми- вимагачі – зараження комп'ютера або мережі програмами-вимагачами, які утримують дані в заручниках до сплати викупу;
- шахрайство – змусити людей повірити в щось, що не відповідає дійсності;
- наклеп – публікація наклепу чи наклепу на іншу особу чи компанію;
- піратство програмного забезпечення – копіювання, розповсюдження або використання програмного забезпечення, не придбаного користувачем програмного забезпечення;
- розсилка спаму – розсилання небажаних електронних листів на десятки чи сотні різних адрес;
- спуфінг — обман системи, яка змушує її вважати вас кимось, ким ви не є;
- крадіжка — крадіжка або захоплення будь-чого (наприклад, обладнання, програмного забезпечення або інформації), що вам не належить;
- неавторизований доступ – отримання доступу до систем, на доступ до яких ви не маєте дозволу;
- вандалізм – пошкодження будь-якого обладнання, програмного забезпечення, веб-сайту чи інших об'єктів;

- прослуховування – підключення пристрою до телефонної лінії для прослуховування розмов [16, с.52].

Кіберзлочинність включає незаконну діяльність, яка здійснюється на комп’ютерах. Традиційні злочини можна вчинити під час використання комп’ютера, але кіберзлочинність включає більш специфічні види злочинів, такі як фішингові схеми та віруси.

Кіберзлочинці атакують такі популярні персональні пристрої, як мобільні телефони, щоб поширювати загрози та проникати в економічні сектори

Здійснивши аналіз літератури, можна виділити такі основні характеристики кіберзлочинності:

- вчинення протиправних дій з використанням комп’ютера, його систем або програм;
- протиправні дії, у яких комп’ютер є або інструментом, або мішенню, або тим і іншим;
- злочини, скоєні в комп'ютерному середовищі;
- питання юрисдикції;
- переважно ненасильницькі злочини;
- завіса анонімності [20, с.43].

Знаряддями вчинення комп’ютерних злочинів виступають засоби комп’ютерної техніки, у тому числі і спеціальне програмне забезпечення. До знарядь безпосереднього доступу можна віднести носії комп’ютерної інформації (лазерні диски, зовнішні жорсткі диски, flech-накопичувачі), різноманітне периферійне устаткування (наприклад, dvd-rom-накопичувачі), а також електронні ключі, особисті ідентифікаційні коди та ін. До знарядь опосередкованого (віддаленого) доступу відноситься насамперед мережеве устаткування, а також засоби доступу до віддалених мереж (засоби телефонного і супутникового зв’язку, модем).

У світі до проблеми боротьби з кіберзлочинністю підходять дуже обережно, а державні органи беруть безпосередню участь у її вирішенні. Адже контролювати кількість інформації, котра щоденно протікає через Інтернет,

просто неможливо. Тому з 2009 року влада США в Пентагоні почала створювати власну кіберармію – Агентство національної безпеки, яке також займається питаннями інформаційної війни. В Євросоюзі є агентство з мережевої та інформаційної безпеки, в НАТО є комітет з кіберзахисту та спільний центр з кіберзахисту [29, с.12].

Під час інформаційних війн зброєю є ЗМІ, соціальні мережі, тролінг, блогосфера. На відміну від зарубіжжя, в Україні немає власних платформ для обміну інформацією (Facebook, Twitter, YouTube, Вконтакте, Одноклассники тощо), в країні також не підтримуються національні електронні програми, ми не виробляємо власні електронні пристрої тощо. Це означає, що ми дуже вразливі під час інформаційної війни, проте слід зауважити, що на сьогодні в Україні діє низка законів та нормативних документів різних рівнів, що охоплюють питання кібербезпеки держави. Це, зокрема, Закони України «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки України», Указ Президента України «Про Національний координаційний центр кібербезпеки» та інші нормативно-правові акти. Крім того, у вересні 2016 року Верховна Рада України прийняла у першому читанні Закон України «Про основні засади забезпечення кібербезпеки України». Стратегічними документами у цій сфері є: Стратегія кібербезпеки України, Стратегія національної безпеки України, а також ратифікована Верховною Радою України «Конвенція про кіберзлочинність» [35, 45, 48, 49].

Окрім того, щоб бути готовою до забезпечення кібербезпеки та відсічі відкритої агресії в кіберпросторі, Україна прийняла низку заходів щодо вирішення стратегічних, правових, політичних, технічних та організаційних питань, пов’язаних із безпечним функціонуванням кіберпростору (рис.1.2).

Рис.1.2 Комплекс реалізованих заходів безпечного функціонування кіберпростору станом на 2019 рік

Чинний Кримінальний кодекс України встановлює (відповідно до розділу XVI) відповідальність за «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Всі міжнародні організації відзначають необхідність скоординованої міждержавної взаємодії при розслідуванні кіберзлочинів. Саме завдяки роботі таких міжнародних організацій, як Організація економічного співробітництва і розвитку, Інтерпол, Група Восьми, Рада Європи, ООН розвивається міжнародна співпраця країн у сфері боротьби з кіберзлочинністю, формується міжнародне законодавство [22]

Висновки до розділу 1

Таким чином, кіберзлочини - це протиправні дії, вчинені за допомогою комунікаційних мереж та інформаційних систем або проти цих систем та мереж. Зі збільшенням використання інформаційних технологій у різних сферах людської діяльності зростає і їх використання з метою вчинення кримінальних правопорушень. Оскільки кіберзлочинність становить загрозу не лише окремій країні, а й міжнародній безпеці загалом, необхідні спільні дії світової спільноти для боротьби з цією загрозою.

Кілька міжнародних документів стверджують, що сьогодні кіберзлочинність загрожує не лише національній безпеці окремих держав, а й безпеці людства та міжнародного порядку. Стурбованість міжнародної спільноти розвитком кіберзлочинності особливо відображена в таких міжурядових угодах, як Бангкокська декларація про запобігання злочинності та кримінальне правосуддя (2005), Бухарестська декларація про міжнародне співробітництво в боротьбі з тероризмом, корупцією та транснаціональною організованою злочинністю (2006), Всесвітнього саміту з питань інформаційного суспільства та Конвенції Ради Європи про кіберзлочинність (2001). Ці документи стосуються спільної протидії кіберзлодіям шляхом прийняття відповідних нормативно-правових актів.

Сьогодні кіберзлочинність є більш серйозною загрозою для нашої держави, ніж це було 5 років тому. На жаль, незважаючи на зусилля правоохоронних органів у боротьбі з кіберзлочинністю, їх кількість не зменшується, а, навпаки, постійно збільшується.

Основні ознаки, що відрізняють цей вид злочину від інших злочинів: висока ймовірність приховування, труднощі розслідування через обмеженість інформації, неможливість уніфікації національного законодавства та підходів до розслідування у цій сфері, труднощі зі збором даних тощо. Крім того, нами було відзначено тенденцію до посилення впливу такого аспекту, як транскордонний характер цих злочинів.

Кіберзлочинність стала великою проблемою в усьому світі. Правоохоронні органи працюють над боротьбою з цим, законодавці приймають нові закони, а поліцейські органи формують спеціалізовані підрозділи для боротьби з кіберзлочинністю. Для успішної боротьби з кіберзлочинністю необхідно залучати ІТ-фахівців та активних членів суспільства, які постраждали від злочинної діяльності та знайти сприятливе середовище (віртуальний простір) для подальшого їх запобігання.

До країн, які найбільше постраждали від кіберзлочинності здебільшого належать країни Північної Америки, зокрема США, Канада та Європейський Союз. Така географія поширення безпосередньо пов'язана з рівнем технологічного розвитку держави та інтенсивністю використання інформаційних систем у бізнес-структурах, державних установах та в приватному житті громадян цих країн.

«Політична кіберзлочинність» визначається як злочини, вчинені з політичних мотивів, протиправні дії, спрямовані на технічні засоби та інформаційні системи органів влади та ЗМІ з метою підірвати, послабити або змінити існуючі політичний режим, державні інститути чи політичні процеси.

РОЗДІЛ 2. ДІЇ СВІТОВОЇ ПОЛІТИКИ ПРОТИ КІБЕРЗЛОЧИННОСТІ

2.1 Державна інформаційна політика в сфері національної кібербезпеки і кібероборони та її нормативно - правове регулювання

Нові інформаційні технології, засновані на широкому застосуванні комп’ютерної техніки та найсучасніших засобів зв’язку, стали невід’ємною частиною сучасного світу. У наш час комп’ютери впроваджуються в різні сфери людської діяльності. Усі ключові риси сучасного суспільства так чи інакше пов'язані з комп'ютерами, комп'ютерними мережами та комп'ютерною інформацією.

Останнім часом кількість користувачів Інтернету в Україні значно зросла, оскільки підключення до глобальної мережі стало доступним і зручним. Сьогодні персональний комп'ютер, КПК, мобільний телефон з підключенням до Інтернету є звичайним і необхідним. Популярність Інтернету не випадкова, адже він забезпечує цілодобовий доступ до величезної кількості інформації, швидку передачу даних, можливість проводити банківські, торгові, біржові операції, грошові перекази та багато іншого. Інтернет – чудовий інструмент для спілкування та передачі інформації.

Кіберзлочинність – це галузь, що розвивається. Потенційні щорічні збитки світової економіки від кіберзлочинності становлять понад 400 мільярдів доларів. Консервативна оцінка становитиме 375 мільярдів доларів, а максимальна – 575 мільярдів доларів. Навіть найменша з цих цифр перевищує національний дохід більшості країн, і уряди та підприємства недооцінюють рівень ризику, з яким вони стикаються через кіберзлочинність, і те, наскільки швидко цей ризик може зростати [1, с. 32-34].

Однією із глобальних тенденцій розвитку світового співтовариства є зростання значення інформації та знань. Інформація є однією з основних

потреб людини та основою будь-якої соціальної організації. Сьогодні це основний ресурс для досягнення цілей соціально-економічного розвитку країни в цілому, включаючи державне управління, підприємництво, охорону здоров'я, освіту, доступне житло, розвиток сільського господарства, захист навколишнього середовища та запобігання стихійним лихам, успішну протидію екстремізму і тероризму.

Україна, як частина світової цивілізації, знаходиться на шляху до інформаційного суспільства, яке надасть необхідні можливості для створення та використання інформації та знань, розширення людського спілкування та призведе до формування нової інформаційно-інноваційної економіки – найважливішого фактору сталого добробуту.

Водночас процеси глобалізації інформаційних ринків, недоступність усієї необхідної інформації, особливо в Інтернеті, для більшості громадян України, монополія на внутрішніх ринках інформаційних послуг, обмеженість неякісних ЗМІ, порушення авторських прав та проблеми з інформаційною безпекою вимагають, щоб державні розробки та реалізації державної інформаційної політики приділяли більше уваги. Враховуючи перехідний характер процесів соціально-економічного розвитку в країні, успішне вирішення цих проблем можливе лише за участю держави. Вона повинна визначити свої пріоритети та діяльність в інформаційній сфері [2].

Необхідність розробки стратегії державної інформаційної політики також визначається необхідністю координації зусиль уряду, приватного сектору та громадянського суспільства, усіх учасників інформаційної діяльності з метою створення умов для розвитку інформаційного суспільства та покращення якості інформації. Підвищення ефективності інформаційної діяльності на основі відповідної державної політики може стати потужним двигуном підвищення конкурентоспроможності української економіки,

створення нових робочих місць і, головне, підвищення якості життя всіх громадян.

Особливими умовами реалізації інформаційної політики вважаються лише ті соціальні явища та процеси, які призводять до радикальних змін у системі суспільно-політичних відносин у суспільстві, що в свою чергу вимагають змін у державній інформаційній політиці на концептуальному рівні. Поява таких умов породжує нову галузь державної інформаційної політики – інформаційну політику за особливих умов, метою якої є розробка шляхом неминучих проб і помилок правових механізмів та інструментів правового регулювання, які дозволяють ефективно адаптувати суспільно-політичні відносини до нових зовнішніх умов, при цьому темпи та якість їх розвитку будуть знижені.

До особливих умов реалізації інформаційної політики в сучасному суспільстві належать:

- виникнення інформаційного суспільства;
- політична, соціальна, культурна, інформаційна, психологічна глобалізація;
- геополітична конкуренція в інформаційно-психологічному просторі;
- інформаційно-психологічна війна [46, с.53].

Процесом формування інформаційного суспільства як особливої умови реалізації державної інформаційної політики є диспропорція між темпами організаційно-регулюючої діяльності органів влади щодо модернізації публічної інформаційної політики змін у системі суспільно-політичних відносин в інформаційному суспільстві.

Політичну, соціальну, культурну, інформаційну, психологічну глобалізацію можна віднести до категорії особливих умов реалізації державної інформаційної політики (див.рис.2.1)

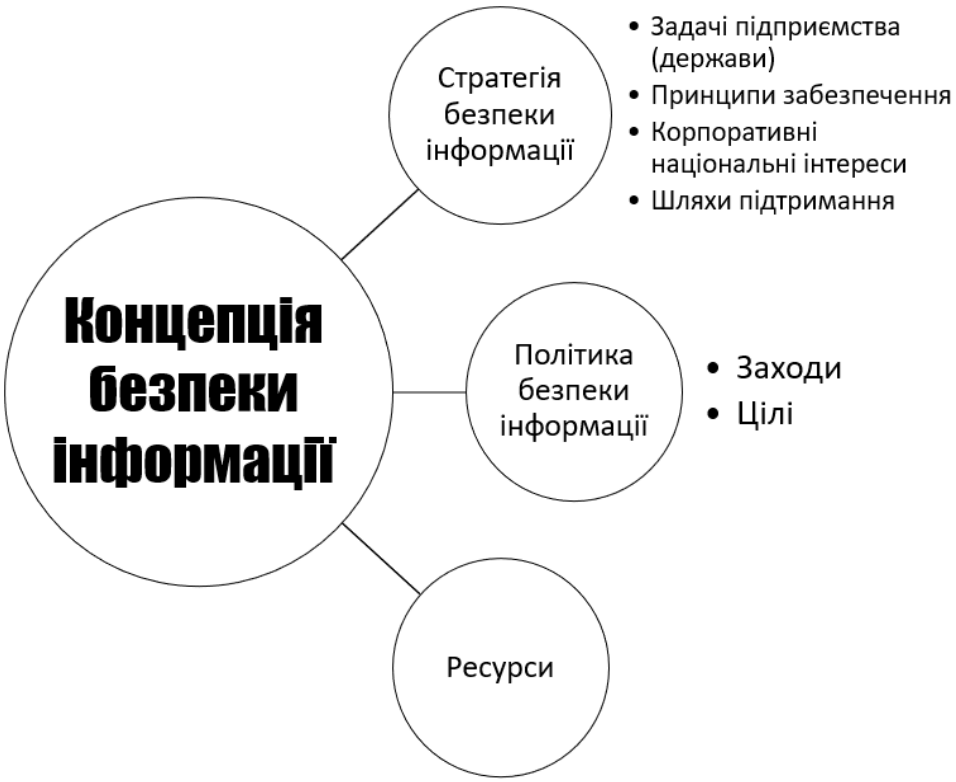


Рис.2.1. Концепція безпеки інформації

В умовах відставання від провідних країн світу в темпах розвитку національного сегмента інформаційно-психологічного простору, виробництва знань і генерації високих технологій держава стає інформаційно залежною від країн-виробників інформаційних ресурсів і стає об'єктом інформаційного неоколоніалізму [26, с.21].

Геополітичну конкуренцію в інформаційно-психологічному просторі віднесено до категорії особливих умов для реалізації державної інформаційної політики з таких причин:

- геополітична конкуренція в інформаційно-психологічному просторі пов’язана з появою нових принципів, пріоритетів і форм політичної боротьби, які не охоплені і практично не врегульовані діючими нормами міжнародного та національного права;
- закритість характеру інформаційно-психологічних процесів ускладнює інформаційне право регулювання цієї категорії суспільних відносин;

- відсутність міжнародного законодавства, що регулює зростання геополітичних суб'єктів в інформаційно-психологічному просторі, а головне, правових норм і механізмів, що гальмують або перешкоджають утворенню геополітичних утворень, призначених спеціально для агресії проти інших держав, є причиною високої гнучкості та швидкості формування, більшість з яких носять віртуальний характер і не вивчаються чинною інформаційною політикою як предмет правового регулювання;

- широке використання арсеналу сил, засобів і методів інформаційно-психологічної війни в мирний час у політичних цілях пов'язано насамперед з відсутністю правових механізмів, що обмежують безконтрольне використання цих сил і засобів [29, с.53].

Держава відіграє ключову роль у формуванні інформаційного суспільства: вона має стати не лише каталізатором змін, а й координатором зусиль різних авторів, механізмом подолання протиріч бізнесу та соціальних інститутів, законодавцем, здатним створити конкурентні умови в інформаційній індустрії, балансом між конкуренцією та регулюванням для створення правової основи інформаційного суспільства [30, с.81-83].

Структурно-функціональна модель інформаційної політики включає кілька взаємопов'язаних елементів, найважливішим з яких є ідеологічна одиниця (або місія) організації, що виступає змістовою основою для здійснення будь-якої інформаційної діяльності. Даний блок, розроблений на стратегічному рівні управління, супроводжується налаштуванням та визначенням конкретних завдань для різних цільових груп, які є суб’єктом інформаційного впливу.

Наступні блоки описують особливості діяльності, спрямованої на формування та поширення цих цінностей (характеристик іміджу) серед різних цільових груп. При цьому можна призначити окремі функції, необхідні для реалізації інформаційної політики. До них належать «Планування», «Обмін повідомленнями», «Поширення», «Аналіз ефективності», «Координація та контроль».

Цей аналіз дозволяє говорити про завдання, які може вирішити держава, що керує своєю інформаційною політикою:

- завдання управління операціями;
- підтримання соціально-економічної та політичної стабільності;
- забезпечення ефективності управлінських рішень;
- залучати інвестиції [43, с. 111].

Розумними пріоритетами інформаційної політики повинні бути механізми та технології створення багатосторонньої (партисипативної) комунікації, результатом якої може бути справедлива і рівноправна взаємодія всіх учасників комунікаційного процесу. Інакше замість такої комунікації відбувається нерівноправна інформаційна взаємодія держави, суспільства та ЗМІ. Це створює інформаційний простір, в якому інтереси одних інстанцій посилюються, а інших послаблюються і навіть ігноруються.

Інформація, що виробляється та поширюється, має бути розрахована на різні групи та прошарки суспільства. Повинні існувати різноманітні думки та тлумачення, які підлягають законодавчим обмеженням щодо поширення певних видів інформації. Все це також є необхідною запорукою успішного розвитку громадянського суспільства, саме тому забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України, особливо в умовах військової агресії Російської Федерації. Його реалізація здійснюється завдяки посиленню спроможностей національної системи кібербезпеки протидії кіберзагрозам та кіберзлочинності у сучасному безпековому середовищі [9].

Фахівці наголошують, що питома вага кіберзагроз зростає, ця тенденція у найближчому десятилітті буде лише посилюватися, адже з розвитком інформаційних технологій та їхньої конвергенції з технологіями штучного інтелекту відбувається вплив на функціонування структур управління як на національному, так і транснаціональному рівнях, що формує нову безпекову ситуацію [21].

Аналізуючи процеси російсько-української війни – кіберпростір разом з іншими фізичними просторами є одним із театрів воєнних дій. Уже стало реальністю функціонування кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й здійснення превентивних ударів у кіберпросторі, що передбачає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних мереж, що ними управляють.

Україна вживає рішучих заходів щодо протидії кіберзагрозам і удосконаленню національної системи кібернетичної безпеки. Зокрема, у жовтні 2017 р. було прийнято Закон України «Про основні засади забезпечення кібербезпеки України», яким на законодавчому рівні визначено об'єкти кібербезпеки та кіберзахисту, критична інфраструктура, цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження суб'єктів їхнього забезпечення та засади координації діяльності [20, с.12-15].

У червні 2018 р. підписано Закон України «Про національну безпеку України», який визначає основи та принципи національної безпеки і оборони, цілі та основні засади державної політики, що гарантують суспільству загалом і кожному громадянину зокрема захист держави від загроз [56].

Затвердження у 2016 р. Стратегії кібербезпеки України стало важливим кроком у запровадженні підходів довгострокового планування у цій надважливій сфері. За роки реалізації Стратегії було докладено багато зусиль щодо становлення та розбудови національної системи кібербезпеки.

У березні 2019 р. Указом Президента України було прийнято Концепцію боротьби з тероризмом в Україні, якою визначено мету, завдання, основні принципи та напрями вдосконалення загальнодержавної системи боротьби з тероризмом з огляду на терористичні загрози національній безпеці України та зроблено прогноз їх розвитку [52].

У вересні 2020 р. Президентом України підписано Указ «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 р. «Про Стратегію національної безпеки України» [52]. Цим документом визначено

пріоритети національних інтересів, зокрема: відстоювання незалежності й державного суверенітету, відновлення територіальної цілісності у межах міжнародно визнаного державного кордону Інформація, комунікація та управління знаннями в глобалізованому світі 31 України, суспільний розвиток, насамперед людського капіталу, захист прав, свобод та законних інтересів громадян України, європейська та євроатлантична інтеграція.

У серпні 2021 р. Указом Президента України було введено у дію Стратегію кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни», в якому зазначено, що забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України [58]. Реалізація цього пріоритету здійснюється шляхом посилення спроможностей національної системи кібербезпеки задля протидії кіберзагрозам у сучасному безпековому середовищі.

Підготовка фахівців із вищою освітою для сфери кіберзахисту розпочата в Україні з 2007 р., коли Постановою Кабінету Міністрів України було затверджено галузь знань 1701 «Інформаційна безпека» та бакалаврські напрями підготовки «Безпека інформаційних і комунікаційних систем», «Системи технічного захисту інформації», «Управління інформаційною безпекою» [53].

У 2010 р. у межах зазначеної галузі й бакалаврських напрямів було введено спеціальності «Безпека інформаційних і комунікаційних систем», «Безпека державних інформаційних ресурсів», «Системи технічного захисту інформації», «Управління інформаційною безпекою», «Адміністративний менеджмент у сфері захисту інформації». За цей час було розроблено і введено у дію всі галузеві стандарти, близько 40 закладів вищої освіти розпочали підготовку кваліфікованих кадрів із зазначених спеціальностей.

Робочою групою консорціуму «Партнерство заради миру» було підготовлено типовий навчальний план з кібербезпеки. Підготовка фахівців за цією спеціальністю має відбуватися у тісній співпраці академічного середовища та компаній роботодавців.

Базуючись на наведених результатах, можна сформулювати основні компетентності у сфері підготовки фахівців для національної системи кібербезпеки (див.рис.2.2):

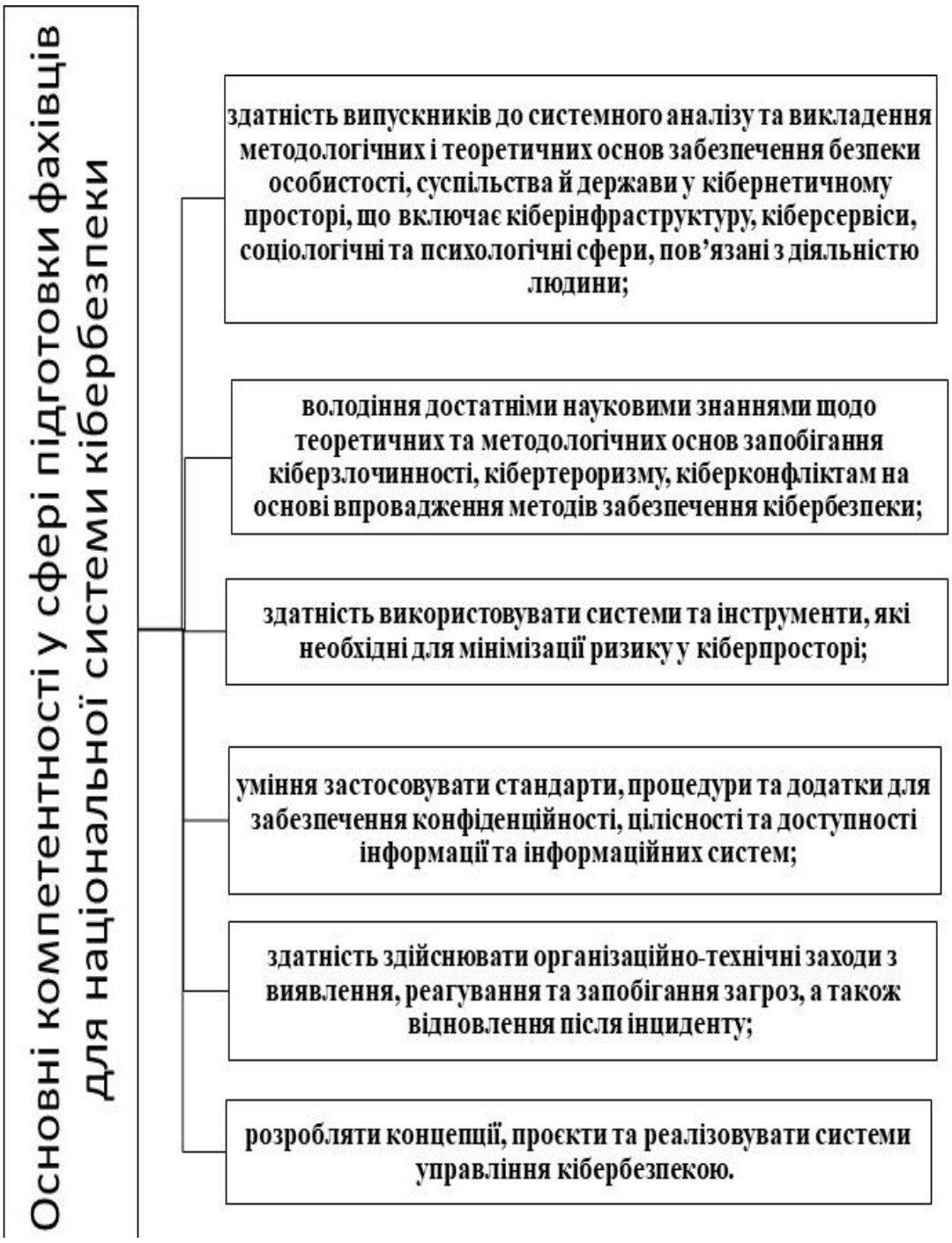


Рис. 2.2 Основні компетентності у сфері підготовки фахівців для національної системи кібербезпеки

Світовий досвід підтверджує необхідність комплексного системного підходу для забезпечення успіху в цій сфері. У 2017 р. Національне агентство із забезпечення якості вищої освіти погодило стандарт вищої освіти стосовно кібербезпеки, в якому чітко виписано вимоги до навчального процесу та отримані знання студентів за цією спеціальністю після закінчення бакалаврату. Таким чином, було здійснено заміну галузі «Інформаційна безпека» однією спеціальністю «Кібербезпека» [42, с.4-8].

Отже, нові виклики, які несе з собою перехід на 5G-мережі, функціонування яких кардинально залежить від коректної роботи програмного забезпечення, а впровадження нової технології матиме нові непередбачувані загрози; пандемія COVID-19 матиме доволі довготривалий вплив на світовий порядок, посилюючи роль електронних комунікацій у всіх сферах життєдіяльності суспільства, що підвищує ступінь вразливості процесів обробки інформації, зокрема персональних даних; післявоєнна відбудова України потребуватиме великої кількості фахівців найвищого ґатунку у сфері захисту інформації та усунення кіберзагроз. Це вимагатиме належного рівня їхньої підготовки у майбутньому задля розбудови незалежної і процвітаючої держави.

2.2 Світовий досвід боротьби із комп'ютерною злочинністю (на прикладі ЄС, НАТО та Інтерполу)

Кожна держава постійно балансує між принципами поваги до прав і свобод людини і громадянина, інтеграцією в міжнародне співтовариство, необхідністю забезпечення економічного зростання та національної безпеки, включаючи обмеження прав і свобод людини і громадянина, встановлення адміністративних форм обмеження бізнесу, захист власних інтересів на міжнародному рівні.

Вибір робиться як населенням, так і владою, але в переліку сфер жодні внутрішні причини не повинні переважати потребу міжнародної співпраці в

боротьбі зі злочинністю, заснованої на принципах відкритості, взаємної підтримки та активності в розвитку. Міжнародне співробітництво в боротьбі з кіберзлочинністю має базуватися на участі всіх країн, що визначається характером самої інформації, як предметом втручання, так і характером скоєних злочинів [36].

Фактично в сучасному світі всі сфери життя знаходяться в прямій залежності від роботи комп'ютерних та інформаційних мереж. Проте широке використання комп'ютерних технологій для обробки інформації за допомогою програмного забезпечення, що дозволяє відносно легко модифікувати, копіювати та знищувати інформацію, підвищує вразливість інформаційного простору [23].

Користувачі інформаційних систем без достатніх підстав вірять у відсутність кібератак і використовують інформаційний простір, не підозрюючи про межі та загрози безпеці системи [29, с.48-52].

У сучасному світі інформація є найважливішою частиною суспільства. Перетворення постіндустріального суспільства в інформаційне означає, що інформація стає глобальною і набуває все більшої важливості.

Для окремих людей, для держави та для суспільства в цілому кожен може законно шукати, отримувати, зберігати, використовувати та поширювати інформацію, для її надходження немає меж [43, с.140].

Дуже важливо розуміти глобальний характер проблеми кіберзлочинності. Так, кібератаки вже паралізують у роботі не лише приватні структури, а й державні структури, від таких атак не буде захищена жодна країна світу. Можливими джерелами кіберзагроз вважаються не лише хакери чи їхні групи, а й окремі держави, терористичні та злочинні угруповання. При розробці засобів і методів боротьби з кіберзлочинністю слід враховувати латентність цього виду злочинів. За оцінками експертів, латентність «комп'ютерної злочинності» в США досягає 80%, у Великобританії – 85%, у Німеччині – 75%, в Україні – понад 90% [46, с.96-98].

За даними міжнародної служби кібербезпеки Symantec Security, щороку в світі реєструється близько 556 мільйонів кіберзлочинів на суму понад 100 мільярдів доларів США [35, с.38].

Кіберзлочинність може завдати шкоди як інтересам держави, так і окремих осіб. Безперечно, специфіка функціонування інформаційних систем, особливо Інтернету, вимагає спільних зусиль різних державних і приватних суб'єктів для вирішення питань кібербезпеки [40, с.16].

В даний час провідні країни світу активно розширюють і створюють підрозділи в збройних силах і спецслужбах, покликаних попередити розвиток наступу.

Наприклад, у Сполучених Штатах, поряд з уже функціонуючим Національним центром кібербезпеки, у складі Збройних сил було сформовано Об'єднане кіберкомандування США для координації зусиль усіх структур Пентагону у глобальній війні та забезпечення адекватної підтримки з боку цивільних федеральних органів, а також взаємодії з аналогічними органами в інших країнах [66].

У той же час ці організації є частково підконтрольними органами, оскільки вищим контролюючим органом є Рада національної безпеки [58].

Велика Британія впроваджує програми кіберзброї, які дозволять уряду протистояти зростаючим загрозам з кіберпростору [40].

В Австралії створено Координаційну групу з безпеки електронної пошти (ESCG). Основним завданням цієї групи є створення безпечного та надійного простору електронних операцій як для державного, так і для приватного секторів. Боротьба з кіберзлочинністю здійснюється не лише окремими державами, а й їхніми блоками, зокрема НАТО. Тому важливість цього питання відображена в усіх урядових документах блоку, прийнятих за останні роки. Вперше Стратегічна концепція НАТО включає нове положення про кіберпростір та військову сферу діяльності Альянсу [39].

Тобто державам належить особлива роль у боротьбі з транскордонними злочинами, які становлять значну частину кіберзлочинності, і лише за

наявності злагоджених правоохоронних органів можна зменшити кількість злочинів у цій сфері. Міжнародне співробітництво здійснюється за кількома напрямами і спочатку включає створення нормативно-правових актів і розробку загальних рекомендацій, а також впровадження ефективних моделей організаційного співробітництва між державами.

Слід мати на увазі, що традиційні механізми міжнародного співробітництва, зокрема запити, взаємодопомога та інші інструменти, використовувалися ще в XIX ст. Складність розробки проектів міжнародно-правових актів у цій справі ускладнюється також тим, що існуючі закони досить важко застосовувати під час боротьби з локалізованими атаками у глобальному масштабі, докази яких розрізнені та віртуальні [66, с. 4].

Міжнародне співтовариство розробило низку законів різного рівня, які мають відношення до боротьби з кіберзлочинністю і відіграють особливу роль. При цьому важливо звернути увагу на спроби держав розширити норми глобальних міжнародних договорів для боротьби з кіберзлочинністю або укласти нові договори. Наприклад, оскільки організовані злочинні групи можуть діяти разом із окремими особами у кіберпросторі, можна застосовувати міжнародні договори для боротьби з організованою злочинністю, зокрема Конвенцію ООН проти транснаціональної організованої злочинності від 15 листопада 2000 р. [23].

До цього додається концепція Конвенції ООН про міжнародну інформаційну безпеку, яка була представлена міжнародній спільноті на конференції в Лондоні в листопаді 2011 року і містить преамбулу, 23 статті, згруповані в основній частині та заключні положення. Основна частина документа складається з п’яти розділів, зміст яких складається в єдиній композиційній одиниці.

Важливо, що в ст.4 Конвенції визначено основні загрози міжнародному миру та безпеці в інформаційному просторі, з яких визначено 11 основних і 4 додаткові. До основних належать, наприклад, використання інформаційних технологій та засобів для актів ворожості та актів агресії; цілеспрямований

деструктивний вплив на критичні структури іншої держави в інформаційному просторі; транскордонне поширення інформації, що суперечить принципам і нормам міжнародного права та національним законам держав [18].

Водночас, ще раз зазначимо, що концепція Конвенції не деталізує принципи міжнародного співробітництва у боротьбі з кіберзлочинністю, за винятком цілеспрямованої боротьби з тероризмом.

Включення розділу 5 до концепції Конвенції слід оцінити позитивно. До них відносять: обмін національними концепціями інформаційної безпеки та оперативний обмін інформацією про кризові події та загрози в інформаційному просторі, заходи щодо їх вирішення та нейтралізації, консультації щодо діяльності в інформаційному просторі, яка може викликати занепокоєння держав-учасниць, співробітництво у вирішенні військових конфліктів. Однак ці форми не враховують потреби в оперативному співробітництві правоохоронних органів з різних питань.

Слід зазначити, що більшість спеціалізованих нормативно-правових актів щодо боротьби з кіберзлочинністю є нормативно-правовими актами Європейського Союзу, який має одну з найрозвиненіших систем інформаційної безпеки у світі. У 2001 році Європейська комісія представила спеціальне повідомлення «На шляху до безпечнішого інформаційного суспільства шляхом підвищення безпеки інформаційної інфраструктури та боротьби з кіберзлочинністю».

Програми Інтерполу побудовані на підготовці операцій з боротьби з комп’ютерними загрозами, що виникають. Вони спрямовані на:

- сприяння обміну інформацією між державами-членами через регіональні робочі групи та конференції;
- освітні курси до створення і підтримки професійних стандартів;
- координація та сприяння здійсненню міжнародних операцій;
- створення глобального списку контактів для розслідування кіберзлочинів;

- допомога державам-членам у разі кібератак або розслідувань кіберзлочинів через бази даних;
- розвиток стратегічного партнерства з іншими міжнародними організаціями та організаціями приватного сектору;
- виявлення нових загроз та обмін інформацією з країнами-членами;
- розробка програмного забезпечення, надання доступу до оперативної інформації та документів [16, с.34-35].

Після техніко-економічного обґрунтування, проведеного соціологічною фірмою Rand Corporation (Додаток Б) , Європейська комісія вирішила створити Європейський центр кіберзлочинності (ЕС3) в рамках Європейської поліцейської організації (Європол). Центр має на меті діяти як координатор у боротьбі ЄС із кіберзлочинністю та забезпечити швидшу відповідь на онлайн-злочинність. Він підтримує держав-учасників та установи Європейського Союзу у створенні оперативного та аналітичного потенціалу для досліджень та співпраці з міжнародними партнерами. ЕС-3 офіційно розпочав свою діяльність у січні 2013 року, маючи повноваження працювати в таких сферах кіберзлочинності:

- злочини, вчинені організованими групами з метою конфіскації великих доходів, одержаних злочинним шляхом, наприклад Інтернет-шахрайство;
- злочини, які завдають серйозної шкоди жертві, наприклад, сексуальна експлуатація дітей в Інтернеті;
- злочини, що зачіпають критичну інфраструктуру та інформаційні системи в Європейському Союзі [27, с.15-16].

ЕС-3 має на меті стати координаційним центром у боротьбі ЄС із кіберзлочинністю шляхом створення оперативного та аналітичного потенціалу для досліджень та співпраці з міжнародними партнерами для створення простору, вільного від кіберзлочинності в ЄС. Європейський центр боротьби з кіберзлочинністю базується в Гаазі (Нідерланди), тому ЕС-3 може розширювати існуючу інфраструктуру та мережу правоохоронних органів

Європолу. Програмний комітет ЕС-3 підтримує уряди ЄС у боротьбі з кіберзлочинністю.

Управління наслідками кіберзлочинності та способи її запобігання є дуже популярною темою для державних служб. Сьогодні не всі держави-члени мають необхідне забезпечення, щоб почати ефективну боротьбу з кіберзлочинністю.

Розслідування шахрайства в Інтернеті та інших злочинів регулярно викривають сотні нових жертв злочинів у Європі. Операції такого масштабу не можуть бути успішно завершені лише національною поліцією. Саме тут значну цінність має Європейський центр кіберзлочинності.

Європол – це спільнота експертів у Європі для оперативної підтримки, координації та експертизи у сфері кіберзлочинності. Європейський центр боротьби з кіберзлочинністю пропонує більш широку спільну діяльність у співпраці з державами-членами ЄС та іншими ключовими зацікавленими сторонами; країни, що не входять до ЄС; з міжнародними організаціями; з органами управління та провайдерами інтернет-послуг, з компаніями, що займаються інтернет-безпекою у фінансовому секторі; з академічними експертами; з організаціями громадянського суспільства [30, с.81-83].

Іншими словами, сучасною тенденцією міжнародної боротьби з кіберзлочинністю є розширення сфери співпраці між державами. Реальністю є оперативна співпраця правоохоронних органів у боротьбі з кіберзлочинністю (Інтерпол, Європол, Євроюст), створення та використання єдиної бази даних про кіберзлочинців, скоєних та запланованих кіберзлочинів.

Всі міжнародні організації відзначають необхідність скоординованої міждержавної взаємодії при розслідуванні кіберзлочинів. Саме завдяки роботі таких міжнародних організацій, як Організація економічного співробітництва і розвитку, Інтерпол, Група Восьми, Рада Європи, ООН розвивається міжнародна співпраця країн у сфері боротьби з кіберзлочинністю, формується міжнародне законодавство [34].

Боротьба з кібертероризмом у тій чи іншій країні належить до функціональних обов'язків підрозділів інформаційно-військових сил, яка має на меті проведення наступальних та оборонних операцій в мережі Інтернет. Проблема полягає у тому, що сучасний стан законодавства в більшості країн не відповідає низці вимог

2.3. Основні аспекти інформаційної політики України

Інформаційна безпека – це стан захищеності життєво важливих інтересів особистості, суспільства і держави, за якого зводиться до мінімуму завдання збитків через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації. Це визначення є оптимальним та відображає усі аспекти взаємодії суб’єктів інформаційних відносин [3].

Існує два аспекти трактування інформаційної безпеки у контексті національної безпеки. З одного боку, інформаційну безпеку розглянуто як самостійний елемент національної безпеки будь-якої країни, а з іншого – інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної тощо.

У Законі України «Про інформацію» державна інформаційна політика визначається як низка основних напрямів і методів діяльності держави щодо отримання, використання, поширення та зберігання інформації. Основними напрямами та підходами Національної інформаційної політики є:

- забезпечення доступу громадян до інформації;
- створення національних інформаційних систем і мереж;
- зміцнення матеріально-технічної, фінансової, організаційної, правової та наукової бази інформаційної діяльності;
- забезпечення ефективного використання інформації;
- створення загальної системи захисту інформації;

- сприяння міжнародному співробітництву у сфері інформації та захисту інформаційного суверенітету України.
- сприяти постійному оновленню, збагаченню та збереженню національних інформаційних ресурсів [55].

Національна інформаційна політика формується та реалізується національними органами загальної компетенції та відповідними органами спеціальної компетенції. Усі громадяни, юридичні особи та державні установи України мають право на інформацію, яка передбачає можливість вільного одержання, використання, поширення та зберігання інформації, необхідної для здійснення ними своїх прав, свобод і законних інтересів, виконання покладених на них завдань і функцій. При здійсненні права на отримання інформації громадяни, юридичні особи і держава не повинні порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи, законні права та інтереси інших громадян, а також права і інтереси юридичних осіб. Кожен громадянин має вільний доступ до персональної інформації, крім випадків, передбачених законодавством України [55, 54].

З метою вдосконалення національної інформаційної політики України Указом Президента «Згідно з рішенням Ради національної безпеки і оборони України від 31 жовтня 2001 р. «Про заходи щодо вдосконалення національної інформаційної політики та забезпечення інформаційної безпеки в Україні» передбачено: для розробки проекту стратегії реалізації національної інформаційної політики варто вирішити наступні завдання:

- створити та запровадити ефективні механізми реалізації прав і свобод громадян, суспільства і держави на інформацію, передбачених Конституцією та законами України;
- подальше вдосконалення законодавства України у сфері інформації;
- розвиток державної інформаційної інфраструктури на основі сучасних інформаційних технологій, удосконалення систем інформаційно-аналітичного забезпечення діяльності Президента України та органів державної влади,

підвищення конкурентоспроможності державних виробників інформаційних продуктів, видів інформаційного виробництва;

• визначення порядку роботи та механізмів державного управління супутниковими, кабельними та комп'ютерними системами передачі інформації;

• формування єдиної національної системи взаємодії з громадськістю;

• подальша лібералізація ринку телекомунікацій України за умови гарантування реалізації національних інтересів та недопущення монополізації інформаційного ринку;

• наука, технології та підготовка кадрів для розвитку інформаційної індустрії;

• забезпечення інформаційного суверенітету України та вдосконалення системи захисту національних інформаційних ресурсів.

Основними завданнями Державної інформаційної політики України є:

• розгляд проекту Концепції роздержавлення українських ЗМІ;

• забезпечити законодавчу базу для запровадження системи суспільного телебачення і радіомовлення в Україні з урахуванням пропозиції Президента України до Закону України «Про створення системи суспільного телебачення і радіомовлення України»;

• законодавче врегулювання питань забезпечення конституційного права громадян на інформацію та захисту журналістів і ЗМІ від судового переслідування за критику (відповідальність за поширення недостовірної інформації, спростування інформації та відшкодування моральної шкоди, пов'язаної з поширенням інформації);

• розробка концепції просторового розвитку телерадіоінформації в Україні;

• розробка концепції розвитку української глобальної інформаційної мережі;

• розробка концепції інформаційної безпеки в Україні;

• розробка Українського інформаційного кодексу [60].

Варто зазначити, що основними викликами державної політики у сфері інформаційно-комунікаційної інфраструктури є забезпечення темпів випереджального розвитку будівництва інфраструктури зв'язку, підвищення інвестиційної привабливості інформаційної галузі, суттєве вдосконалення національної телекомунікаційної мережі та послуг поштового зв'язку, в основному базуючись на новітніх вітчизняних технологіях, інтегруватися у світову інформаційну структуру, в тому числі в Інтернет, створювати сприятливі умови для отримання населенням світових інформаційних ресурсів.

Однією з головних загроз інформаційній безпеці, як зазначено в Законі України «Про основи національної безпеки», є «спроби маніпулювання суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації». Доктрина інформаційної безпеки України визначає такі загрози національній інформаційній безпеці: поширення у світовому інформаційному просторі викривленої, недостовірної та необ'єктивної інформації, що завдає шкоди національним інтересам України, вплив зовнішньої деструктивної інформації на суспільну свідомість через засоби масової інформації та Інтернет Деструктивний вплив інформації, спрямованої на підрив конституційного ладу, суверенітету, територіальної цілісності та недоторканності України Прояви сепаратизму за національною, мовною, релігійною та іншими ознаками в засобах масової інформації та Інтернеті [58].

З метою прискорення інтеграції України у світовий інформаційний простір необхідно розробити та здійснити заходи щодо глибокої комп'ютеризації, насамперед, навчальних закладів, заохочення їх доступу до вітчизняних та світових інформаційних ресурсів. Потребує суттєвого прискорення інформатизація державних установ, фінансового сектору економіки та грошового обігу, бухгалтерського обліку, перехід на електронний документообіг, архівний документообіг, комп'ютеризація статистичної інформації та покращення зв'язку державних установ з

населенням за допомогою електронних каналів.. Актуальним завданням є гармонізація національного законодавства у сфері зв’язку з правовими нормами, прийнятими в країнах ЄС.

В Україні створено низку центральних органів державної виконавчої влади, на які покладено реалізацію державної інформаційної політики. Перш за все, слід зазначити: Державний комітет інформаційної політики, телебачення і радіомовлення України, Державний комітет зв'язку та інформатизації України, Державний комітет телебачення і радіомовлення.

Можемо зауважити, що Державний комітет України з питань інформаційної політики, телебачення і радіомовлення (Держкомінформ) діє як центральний орган виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України. Основні його повноваження : консультація з питань розробки державної політики у сфері інформації та видавничої справи, забезпечення її реалізації, здійснення керівництва нею у цих сферах, виконання міжвідомчої координації та функціонального керівництва покладеними на нього питаннями. У своїй діяльності керується Конституцією України, законами України, указами Президента України, постановами Кабінету Міністрів України. Узагальнює практику застосування законодавства з питань, що належать до його компетенції, формує пропозиції щодо вдосконалення законодавства та вносить їх у встановленому порядку на розгляд Президента України та Кабінету Міністрів України. У межах своєї компетенції організовує виконання актів законодавства та здійснює контроль за їх виконанням [63].

За умов стрімкого розвитку інформаційного суспільства в Україні та інформаційного простору спостерігається активізація застосування комунікаційно-інформаційних технологій у багатьох сферах життя, зростають загрозливі наслідки для держави проблеми безпеки інформаційної політики.

Основні загрози для інформаційної політики країни, відбуваються на тлі масової та агресивної інформаційної російської пропаганди, а також кіберзлочинів які країна агресор активно застосовує, що в подальшому

розпалює в Україні міжнаціональну ворожнечу, посягає на територіальну цілісність та державний суверенітет України [42, с.4-12].

Варто зазначити, що інформаційне середовище, інформаційні ресурси, інформаційні технології широко впливають на темпи і рівень науково-технічного, соціально-економічного і культурного розвитку. Саме безпека інформаційного простору та рівень його розвитку є факторами у галузях національної безпеки держави, які впливають на стан політичного, економічного, оборонного та інших сфер національної безпеки держави.

Основною метою реалізації положень принципів інформаційної безпеки України є створення в Україні розвиненого національного простору і захист її інформаційного суверенітету.

Забезпечення безпеки для інформаційної політики України ґрунтується на таких принципах:

- пріоритетності запобіжних факторів:
- взаємодії органів державної влади;
- підвищення захисту персональних даних;
- безперервності і комплексності заходів у галузі забезпечення інформаційної безпеки і захисту інформації;
- комплексності, дієвості і постійності заходів із захисту інформації та інформаційних ресурсів в інформаційному просторі [38].

Саме тому необхідною є державна підтримка вітчизняного виробника інформаційної продукції, інформаційно-телекомунікаційного обладнання, засобів телекомунікації, структур забезпечення інформаційної безпеки та кібербезпеки.

Для України вступ у нову фазу суспільного розвитку означає створення ситуації, за якої вдосконалюється не лише організація інформаційної бази української нації та держави – єдиної системи інформаційних баз, а й розвиток інформаційного виробництва та соціальні інформаційно-комунікаційні системи, основа українського інформаційного простору, та забезпечення відповідних позицій в міжнародному співробітництві.

Ключем до цього розвитку є організація безпеки національного інформаційного суверенітету України як об'єкта глобальної інформації. Ефективна інформаційна безпека нашого суспільства є запорукою існування та розвитку національних інформаційних ресурсів в умовах глобальних впливів [34].

Процеси глобалізації, які в останні десятиліття були каталізовані інформатизацією на основі електронних технологій, окрім свого позитивного значення для розвитку прогресу, несуть нові виклики та загрози інформаційній інфраструктурі, національному інформаційному суверенітету, ідентичності. Тому робота з нейтралізації кіберзагроз як важливої складової інформаційної політики є запорукою ефективного використання та довгострокового розвитку суверенних інформаційних систем для кожної держави та нації.

Розробка ефективних інструментів забезпечення інформаційного суверенітету є важливою передумовою суспільного розвитку та є пріоритетною сьогодні. Питання кібербезпеки є надзвичайно важливими для української держави на сучасному етапі, що пов’язано насамперед з необхідністю протистояти незаконним вторгненням в інформаційний простір України, збереження інформаційних ресурсів, захисту населення від негативного інформаційного впливу та інформаційної політики [33].

Крім того, стратегічно визнаним пріоритетом української зовнішньої політики є європейська інтеграція, що потребує постійного вдосконалення нормативно-правової бази кібербезпеки України, яка відповідала б не лише міжнародним стандартам, а, головне, національним інтересам України в інформаційній сфері [33].

Поразка в інформаційній війні, включаючи кібервійну, неминуче може призвести до розпаду держави. У сучасних умовах багато важливих систем промислового та оборонного секторів економіки, таких як системи управління повітряним рухом, енергетичні та атомні компанії та електромережі, засновані на інформаційно-комунікаційних технологіях, є потенційними ризиками через їхню вразливість до зовнішнього втручання.

Дефіцит інформації та її повністю або переважно негативний характер у сучасному світі може позначитися на зовнішньополітичній та економічній діяльності всієї країни, її окремих громадян та їх організацій. Тому це питання є загальнодержавним і, якщо його ігнорувати, становить загрозу національній безпеці.

Інший варіант – використання найжорсткіших тоталітарних методів контролю, але це діє лише на короткий час. Тому створення належних умов для розширення інформаційної, особливо символічної присутності у світовому інформаційному просторі, є найважливішим завданням національної політики інформаційної безпеки.

Тому до зовнішніх загроз кіберпростору належать хакерські атаки, що здійснюються з територій інших держав, спрямовані на порушення роботи комп'ютерних систем, викрадення конфіденційної інформації та ін. [27, с.34].

Боротьба з кіберзлочинністю має здійснюватися системно, виходячи з поточних ризиків і викликів у кіберпросторі, а інституційне середовище кібербезпеки необхідно постійно вдосконалювати. Ефективність заходів у цій сфері має досягатися шляхом оцінки загроз організованої кіберзлочинності, тим самим виявляючи поточні загрози та ризики у кіберпросторі. У сучасному глобалізованому світі Україні необхідно постійно працювати над удосконаленням системи кібербезпеки.

Діяльність провідних країн світу у кіберпросторі, глибокі зміни у внутрішній інформаційній політиці та формування потужних транснаціональних злочинних угруповань, що спеціалізуються на кіберзлочинності, вимагають розробки пріоритетів трансформації українського сектору кібербезпеки з урахуванням зазначених вище тенденцій.

Слід зазначити, що в швидкоплинному перебігу суспільного життя з революційними процесами в розвитку інформаційних технологій багато чинних нормативних актів, як національних, так і міжнародних, поступово втрачають свою актуальність, відповідність процесам, які вони регулюють, і

потребують уточнення або перегляду. Розвиток інформаційної діяльності породжує необхідність правового регулювання нових аспектів цієї діяльності.

Потрібне досконале юридичне обґрунтування для організації ефективної боротьби з кібертероризмом в умовах посилення глобального впливу, нових інформаційних технологій. Збір відповідних нормативно-правових актів необхідно постійно вдосконалювати з урахуванням відповідного міжнародного законодавства, його розвитку та національної законодавчої практики, що має відповідати інтересам національної інформаційної діяльності.

Питання правового регулювання як виконання державних завдань, зокрема забезпечення кібербезпеки та запобігання кіберзагрозам, має бути в центрі уваги. Пошук можливих рішень цього комплексу проблем є перспективним для подальших досліджень у галузі юриспруденції [28].

Оскільки існуючі на даний момент інформаційні технології дозволяють як приховувати місцезнаходження, так і використовувати дані інших, слід розробити наступні кроки:

1. На національному рівні:

- виступати та брати участь у розробці міжнародної стратегії боротьби з кіберзагрозами та створенні єдиних міжнародно-правових механізмів регулювання кіберпростору;

- загальною метою та напрямком Стратегії кібербезпеки має бути забезпечення віртуальної безпеки особи, організації та держави шляхом визначення системи пріоритетів, принципів та дій у сфері внутрішньої та зовнішньої політики;

- конкретні/приватні сфери стратегії повинні встановлювати стандарти співпраці суб’єктів інформаційного суспільства – окремих осіб, організацій та держави – у сфері кібербезпеки.

-розробка та впровадження багаторівневої інституційної системи кібербезпеки, яка включатиме:

1) науково-аналітичний рівень, який вивчає ризики кібербезпеки відповідно до можливостей кіберзагроз та масштабів негативних наслідків; оновлені інструменти та методи кібербезпеки. Це одне з найважливіших завдань, тому що проблема полягає в складності класифікації загроз, що виходять з території держави. У результаті цієї тенденції необхідно підкреслити, що кожна держава повинна вживати заходів для виявлення кіберзагроз та своєчасного, запобігання, захисту та мінімізації наслідків;

2) виконавчий рівень, який передбачав би у два напрямки – внутрішній (між національними структурами, відповідальними за виявлення кіберзагроз та реагування на них) та зовнішнішній, коли координація здійснюється між національними структурами та подібними іноземними регіональними/міжнародними установами [25].

Необхідно посилити заходи внутрішньої політики для стимулювання розвитку технологічної складової кібербезпеки, а саме:

- реалізовувати регіональне та міжнародне співробітництво у сфері кібербезпеки та здійснювати моніторинг діяльності злочинних, терористичних груп та окремих хакерів, що діють у кіберпросторі;
- активно брати участь у розвитку міжнародного співробітництва у сфері та структур, спрямованих на виявлення кіберзагроз, своєчасне виявлення, запобігання, захист та мінімізацію наслідків.

На міжнародному рівні:

- розробка та імплементація міжнародної угоди у сфері запобігання та розслідування кібератак та оновлення чинних нормативних актів;
- створення міжнародного органу з регіональними представництвами. Цей орган має бути еквівалентним ООН у кіберпросторі, тобто він повинен мати декілька структур, виконувати функції, які мають бути такими ж, як і на національному рівні [19, с.28-29].

Лише вирішуючи складні питання інформаційної безпеки, можна захистити інтереси суспільства і країни, гарантувати право громадян на отримання вичерпної, об'єктивної та якісної інформації. Існує два аспекти пояснення інформаційної безпеки в контексті національної безпеки. З одного боку, інформаційна безпека розглядається як самостійний елемент національної безпеки будь-якої країни, а з іншого – є невід'ємною частиною будь-якої іншої безпеки (військової, економічної, політичної тощо).

Висновки до розділу 2

Кібербезпека все більше розглядається як стратегічна проблема на державному рівні, яка впливає на всі сфери життя. Не є винятком і сучасний етап розвитку України, як і багатьох країн світу, який характеризується максимальною комп'ютеризацією всіх сфер життя. У той же час переміщення багатьох процесів, пов'язаних у тому числі й з критичними інфраструктурами у так званий кіберпростір робить їх вразливими до численних кіберзагроз.

Забезпечення безпеки у кіберпросторі є актуальним для нашої країни сьогодні, оскільки проти неї ведеться гібридна війна, що виявляється, серед іншого, у кібератаках на державні органи та установи України, а також на критично важливу інфраструктуру. З огляду на це, держава має приділяти максимум уваги кібербезпеці.

Інформаційна безпека є інтегрованою складовою національної безпеки і її розглядають як пріоритетну функцію держави. Інформаційна безпеки, з одного боку, передбачає забезпечення якісного всебічного інформування громадян та вільного доступу до різних джерел інформації, а з іншого – це контроль за непоширенням дезінформації, сприяння цілісності суспільства, збереження інформаційного суверенітету, протидія негативним інформаційно-психологічним пропагандистським впливам та захист національного інформаційного простору від маніпуляцій, інформаційних війн та операцій.

Розвиток технологій у сучасному світі не тільки дозволяє людству вирішувати багато проблем його постійної еволюції, але й приносить нові виклики та загрози у сфері віртуального кіберпростору.

Тому, на жаль, національний інформаційний простір України стикається з серйозними загрозами та викликами, що створюють загрозу для функціонування держави, політичного та економічного розвитку, інтеграції до європейських та євроатлантичних структур. Загрози національній безпеці України в інформаційній сфері – сукупність умов і факторів, за яких інформація може негативно впливати на свідомість і поведінку громадян, створюючи тим самим загрозу життєво важливим інтересам держави, суспільства та особи, а також інформаційним ресурсам. інформаційна та технологічна інфраструктура.

РОЗДІЛ 3. ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ

3.1. Особливості атак на державні інформаційні ресурси до та на початку повномасштабного вторгнення Росії в Україну

Питання кіберзлочинності є надзвичайно актуальним на державному рівні. У більшості випадків кібератакам піддаються об’єкти критичної інфраструктури: енергетичні, транспортні та банківські. Вартість захисту зазвичай у 10 разів перевищує саму атаку. Тому кібербезпека є пріоритетною сферою багатьох національних політик.

ІТ – армія Російської Федерації постійно здійснює атаки на кіберпростір України та міжнародне співтовариство, тому слід бути готовим до можливої активізації бойових дій у кіберпросторі. Усі громадяни повинні пам’ятати, що кожного разу, коли вони вмикають комп’ютер або відкривають мобільний браузер, вони є потенційною мішенню для кіберзлочинців, тому захистити себе в Інтернеті надзвичайно важливо [67].

Суспільство має повністю усвідомлювати ризики, з якими воно може зіткнутися в кіберпросторі, тому 23 лютого 2006 року, відповідно до прийнятого в Україні Закону України «Про державну службу спеціального зв’язку та захисту інформації України», на базі ліквідованого Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України була створена Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку). Це спеціалізований орган центрального адміністративного органу у сфері спеціального зв’язку та захисту інформації, головний орган відомств національної оборони та безпеки та головний орган національної системи мережевої безпеки, який координує діяльність суб’єктів мережевої безпеки [66].

Державна служба спеціального зв'язку та захисту інформації України виконує 93 завдання й функції та формує державну політику в 16 сферах

(згідно із Законом України “Про Державну службу спеціального зв'язку та захисту України”). У штаті Держспецзв'язку та підприємств, що належать до сфери управління Служби, працюють понад 10 тис. фахівців, з-поміж яких 80% – військовослужбовці.

Проаналізувавши оперативну інформацію Держспецзв’язку щодо захисту державних інформаційних ресурсів за період з 24 по 30 червня 2020 року ми виявили, що система кіберзахисту державних інформаційних ресурсів та об’єктів критичної інфраструктури на об’єктах моніторингу зафіксувала 37102 підозрілих події, що на 16% менше, ніж за попередній тиждень цього ж місяця. Переважна більшість зафіксованих підозрілих подій стосується спроб мережевого сканування (50%), виявлення нестандартних протоколів або подій (20%), веб-атак (14%), виявлення мережевого трояна (11%) та спроб отримання прав адміністратора (4%). Система захищеного доступу державних органів до мережі Інтернет заблокувала 9608 різних видів атак, що на 7% більше, ніж попереднього тижня цього ж місяця. Переважна більшість (99%) - це мережеві атаки прикладного рівня. Також заблоковано 4 DDoS-атаки [37].

Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA у цей період зареєструвала та опрацювала 498 кіберінцидентів. Переважна більшість опрацьованих інцидентів належить доменній зоні UACOM (близько 99%). Основна кількість інцидентів стосується розповсюдження ШПЗ (91% від загальної кількості) та фішингу (8%).

Російські військові здатні не тільки воювати за допомогою ракет і артилерії, але й використовувати шкідливий код для виведення з ладу критичної інфраструктури в Україні, тероризувати громадян і викрадати їхні конфіденційні дані. Такий вид війни, коли «класичні» бойові дії супроводжуються атаками в кіберпросторі, називають кібервійною.

Як зазначив віце-прем’єр-міністр – міністр цифрової трансформації України Михайло Федоров, вперше за всю історію воєнних дій бойові дії вийшли у невидимий цифровий світ. Сьогодні кіберфронт є одним із важливих фронтів у боротьбі з російськими агресорами. У квітні (2022) голова

Держспецзв'язку та захисту інформації Юрій Щиголь повідомляв, що кількість кібератак на Україну цього року вдвічі більша, ніж торік.

Вони спостерігалися з найбільшою інтенсивністю та витонченістю напередодні повномасштабного російського вторгнення в Україну та в перші місяці після нього. Водночас, за даними Держспецзв'язку, найбільший інтерес для окупантів становлять українські органи державної влади та місцевого самоврядування, відомства сектору безпеки та оборони, життєво важливі фінансова, енергетична, транспортна, телекомунікаційна та логістична сфери.

Варто зазначити, що російські хакери загрожують не лише Україні, а й усьому цивілізованому світу. Водночас в України є досить впливові союзники. Тому дії, що відбуваються сьогодні на глобальній кіберарені, буквально можна назвати першою світовою кібервійною [37].

У Декларації високого представника ЄС від імені всіх держав ЄС зазначається, що не спровокована та необґрунтована військова агресія Росії проти України супроводжувалася зростанням шкідливої кіберактивності. Хакери та хакерські групи без розбору атакують ключові організації по всьому світу. У контексті війни проти України зростання шкідливої кіберактивності несе неприйнятні побічні ефекти, непорозуміння та ризик можливої ескалації.

Російське вторгнення в український кіберпростір почалося ще до того, як російська армія фактично перетнула український кордон. Як повідомила компанія ESET, росіяни, можливо, почали готуватися до кібератаки за кілька місяців до початку повномасштабного вторгнення, вже зламавши сайти організацій, за якими вони стежили.

Так, наприкінці вересня (2021 року) СБУ викрила у Львові групу хакерів, які зламали акаунти майже 30 мільйонів громадян ЄС та України з метою поширення російської пропаганди. Як зазначили в СБУ, хакери продавали конфіденційну інформацію через анонімні даркнет-платформи та збирали платежі через заборонені в Україні електронні платіжні системи YuMoney, Qiwi та WebMoney. Однак, хоча російські кіберзлочинці діють досить широко, вони найбільше зосереджені на Україні.

У Міністерстві цифрової трансформації зазначалося, що найбільша кібератака в історії нашої країни сталася 15 лютого, за 9 днів до початку повномасштабної атаки. Згодом сайти Міністерства оборони та ЗСУ зазнали DDoS-атаки. Також зафіксовано збої в роботі мережевих сервісів державних банків - "Ощадбанку" і "ПриватБанку". Головною метою цієї атаки була дестабілізація, бажання посіяти паніку, якийсь хаос у діях українців. Близько 20:00 того ж дня, слідом за банком, було здійснено потужну DDoS-атаку і на портал Дія, що було очікувано. Вихідними векторами є Росія і Китай. Близько 600 000 пакетів шкідливого трафіку в секунду. Українські експерти швидко «зрізали» цей напрямок, але атака повернулася з Чехії та Узбекистану. І її знову «забракували». Для користувачів Дії атака пройшла непоміченою [63].

Напередодні початку російсько-української війни, 23 лютого, сталася чергова масштабна DDoS-атака, під час якої російські хакери атакували сайти різних українських міністерств, Верховної Ради, СБУ та інших державних установ. Пізніше, за годину до повномасштабного вторгнення, супутникова мережа Viasat стала об’єктом кібератаки противника. Тоді російські хакери атакували альтернативні супутникові канали зв’язку. Атака викликала багато проблем, особливо в Європі, де вийшли з ладу десятки тисяч супутникових терміналів, які використовували підприємства та різні організації.

Паралельно з цими атаками також здійснювалися спроби зламу державних реєстрів України, зокрема Державного реєстру нерухомого майна та Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань, оскільки це два ключових реєстри для забезпечення безпеки громадян та їхньої власності. Тоді Міністерство юстиції прийняло швидке та рішуче рішення повністю відключити ці реєстри від загальної мережі, забезпечивши їхню автономну роботу та зберігаючи всі дані на пов’язаних серверах. Це рішення виявилося правильним, оскільки з моменту припинення доступу 24 лютого до моменту його поступового відновлення жодному кіберзлочинцю не вдалося отримати доступ до інформації, що міститься в цих реєстрах [63].

Рішення про тимчасове зберігання даних за кордоном також є важливим кроком у збереженні українських даних. У цьому нам допомогла американська компанія Amazon. У результаті за перші тижні війни 36 органів влади України перенесли на ресурси Amazon понад 60 своїх ключових реєстрів і систем, серед яких: МВС, МОЗ, система ProZorro, Всеукраїнська школа онлайн тощо.

Ще однією потужною атакою рашистів на Україну стала атака на «Укртелеком», одного з найбільших операторів зв'язку, наприкінці березня 2022 року. Зловмисники намагалися вивести з ладу обладнання компанії, сервери та взяти під контроль мережу [54].

Невдовзі, на початку квітня 2022 року, енергетичний сектор України став ціллю російських кіберзлочинців, але атаку вдалося вчасно зупинити. Якщо атака була б успішною, близько 2 мільйонів українців могли б залишитися без світла.

За даними Національної спецслужби, план зловмисника полягав у виведенні з ладу кількох елементів інфраструктури, а саме: електропідстанцій, електронно-обчислювальних машин під управлінням операційних систем Windows (комп'ютери користувачів, сервери та автоматизовані робочі місця), комп'ютерів, керованих операційними системами Linux, серверного обладнання, активне мережеве обладнання. Однак у відомстві зазначили, що порівняно з зимою та весною 2022 року інтенсивність та якість російських кібератак поступово знизилися, оскільки російські хакери не підготувалися так добре, як раніше. Вони не можуть витрачати на це час, тому що вони повинні захистити себе, оскільки виявилося, що їхні системи також вразливі. Крім того, не варто забувати, що ціна великомасштабної кібератаки є досить високою, а під впливом санкцій фінансові ресурси ворога вичерпуються досить швидко [52].

Головний системний інженер "ВОЛЗ" та експерта із захисту від DDoS-атак, наголошує на тому, що зловмисники можуть «вкласти» мільйони доларів у підготовку до однієї атаки. Типова DDoS-атака на невеликий сайт може починатися від 10 доларів США. Якщо говорити про масову атаку на зразок

лютого 2022 року, коли користувачі годинами не могли отримати доступ до банківських систем і веб-сайтів державних установ, вони коштують набагато дорожче. Варто також розуміти, що у випадку постійної і, відповідно, дорогої DDoS-атаки, процес підготовки до атаки, включаючи аналіз інформаційних систем жертви, пошук вразливостей, залучення ресурсів/ботів тощо, коштує недешево.

Нами було визначено, що початок військової операції повністю змінив форму роботи Мінцифри та спрямував основні сили на протистояння РФ на кібернетичному та інформаційному фронтах. Самостійно захиститися від кіберзагроз неможливо, тому взаємодія повинна здійснюватися на всіх рівнях, включаючи країни та бізнес. У внутрішньому плані кожен суб'єкт і об'єкт національної системи кібербезпеки повинні мати власні ролі та не повинні лише покладатися один на одного.

За даними Мінцифри, безпосередньо за кіберзахист в Україні відповідає відомство зі спеціальним державним спеціальним статусом зв'язку. Він є філією Національного центру кіберзахисту, а його підрозділ CERT-UA займається моніторингом і виявленням потенційних кіберзагроз. Кіберзахистом також займаються МВС, Міноборони, Генштаб і СБУ [65].

Кіберполіція відповідає за розслідування кіберзлочинів, Міністерство оборони та Генштаб – забезпечення охорони військових об'єктів та критичної інфраструктури, а СБУ – запобігання терористичним атакам у кіберпросторі. Крім того, наприкінці серпня минулого року президент України Володимир Зеленський підписав указ про створення кібервійськ у структурі Міноборони України, але їх не встигли створити до початку повномасштабної війни з Російською Федерацією. Мінцифри має постійно працювати над подоланням «цифрової блокади» Росії.

Водночас у той час, коли ресурси російського кіберпростору вичерпуються, українська «ІТ-армія» досягла великих успіхів на передовій кібервійни. На початку війни Міністерство цифрової трансформації створило

першу в історії України «ІТ-армію», у якій налічувалося понад 200 тисяч добровольців.

Міністр Михайло Федоров зазначив, що українські айтішники лише захищалися до 24 лютого, але з моменту повномасштабного вторгнення почали боротися і на кіберфронті. У результаті було скомпрометовано велику частину важливої інфраструктури Російської Федерації. Росіянам доведеться витратити чимало сил на його відновлення чи протидію атаці української «ІТ-армії».

Однією з перемог української «ІТ-армії» став злом сайту російської приватної військової компанії «Вагнер». Українські кіберзахисники отримали особисті дані найманців "Вагнера", які ведуть злочинну діяльність на території України.

Загалом з 29 серпня по 11 вересня 2022 року українська «ІТ-армія» паралізувала роботу понад 2400 російських онлайн-ресурсів. Зокрема послуги «Газпромбанку», «Московського кредитного банку» та «Совкомбанку». Крім того, кібератака тимчасово вивела з ладу основні російські пропагандистські видання Rambler, Gazeta.Ru, MK.

Зауважимо, що до «ІТ-армії» може приєднатися будь-який користувач Інтернету. Найбільше завдань у таких групах полягає у скаргах на російські акаунти в соцмережах. Зазвичай достатньо 5-10 скарг, щоб система перевела обліковий запис на перевірку модерацією. Велика кількість скарг часто призводить до автоматичного блокування облікового запису в обхід перевірки. Таким чином ІТ-армія може ефективно вивести з ладу російських пропагандистів. Одним із найскладніших варіантів ведення ІТ-війни є хакерство, найпопулярнішим з яких є DDOS. Суть DDOS-атаки полягає в надсиланні великої кількості запитів на веб-сайт, через що сервер перевантажується і виходить з ладу, а потім онлайн-ресурси стають недоступними.Чи зможе веб-сайт відновити роботу за день, тиждень чи місяць – усе залежить від кваліфікації ворожої ІТ-команди [67].

Часто DDOS-атаки організовують люди, які мають доступ до великої кількості фізичних комп’ютерів або серверів, що може бути досить дорогим з економічної точки зору. Але оскільки українська «IT-армія» складається з тисяч незалежних людей, кожна зі своїм комп’ютером, ми можемо здійснити атаку такого масштабу ефективно та безкоштовно, а пересічній людині доведеться витратити десятки тисяч доларів.

Як відомо, Україні протистояти окупантам допомагає весь цивілізований світ. Яскравим прикладом світової підтримки є звернення міжнародної хакерської мережі Anonymous до захисників України, яка оголосила війну російській владі у відповідь на повномасштабне вторгнення Росії в Україну.

Ще на початку російського вторгнення хакери заблокували пропагандистський веб-сайт Russia Today, зламали веб-сайт Міністерства оборони Росії та розкрили базу даних номерів телефонів, електронних адрес та імен співробітників. Крім того, вони здійснили кілька дзвінків до російського уряду, в яких повідомили про свою чергову кібератаку проти держави-терориста. Одним із найгучніших прикладів роботи Anonymous став злом провладної російської відеоплатформи RuTube. Тоді серйозно постраждали майже 75% баз даних та інфраструктури, які обслуговує основна версія, 90% резервних копій і кластери, які використовуються для відновлення бази даних платформи.

У ході дослідження ми з’ясували, що в Україні зосереджені далеко не всі IT - активісти - вони працюють зі всього світу, адже співвідношення на даний момент 99 до 1, тобто весь світ проти Росії. Варто підкреслити, що на Росії хакери відносяться в основному до силовиків, тобто ними керують ГРУ, ФСБ, Управління "К" МВС РФ, група ІВ, тобто люди, які системно служать у російській армії. А весь світ активістів, ті самі Anonymous, "Мамкины хакеры", No name, зараз "ламають" Російську Федерацію.

3.2. Дослідження стану державної інформаційної політики до та після повномасштабного вторгнення Росії в Україну

Останніми роками, до повномасштабного вторгнення, Україна швидко оцифровувала та в деяких сферах лідирувала серед високотехнологічних країн світу. Було зроблено багато, що значною мірою дозволило країні сьогодні досягти успіху в цифровому просторі та інформаційному секторі.

Зокрема, Україна стала першою країною у світі, яка повністю легалізувала цифрові паспорти в смартфонах. Для будь-якої життєвої ситуації, де потрібен паспорт, українцям достатньо мати при собі телефон із цифровим паспортом. З 23 серпня 2021 року біометричні паспорти та ID-картки Дії на законодавчому рівні стають повним аналогом паперу та пластику, а Україна – новатором у використанні цифрових документів.

Верховна Рада у другому читанні ухвалила законопроект №4355 «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» про цифрові паспорти.

Віце-прем'єр-міністр – міністр цифрової трансформації Михайло Федоров зазначив, що Україна є першою країною у світі, яка запровадила цифровий паспорт, який юридично прирівнюється до звичайного документа. Користувачі Дії більше не стикатимуться з паперовими паспортами. Це не лише велика подія в сучасній українській історії, а й величезний крок до впровадження системи «без паперу». Це унікальний світовий випадок, яким можна і потрібно пишатися.

Мінцифри запустило цифровий паспорт у мобільному додатку Дія у квітні 2020 року. Цифрові паспорти безпечніші та зручніші, ніж паперові. У 2022 році ними змогли скористатися близько 20 мільйонів українців, з них понад 5,5 мільйонів мають ID-картки, ще 18 мільйонів мають закордонні біометричні паспорти. Їх використання є дослідним проектом і регламентується відповідними постановами Кабінету Міністрів України [63].

Таким чином, законопроект «Про внесення змін до Закону України "Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус" № 1368-IX набув чинності з 23 серпня 2021 року та забезпечив можливість використання електронних документів у мобільному застосунку на рівні із звичайними паспортами. Це перший крок до запровадження безпаперового режиму в Україні – коли державні органи не матимуть права вимагати паперові документи, якщо інформація вже є у реєстрах.

Цифрові паспорти можна пред'являти в межах України для ідентифікації та підтвердження громадянства, крім випадків перетину державного кордону, в'їзду на тимчасово окуповану територію України та виїзду з неї. Ухвалений законопроект також визначає терміни, зокрема використання електронних паспортів [45].

Українці можуть користуватися цифровими паспортами в більшості життєвих ситуацій. Їх приймають ЦНАПи для надання даржавних послуг, державні установи та суди. Цифрові паспорти можна використовувати для отримання відправлень на пошті, перевірки віку в супермаркетах, банках – для підтвердження особи та проведення касових операцій, а також для відкриття банківських рахунків онлайн. З цифровим паспортом ви також можете подорожувати Україною літаком і поїздом, зупинятися в готелях тощо.

Цифрові документи в смартфонах також використовують у Польщі та Південній Кореї. Подібні проекти реалізуються у Великобританії, Фінляндії та США. Громадяни Естонії використовують цифрові паспорти, щоб отримувати державні послуги онлайн, керувати банківськими рахунками та голосувати через Інтернет. Однак Україна стала першою країною у світі, де цифрові паспорти в смартфонах мають таку ж юридичну силу, як паперові та пластикові документи.

У вересні 2021 року Україна почала переходити на режим «без паперу» – держоргани не мають права вимагати паперові документи, якщо необхідна інформація вже є в реєстрі. Ухвалення закону про цифровий паспорт стало

одним із найважливіших кроків на шляху до цієї мети, оскільки сам паспорт є основним документом для доступу до державних послуг. Він також розпочав масову оцифровку бізнесу, а також оптимізував внутрішні процеси для запуску нових цифрових продуктів.

Закон розроблено за сприяння програми EGAP, яка фінансується урядом Швейцарії та виконується Східноєвропейським фондом SURGe за підтримки уряду Канади. Важливо також зазначити, що закон ухвалено за сприяння та підтримки Президента України, Прем'єр-міністра України, Ради цифрової трансформації, Державної міграційної служби та Міністерства внутрішніх справ.

Аналізуючи вищесказане, можна зробити висновок, що незважаючи на війну, в Україні все ще розвиваються старі та нові проекти, тому можна сказати, що країна має хороше цифрове майбутнє, але щоб досягти цього, українські IT-спеціалісти на державному рівні мають сформулювати план цифрового розвитку.

Крім того, ми визначили, що незважаючи на війну, боротьбу на інформаційному фронті та в кіберпросторі, Міністерство цифрової трансформації працює над планом розвитку цифровізації в Україні після війни.

Сьогодні це дуже важливо, тому що країні необхідно відроджувати економіку та відбудовувати промисловість, на що потрібні роки.

Як ми вже згадували вище, навіть у воєнний час IT-підрозділи показали стійкість до стресових ситуацій. Галузь продовжує виконувати контракти, експортувати послуги, забезпечувати валютні надходження та підтримувати економіку. Тому можна сказати, що IT-індустрія дуже допомогла Україні пережити цю війну.

Наприклад, у першому кварталі 2022 року IT-галузь забезпечила рекордний за всі роки свого існування квартальний експорт у $2 млрд, повідомляє НБУ. Їй вдалося виконати 95% контрактів.

IT-сфера сьогодні працює набагато краще, ніж інші галузі, головним чином завдяки своїй мобільності, гнучкості та можливості працювати віддалено.

Таким чином, поки країна відбудовується, IT-галузь може значною мірою забезпечити її економічну стабільність. Але для цього Міністерство цифрової трансформації має розробити конкретні плани підтримки галузей, які потребують зростання. Йдеться не лише про економічні важелі, а й про стимулювання інвестицій, розвиток освіти тощо.

Зазначимо, що сьогодні, незважаючи на воєнний стан, держава продовжує підтримувати IT-галузь. Так, є спеціальний юридично-податковий простір Дія.City – це низькі податки, норми законодавства Великої Британії та нова гнучка форма співпраці між спеціалістами та компаніями – гіг- контракти.

З 8 лютого 2022 року в Україні запрацював спеціальний правовий режим «Дія.City» для розвитку IT-галузі. У виступі президента Володимира Зеленського, зазначалося, що завдяки Дія.City частка IT у ВВП України зросте з 4% до 10%, а дохід сягне $16,5 млрд. За його словами, першими до режиму приєднаються провідні іноземні та українські IT-компанії.

Операційний менеджер British Revolut Дмитро Стрельчук розповів, що компанія буде першою в Дія.City. За словами міністра цифрової трансформації Михайла Федорова, Revolut, який працює в 36 країнах, є найдорожчим стартапом у Великобританії [63].

Пізніше засновник SoftServe Тарас Кицмей заявив, що компанія також хоче подати заявку, щоб однією з перших приєднатися до режиму.

Режим створений для аутсорсингових компаній, R&D-компаній, продуктових компаній, стартапів. Резидентами спецрежиму можуть стати компанії, які займаються, зокрема:

- розробкою і тестуванням програмного забезпечення;
- виданням та розповсюдженням програмного забезпечення;
- навчанням комп'ютерної грамотності, програмування, тестування та технічної підтримки ПЗ;

- Digital marketing та Ads з використанням програмного забезпечення, розробленого резидентами;

Для компаній розроблені певні критерії входу. Так, для аутсорсингових, R&D і продуктових компаній є вимоги щодо питомої ваги доходів від здійснення встановлених видів діяльності, середньої зарплати, кількості працівників/GIG-спеціалістів. Для стартапів також є вимоги до річного доходу та терміну реєстрації. Для компаній-резидентів передбачено спеціальний податковий режим. Зокрема, вони сплачуватимуть (див.рис.3.1):

Рис.3.1 Податковий режим для компаній-резидентів

Режим ґрунтується на моделі ґіґ-економіки, тобто моделі трудових відносин, заснованій на короткострокових контрактах або неформальних домовленостях.

Законопроект Дія.City викликав багато дискусій серед представників IT-галузі, але хоча Дія.City запрацювала лише на початку лютого 2022 року, його резидентами стали понад 250 компаній. І заявки продовжують з’являтися.

У той же час після війни необхідно розширити підтримку галузі. І це також має бути національним пріоритетом.

Щодо стратегії розвитку, то бачення цифрового майбутнього України було представлено на першому в історії України міжнародному саміті Дія у Давосі. Загалом на форумі в Давосі Україна була в центрі уваги. Росія була не допущена до заходу вперше за десять років. Натомість під час саміту на базі традиційного Російського дому в Давосі відкрився Російський дім військових злочинців.

На Всесвітньому економічному форумі було приділено велику увагу глобальним наслідкам війни в Україні та російського вторгнення. Однак обговорювалося й майбутнє відновлення країни. Звичайно, це було б неможливо без цифрової економіки. Міністерство цифрової трансформації визначило свою головну мету щодо розвитку ІТ-сектору – зробити Україну найбільш розвиненою та успішною цифровою країною. У міністерстві зазначили, що, як і до війни, зберегли плани перевести 100% державних послуг в онлайн-сферу, забезпечити 95% населення якісним інтернетом, навчити українців цифровим навичкам, збільшити частку ІТ у ВВП. З цією метою Міністерство освіти продовжить розширювати можливості програми Дія, підтримувати Дія city, реформувати ІТ-освіту та розвивати стартап-екосистему.

Підсумуємо, що, наразі спільно з індустрією активно формується стратегія розвитку ІТ-галузі попри військовий час. Важливо максимально враховувати всі потреби галузі. Загалом цифрова стратегія базується на підтримці продуктового напрямку. Протягом останнього десятиліття аутсорсинг був основою українського ІТ-ринку. Він має і матиме підтримку держави.

Водночас потенціал України у виробництві високотехнологічної продукції величезний. Це не просто додаткові робочі місця, а виробництво з доданою вартістю, яке може значно поповнити бюджет.

Для реалізації цього потенціалу необхідно не лише використовувати механізми підтримки продуктового бізнесу та залучення інвестицій, але й сприяти розвитку підготовки та навчання відповідних спеціалістів, тому за підтримки уряду в Україні стартувала програма підготовки ІТ-спеціалістів «Старт в ІТ».

Постановою КМ України від 24.06.2022 №737 затверджено Порядок реалізації експерименту з організації навчання осіб за освітніми програмами у сфері інформаційних технологій «Старт в ІТ» [53].

Умови гранту – особа, яка завершила навчання, протягом 30 календарних днів зобов’язується працевлаштуватись за отриманою кваліфікацією на умовах:

- трудового договору (контракту), гіг-контракту за наймом;

- укладення цивільно-правового договору про виконання робіт (надання послуг);

- зареєструватися як ФОП чи провадити незалежну професійну діяльність за набутою кваліфікацією.

Програма розрахована на осіб, які є громадянами України (п.п.5, 9 Порядку) та:

- які перебувають у простої;

- з якими зупинено дію трудового договору;

- яким надано відпустку без збереження заробітної плати без обмеження строку, встановленого частиною першою ст.26 Закону України «Про відпустки» відповідно до частини третьої ст.12 Закону України «Про організацію трудових відносин в умовах воєнного стану»;

- внутрішньо переміщені особи працездатного віку;

- зареєстровані безробітні, які мають право на отримання соціальних послуг з професійної підготовки, перепідготовки та підвищення кваліфікації відповідно до Законів «Про загальнообов'язкове державне соціальне страхування на випадок безробіття» і «Про зайнятість населення» та інші особи, за винятком тих, на які дія Порядку не поширюється.

Сертифікат на навчання формується в електронній формі на "Порталі Дія" за результатами розгляду документів Центром зайнятості та видається одноразово (п.11 Порядку).

Перелік навчальних закладів та перелік освітніх програм у сфері інформаційних технологій, за якими може проходити навчання з отриманням сертифікатів, визначається та затверджується Мінцифри (ст. 6 порядку). Після погодження Мінцифрою освітнього проекту та визначення суб'єкта освітньої діяльності, який здійснює навчання за затвердженим освітнім проектом, його перелік буде опубліковано на офіційному сайті центру зайнятості.

Метою пілотного проекту є реалізація права громадян на працю та сприяння зайнятості населення. 24 червня український уряд затвердив грантову програму підготовки фахівців у сфері IT в рамках проекту «eRobota». Команда

проекту сподівається, що 80-90% студентів зможуть знайти роботу в ІТ-сфері та працювати на потреби країни.

Крім того, держава повинна надалі сприяти розвитку аутсорсингових компаній, що стали драйвером розвитку ІТ-України. Важливо дати можливість фахівцям сфери ІТ реалізувати себе на Батьківщині. Сьогодні в Україні на 1 млн населення приходиться 75 стартапів. Для порівняння, у Ізраїлі — 975, у Естонії — 865, у Ірландії — 665, у Данії — 573, у Фінляндії — 525.

Міністерством цифрової трансформації визначено, що в Україні є все, щоб мати показники вищі, ніж у будь-якій з цих країн, тож воно активно працює над розвитком української стартап-екосистеми.

На початку війни зарубіжні кіберспеціалісти відзначали координованість дій військових та хакерів. Наприклад, 1 березня Росія обстріляла ракетами київську телевежу, що призвело до зупинки телевізійного мовлення. Водночас росіяни здійснили кібератаку по Концерну радіомовлення, радіозв'язку і телебачення [47].

Щойно почалася велика війна, найпопулярніші російські APT-групи – угруповання висококваліфікованих хакерів – приєдналися до атак на Україну.

Експерти стверджують, що Росія недооцінила Україну не тільки у військовій, а й у кіберсфері. Україна зробила значні інвестиції для покращення кіберзахисту після двох масштабних кібератак у 2015 році та 2017 роках.

Крім того, підтримка країн та глобальних волонтерських організацій дає значні переваги, що має привести до перемоги України на обох фронтах.

Задля покращення стану захищеності інформаційної політики, а також національних електронних інформаційних ресурсів, було розроблено комплекс заходів, спрямованих на посилення захисту персональних даних громадян від витоків, а також підвищення ефективності взаємодії між суб’єктами забезпечення кібербезпеки та удосконалення нормативно-правової бази у сфері кібербезпеки.

В умовах сучасного інформаційного протистояння, експансіоністської політики Російської Федерації національний інформаційний простір України не є належним чином захищеним від зовнішнього негативного пропагандистського інформаційно-психологічного впливу та загроз. Тому захист інформаційного

суверенітету, створення сильної та ефективної системи інформаційної безпеки України, розробка ефективних стратегій і тактик протидії медіа-загрозам мають бути першочерговими завданнями органів державної влади та недержавних інституцій.

Можна підсумувати, що в умовах активізації діяльності іноземних агентів, націлених на нашу державу, особливо спецслужб Російської Федерації, посилення кіберзахисту державних інформаційних ресурсів та захисту персональних даних громадян України від витоку стало пріоритетом державної інформаційної політики у сфері кібербезпеки.

3.3. Практичні рекомендації попередження кіберзлочинності в Україні

Україна для забезпечення безпеки інформаційної політики має вживати низку заходів:

У зовнішньополітичній сфері:

- ✓ покращення інформаційного забезпечення державної політики, діяльності українських громадських організацій та комерційних структур;
- ✓ надавати організаційно-технічну, ресурсну та інформаційну допомогу українським ЗМІ з метою формування позитивного іміджу України в інформаційній сфері;
- ✓ посилення просвітницької роботи щодо переваг членства України в Європейському Союзі, посилення практичної співпраці з НАТО, іншими міжнародними організаціями та країнами-партнерами у сфері безпеки та ефективних шляхів зміцнення національної безпеки України, особливо з огляду на перспективу розгляду повноправного членства в НАТО;
- ✓ інтегруватися в економічно життєздатні та організовані міжнародні інформаційні та комунікаційні системи на основі рівності, кіберзахисту та збереження інформаційного суверенітету;
- ✓ забезпечити своєчасне виявлення та нейтралізацію зовнішніх загроз національному інформаційному суверенітету, зокрема за допомогою методів кібербезпеки:

- ✓ сприяти встановленню та дотриманню міжнародних правил поведінки держав в інформаційному просторі;
- ✓ підвищення рівня міжнародного співробітництва у сфері інформаційної безпеки на національному та галузевому рівнях, поширення інформації у світовому інформаційному просторі, формування позитивного іміджу України як надійного партнера у міжнародних відносинах та популяризація позитивного надбання України;
- ✓ підтримувати існуючу підготовку з протидії інформаційним загрозам для приватних і національних інформаційних інфраструктур та ініціювати нові типи такої підготовки;
- ✓ впровадження засобів запобігання впливу зовнішньої інформації, зокрема шляхом підвищення якості національного культурно-інформаційного продукту;
- ✓ застосовувати комплексні та ефективні заходи для поширення об'єктивної інформації про Україну за кордоном та протидії загрозам інформаційній безпеці, зокрема шляхом оперативного та обґрунтованого спростування дезінформації про Україну у світовому інформаційному просторі та усунення негативних стереотипів щодо України у світовому інформаційному просторі [6, с. 25-29].

Для недопущення інформаційної експансії, діяльність країни в інформаційному просторі має здійснюватися за такими напрямами:

1) Реалізація превентивної стратегії і тактики (профілактичні заходи)

2) Реалізація стратегії реагування (бойове реагування на інформаційні атаки противника та активні атаки)

3) Захист національного інформаційного простору.

Основна мета – забезпечити домінування та домінування ЗМІ в інформаційному просторі. Крім того, першочерговими завданнями

інформаційної структури влади для захисту інформаційної політики мають бути:

- ✓ контроль над потоками інформації;
- ✓ надання об’єктивної та всебічної інформації;
- ✓ професійне коментування та роз’яснення подій;
- ✓ систематичне донесення офіційних позицій чиновників і політичних лідерів.

Таким чином, інформаційна безпека є невід'ємним складником кожної зі сфер національної безпеки. Інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки, яка характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз, є сукупністю інформаційно-психологічної (психофізичної) та інформаційно-технологічної безпеки держави.

Тому розвиток України (як суверенної, демократичної, правової та економічно стабільної країни) можливий лише шляхом забезпечення належного рівня інформаційної безпеки, надання всебічної державної підтримки та телекомунікаційного обладнання виробникам національного інформаційного продукту, створення регуляторної, фінансової та інших передумов, необхідних для успішної конкуренції на світовому та національному ринку інформаційно-телекомунікаційних послуг.

Щодо зовнішньої політики, то це інтеграція до інформаційного простору СС, а також інтеграції до структур НАТО, яка дає фізичний, матеріальний і психологічний аспект перспективним противникам України не зашкодити нашому кіберпростору та інформаційному полю [7, с. 439].

Щодо захисту кожного громадянина країни персонально, варто зазначити, що на сайті Держспецзв’язку зазначається, що в разі будь-яких кіберінцидентів, кібератак або підозрілих дій щодо інформаційно-телекомунікаційних систем громадянину слід інформувати урядову команду

реагування на комп'ютерні надзвичайні події України CERT-UA. Крім того, на сайті зібрана велика кількість правил цифрової гігієни, дотримання яких дозволяє убезпечити власні персональні дані від ворожих атак.

Найголовніші з них зокрема такі:

1. Ніколи не натискайте на невідомі посилання. Зрештою, інколи достатньо лише натиснути подібне посилання, щоб стати мішенню для шахраїв.

2. Не вводьте свої особисті дані на ресурсах, у надійності яких ви не впевнені. Перш ніж ділитися інформацією про себе чи свою картку, запитайте себе: "Що це за сайт? Де я його знайшов? Чи довіряю я людині, яка дала мені посилання?". Якщо ви не впевнені, запитайте інших, чи знають вони про такий ресурс.

3. Використовуйте надійний пароль. Вони мають бути різними для різних облікових записів, тривалими та складними. По можливості слід використовувати двофакторну аутентифікацію.

4. Використовуйте надійну антивірусну програму.

5. Жодного російського і піратського програмного забезпечення - встановлюйте тільки програми з офіційних джерел.

6. Регулярно створювати резервні копії даних. Це дасть можливість відновити важливу інформацію в разі успішної кібератаки.

Після опрацювання різних статей, що містяться на сайті Держспецзв’язку, ми прийшли до висновку, що російські хакери ніколи не полишають спроб атакувати Україну та інші держави в цифровому просторі. Тому українці мають бути готовими до атак на свої комп'ютери й гаджети та знати базові правила цифрової безпеки і перш за все самостійно цікавитися новими можливостями збереження особистих даних та нести відповідальність за свою кібербезпеку.

Висновки до Розділу 3

У середовищі, де кіберзагрози продовжують з’являтися та розвиватися, ми не можемо залишатися осторонь: поточний стан світової інформаційної політики змушує нас постійно вдосконалювати наш підхід до боротьби з кіберзлочинністю, заохочуючи створення національних моделей, спрямованих на покращення національної кібербезпеки. Стрімкий розвиток інформаційних технологій є причиною розвитку кіберзлочинності. Вже сьогодні збитки, завдані віртуальними злочинцями в Україні, обчислюються десятками мільйонів гривень.

В умовах сучасних глобальних та регіональних інформаційних протистоянь, деструктивних комунікативних впливів, зіткнення різновекторних національних інформаційних інтересів, поширення інформаційної експансії та агресії, захист національного інформаційного простору та гарантування інформаційної безпеки стають пріоритетними стратегічними завданнями сучасних держав у системі глобальних інформаційних відносин. Збереження інформаційного суверенітету, формування ефективної системи безпеки в інформаційній сфері є актуальною проблемою і для України, яка часто є об’єктом зовнішньої інформаційної експансії, маніпулятивних пропагандистських технологій та руйнівного інформаційного вторгнення.

Міжнародні експерти вважають, що атаки кіберзлочинців у майбутньому будуть більш масовими не лише з метою заробити гроші чи шпигувати, а й з метою демонстрації влади. Забезпечення безпеки у кіберпросторі є актуальним для нашої країни сьогодні, оскільки проти неї ведеться повномасштабна війна, що виявляється, серед іншого, у кібератаках на державні органи та установи України, а також на критично важливу інфраструктуру. Зважаючи на це, держава загалом, та кожен свідомий громадянин зокрема, повинен приділяти велику увагу кібербезпеці, адже незважаючи на те, що розвиток технологій у сучасному світі не тільки дозволяє людству вирішувати багато проблем його постійної еволюції, він також приносить нові виклики та загрози у сфері віртуального кіберпростору.

Увага до проблем гарантування інформаційної безпеки України зумовлена антиукраїнськими впливами, які пропагують ідеї сепаратизму, насильства, національної ворожнечі і є спробами руйнування національної ідентичності України, знищення міжнаціональної злагоди, посягання на конституційний лад України, територіальну цілісність держави. Проблема гарантування інформаційної безпеки України так актуалізується в умовах повномасштабної війни, коли з боку Російської Федерації відбувається інформаційна експансія, упереджене та тенденційне висвітлення фактів та явищ, а технології російських інформаційно-психологічних операцій спрямовані на забезпечення домінування в українському (а також у глобальному) інформаційному просторі та на утримання медійної переваги. Через російські пропагандистські інформаційно-психологічні кампанії, акції, медіазаходи відбувається вплив не лише на суспільну свідомість громадян України, а й на світову громадськість.

Рішення комплексної проблеми інформаційної безпеки дасть змогу як захистити інтереси суспільства і держави, так і гарантувати права громадян на отримання всебічної, об’єктивної та якісної інформації.

ВИСНОВКИ

Таким чином, кіберзлочинність – це проблема, з якою стикається людство у 21 столітті. Незважаючи на всі заходи, вжиті окремими особами, компаніями або державою, кіберзлочинність продовжує своє поширення , збільшуючи прибутки злочинців та виснажуючи кишені простих громадян. Тому сьогодні особливо важливо переглядати всі існуючі заходи та активно розробляти нові, які приносять більшу користь та надійніший захист від кіберзлочинців.

Всупереч цьому, як ми з'ясували в процесі аналізу національного законодавства України, що регулює суспільні відносини, ми можемо стверджувати, що наша держава вживає необхідних заходів щодо запобігання та боротьби з комп'ютерною злочинністю.

Також ми дослідили світовий та вітчизняний досвід державної політики у протидії кіберзлочинності та визначили ключові аспекти розвитку інформаційної політики в України.

У роботі ми широко охарактеризували інформаційну політику в Україні та її нормативно-правове регулювання і дійшли висновку, що проблема запобігання та сприяння кіберзлочинності в Україні є комплексною. Закони сьогодні повинні відповідати вимогам сучасного стану розвитку техніки. Пріоритетним напрямом є також організація взаємодії та координація зусиль правоохоронних органів, спеціальних служб та судової системи, які забезпечують їх необхідною матеріально-технічною базою. Сьогодні жодна країна не в змозі самостійно боротися з кіберзлочинністю. Міжнародне співробітництво в цій сфері має терміново активізуватися. Експерти впевнені, що найближчим часом хакери стануть загрозою номер один і витіснять тероризм. Незважаючи на віртуальний характер злочинів, збитки, які вони завдають, цілком реальні.

Унаслідок унікального геополітичного розташування, багатства духовної та історичної спадщини українського народу, Україна має стати

інформаційно розвиненою державою, повноправним і впливовим учасником європейського життя, посісти гідне місце у глобалізованому світі, забезпечивши при цьому захист власного інформаційного простору від небажаного інформаційного впливу;захист національних зокрема державних інформаційних ресурсів; безпечне функціонування інформаційних та телекомунікаційних систем, зокрема тих, що функціонують в інтересах управління державою а також захист інформації, що циркулює в них.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Біленчук Д.П. Кібершахраї - хто вони? //Міліція України, 2016. № 7-8. С. 32-34

2. Боротьба зі злочинним використанням інформаційних технологій: Резолюція Генеральної Асамблеї ООН № 53/70 від 4 січня 2015 р. - С. 1-2.– режимдоступу:https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix. дата звернення: (11.06.2022)

3. Державна служба спеціального зв'язку та захисту інформації України https://uk.wikipedia.org/wiki дата звернення: (12.06.2022)

4. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 2014. 328 с. Режим доступу: http://old2.niss.gov.ua/content/articles/files/Dubov_mon89e8e.pdf дата звернення: (10.06.2022)

5. Заява Високого представника від імені Європейського Союзу щодо вторгнення в Україну збройних сил Російської Федерації https://www.eeas.europa.eu/node/111507_en. дата звернення: (10.06.2022)

6. Зупинити кіберзлочинність можна тільки разом.-// Україна: бізнес огляд №5-6 від 11.02.2013

7. Іванов В. Законодавство і журналістика. Формування правової бази в Україні та світовий досвід. К.: Школяр, 2014. 80 с.

8. Іванченко Ю М. Сутність, основні напрями та методи державної інформаційної політики в Україні // Державне управління: теорія і практика. 2005. № 2. С.15-18.

9. Інформаційна складова державної політики та управління: монографія / С. Г. Соловйов, О. Є. Бухт, Ю.В. Нестеряк [та ін.]; за зав.ред.Н.В.Грицяк; нац. академічний хвороба при Президентові України. К.: КІС, 2015. 319 с.

10. Інформаційне право: Підручник В. Я. Настюк (керівник), Л. П. Коваленко та ін .; для зав.ред.В.Я. Настюка, Л. П. Коваленко Харків: Право, 2016. 280 с.

11. Інформаційне суспільство: аналіз політичних аспектів зарубіжних концепцій: Монографія / Картунов О.В., Маруховський О.О.; за зав. ред. Картунов Олексій Васильович; Економіко-правовий коледж «КРОК». К.: Університет економіки та права «КРОК», 2012. 343 с.

12. Іноземцев В. Л., Кузнєцова Е. С. Атлас 2010. Le monde diplomatique / В. Л. Іноземці - М.: Центр дослідження постіндустріального суспільства, 2010. - 224 с.

13. Кібербезпека в інформаційному суспільстві: інформаційно-аналітичне резюме / відп. ред О.Довгань; Команда. О. Довгань, Л. Литвинова, С. Дорогих; НДІ інформатики та права НАПН України; Національна бібліотека України імені В. І. Вернадського. – К.: вид-во АртЕк, 2018. №1-12.

14. Князєв В., Бакуменко В. Філософсько-методологічні засади державно-управлінських рішень // Вісн. UADU. 2000. № 2. С. 341-344.

15. Коваленко Л. П. Теоретичні проблеми розвитку інформаційного права України: моногр. Х.: Право, 2012. 248 с.

16. Комп'ютерна злочинність та інформаційна безпека. А.П.Леонов; під загальною ред.А.П.Леонова. Мінськ: АРІЛ, 2000. 552 с.

17. Конвенції вище кіберзлочинності [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/main. дата звернення: (16.08.2022)

18. Конвенція про кіберзлочинність. Конвенцію ратифіковано із застереженнями та заявами Законом № 2824-IV від 09.07.2005 ВВР 2006 пп.5-6 ст.7 Конституція України: прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80. дата звернення: (10.09.2022)

19. Кохановська О. В. Правове регулювання у сфері інформаційних відносин: моногр. К .: Національна академія внутрішніх справ України, 2011. 212 с.

20. Кравцова М. О. Запобігання кіберзлочинності в Україні : монографія. Харків : Панов, 2016. 212 с

21. Красноступ Г. М. Основні напрями правового забезпечення державної інформаційної політики // Офіційний веб-сайт Міністерства юстиції України [Електронний ресурс] – доступ: http://old.minjust.gov.ua/30768. дата звернення: (10.09.2022)

22. Кримінальний кодекс України від 28 листопада 2019 року, підстави - 263-IX, 284- IX. [Електронний Ресурс] - режим Доступ: https://zakon.rada.gov.ua/laws/main/2341-14. дата звернення: (13.11.2022)

23. Крутських А. В. І. Л. Сафонова. Міжнародне співробітництво в регіоні інформативної безпеки – режим. Доступ: https://publications.lnu.edu.ua/bulletins/index.php/intrel/article/view/10365 дата звернення: (13.07.2022)

24. Ліпкан В. А. Національна безпека України: Навч. 2-й вид. К.: КНТ, 2009. 576 с.

25. Литвиненко О. Інформаційні технології та Україна в глобальному контексті // Люди і політика. 2001. № 1. С.10-17.

26. Лужецький В. А. Безпека інформації: Навч. Шлях. Вінниця: УНІВЕРСУМ-Вінниця, 2009. 240 с.

27. Манжай О. В. Використання кіберпростору в оперативно розшуковій діяльності. Право і Безпека. 2009. № 4. С. 215–219.

28. Мельник М. Сутність поняття «державна політика інформаційного суспільства»: узагальнення європейських та національних інтерпретацій // Науковий вісник «Демократичне управління». 2012. [Електронний Ресурс] – режим Доступ: http://www.lvivacademy.com/vidavnitstvo_1/visnik9/fail/Melnyk.pdf дата звернення: (13.07.2022)

29. Мережі та мережеві війни: майбутнє терору, злочинності та бойових дій / за ред. Дж. Арквілі, Д. Ронфельдта; перев. з англ. А. Іщенко. К.: Вид Хаус. «Києво-Могилянська академія», 2005. 350 с.

30. Моїсеєв Н. Інформаційне суспільство як етап нової історії // Вільне мислення. 2016. № 1. С. 81–83.

31. Москаленко А., Губерський Л., Іванов В. Основи масової інформаційної діяльності. К., 2014. 71 с.

32. Нікуленко Д. Кібербезпека: слабкі моменти // Юридична газета. 14 травня 2019 р. [Електронний ресурс] – Режим доступу: http://yurgazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html дата звернення: (13.07.2022)

33. Нестеряк Ю. В. Нормативно-правові основи державної інформаційної політики України в умовах розвитку інформаційного суспільства // Теорія і практика державного управління. 2016. С. 111-119

34. Окінавська хартія про глобальне інформаційне суспільство. [Електронний Ресурс] - режим Доступ: https://zakon.rada.gov.ua/laws/show/998_163 дата звернення: (13.07.2022)

35. Організаційно-правове забезпечення захисту від кримінальних правопорушень із застосуванням інформаційних технологій: наук.-практ. Шлях. / [В.М. Болгов, Н.М. Гадіон, О.З.Гладун та ін.]. К .: Національна академія прокуратури України, 2015. 202 с.

36. Оксфордський тлумачний словник англійської мови [Електронний ресурс]. – Режим доступу: http://www.oxforddictionaries.com/definition/english/hacker дата звернення: (14.06.2022)

37. Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України https://cip.gov.ua/ua дата звернення: (15.08.2022)

38. Пахнін М. Л. Принципи, завдання та інструменти державної інформаційної політики України в сучасних умовах // Теорія і практика державного управління. 2014. с.1-9.

39. Перша світова кібервійна https://www.unian.ua/techno/persha-svitova-kiberviyna-yak-ukrajina-boretsya-na-drugomu-fronti-11998566 дата звернення: (13.06.2022)

40. Петровський О.М., Лівчук С.Ю Проблеми боротьби з кіберзлочинністю: міжнародний досвід та українські реалії «YoungS cientist» № 12.1 (76.1) грудень, 2019

41. Погорецький М. Кіберзлочинність: визначення поняття // Вісник прокуратури. 2012. № 8. С. 89–96.

42. Пожуєв В. І. Формування державної інформаційної політики в умовах глобалізації // Гуманітарний вісник Запорізької державної інженерної академії. 2016. С. 4-12

43. Політологія. Підручник Ю. В. Ірхін, В. Д. Зотов, Л. В. Зотова. М.: Юрист, 2012. 511 с.

44. Про авторське право та суміжні права: Закон України від 04.11.2018р. № 5142. [Електронний Ресурс] – режим Доступ: https://zakon.rada.gov.ua/laws/show/3792-12 дата звернення: (13.09.2022)

45. Про адміністративні послуги: Закон України від 6 вересня 2013 р. № 5203-VI [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/52 03-17 дата звернення: (19.06.2022)

46. Проблеми української політики: Аналіз доповідей Інституту політичних та етнонаціональних досліджень. І. Ф. Кураса НАН України. К .: ІПіЕНД імені І. Ф. Кураса НАН України, 2010. 410 с.

47. Про Доктрину інформаційної безпеки України: Указ Президента України від 07.08.09 № 514/2009 // Офіційний вісник України. № 52. 2009.

48. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 1 лютого 1993 р. №5412. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2782-12 дата звернення: (14.06.2022)

49. Про електронні довірчі послуги: Закон України від 5 жовтня 2017 р. № 852-IV. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/21 55-19 дата звернення: (14.06.2022)

50. Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 р. № 851-IV. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/851-15 дата звернення: (21.04.2022)

51. Про затвердження Концепції розвитку електронного урядування в Україні: постанова Кабінету Міністрів України від 13 грудня 2010 р. № 2250-р. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/go дата звернення: (21.04.2022)

52. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі: Указ Президента України від 31 лип. 2000 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/92 8/2000 дата звернення: (21.10.2022)

53. Про заходи щодо удосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Постанова РНБО від 28 р. Квітень 2014. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/n0004525-14 дата звернення: (21.04.2022)

54. Про інформаційні агентства: Закон України від 01.06.1992 №7415 [Електронний Ресурс] - режим Доступ: https://zakon.rada.gov.ua/laws/show/74/95-%D0%B2%D1%80 (дата звернення: (21.04.2022)

55. Про інформацію: Закон України від 21 січня 1992 р. [Електронний ресурс] - режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: (20.04.2022)

56. Про національну безпеку України: Закон України від 21.06.2018 № 964-IV [Електронний Ресурс] – режим Доступ: https://zakon.rada.gov.ua/laws/show/2469-19#n355 (дата звернення: 17.10.2022)

57. «Про основні засади кібербезпеки України»: Закон України від 5 жовтня 2017 р. № 2163-VIII. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19/conv (дата звернення: 19.10.2022)

58. Про постанову Ради національної безпеки і оборони України від 6 травня 2015 р. «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 р. № 287/2050. [Електронний Ресурс] - режим Доступ: https://zakon.rada.gov.ua/laws/show/287/2015 (дата звернення: 18.08.2022)

59. Про порядок повідомлення засобами масової інформації про діяльність органів державної влади та місцевого самоврядування в Україні: Закон України відвід 23.09.1997 № 539 / 97- bp [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show (дата звернення: 11.11.2022)

60. Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність щодо криміналізації расистських та ксенофобських дій, вчинених через комп'ютерні системи: Закон України від 21 липня 2006 р. № 23-V. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua (дата звернення: 14.06.2022)

61. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7 вересня 2005 р. № 2824-IV. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2824-15 (дата звернення: 09.05.2022)

62. Про рекламу: Закон України від 3 липня 1996 р. №5841. [Електронний Ресурс] – режим Доступ: https://zakon.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80 (дата звернення: 16.06.2022)

63. Про стимулювання розвитку цифрової економіки в Україні: Закон України Документ 1667-IX, чинний, поточна редакція — Прийняття від 15.07.2021. [Електронний ресурс] – режим доступу: https://zakon.rada.gov.ua/laws/show/1667-20#Text (дата звернення: 10.05.2022)

64. Про суспільне телебачення і радіомовлення України: Закон України від 17 квітня 2014р. № 1452. [Електронний ресурс] – режим доступу: https://zakon.rada.gov.ua/laws/show/1227-18 (дата звернення: 06.04.2022)

65. Про телебачення і радіо: Закон України від 21.12.1993 № 3759-XII. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/3759-12 (дата звернення: 07.04.2022)

66. Прохоренко В. Кіберзлочинність стає актуальним поняттям для України – НБУ. - //Економічна правда від 26.02.2013.

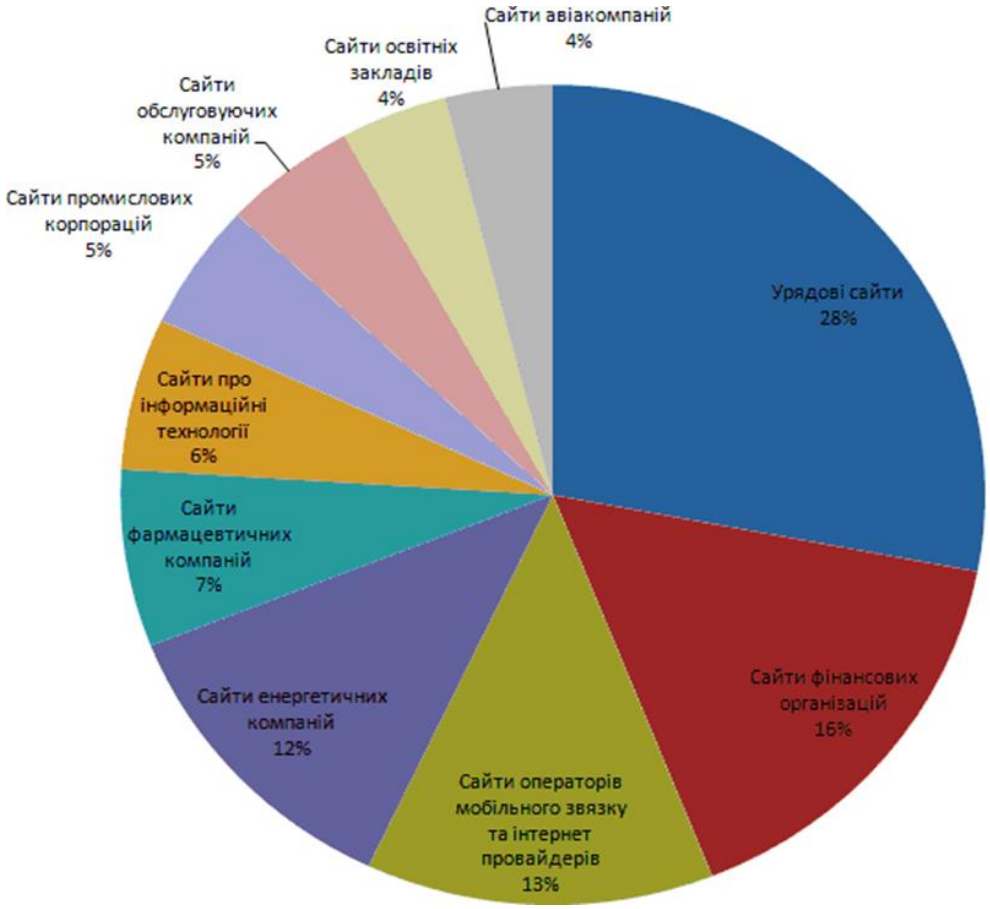
67. Україна та США стали першими у списку жертв кібератак // 24 канал – 2015 [Електронний ресурс]. - Режим доступу : http://24tv.ua/ukrayina/ukrayinata_ssha_stali_pershimi_u_spisku_zhertv_kiberatak/n565572 (дата звернення: 07.04.2022)

68. Україна – осередок кібератак [Електронний ресурс] - Режим доступу: https://scienceukraine.in.ua/sciblogs/ukraina-v-fokusi-kiberatak (дата звернення: 06.04.2022)

ДОДАТКИ

Додаток А

Компонентна структура веб-сайтів, які зазнали кібератак у 2014 році



Додаток Б

Показники країн із найбільш частими випадками кіберзлочинності