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

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ Н.Ф.Ржевська
«_____»_____ 20__р.

ДИПЛОМНА РОБОТА

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

ЗА СПЕЦІАЛЬНІСТЮ 291 «МІЖНАРОДНІ ВІДНОСИНИ, СУСПІЛЬНІ КОМУНІКАЦІЇ ТА РЕГІОНАЛЬНІ СТУДІЇ»

ЗА ОСВІТНЬО-ПРОФЕСІЙНОЮ ПРОГРАМОЮ «МІЖНАРОДНА ІНФОРМАЦІЯ»

Тема: «Кіберзлочинність як виклик державній інформаційній політиці»

Виконавець: студент 2 курсу, 208 групи, Харін Сергій Олегович

Керівник: доцент кафедри міжнародних відносин, інформації та регіональних студій, к. іст. н. Дерев'янко Ігор Петрович

Нормоконтролер: _____ _____
(підпис) (П.І.Б.)

КИЇВ 2020

ЗМІСТ

ВСТУП

Актуальність теми дослідження. На сучасному етапі становлення і розвитку інформаційного суспільства процес інформатизації є глобальним, всеохоплюючим, що проникає в усі сфери суспільного життя. Він перетворюється в один з основних чинників суспільного розвитку і багато в чому характеризує сучасну соціальну динаміку. Завдяки процесу інформатизації в суспільстві відбуваються системні зміни, відповідно до яких і всі сегменти суспільства, і кожна людина включаються в глобальний інформаційний простір, стаючи при цьому елементами глобальної інформаційної системи і, відповідно, в тій чи іншій мірі залежними від неї.

Зазначена інформаційна залежність стосується всього світу в цілому, всіх держав і людей, що беруть участь в процесі виробництва, зберігання та використання інформації в ході інформаційного обміну та інформаційної взаємодії. Інформаційна взаємодія вже стала планетарним фактором, створивши цілий ряд соціальних трансформацій і ввівши в систему соціальних відносин такі процеси, як інформаційні війни, інформаційна зброя, інформаційний тероризм, інформаційна злочинність і інформаційна безпека тощо.

Сучасні соціальні практики показують, що суспільний розвиток на основі глобальної інформатизації створює якісно нові виклики, загрози і ризики інформаційної безпеки. Ця обставина робить актуальним дослідження інформаційної безпеки.

В процесі інформаційної глобалізації в світі фактично виник єдиний інформаційний простір, який призвів до уніфікації інформаційних і телекомунікаційних технологій всіх країн – суб'єктів інформаційного суспільства. Поява загальносвітового інформаційного простору з неминучістю спричинило видозміну елементів політичної системи. Зокрема, поряд з появою нових політичних акторів і трансформацією традиційних політичних інститутів виникли нові форми політичної боротьби, механізми і способи політичного впливу. В результаті в структурі політичної системи позначилися тенденції масштабного ускладнення ряду її підсистем, і перш за все політичної комунікації.

Висока ефективність засобів інформаційного впливу, широкий спектр їх застосування і прихованість впливу є причинами пильного інтересу вчених багатьох країн до досліджень в області розробки теорії і практики застосування інформаційної зброї і, як наслідок, теорії ведення інформаційних війн. Зростання в цих умовах теоретичної актуальності і практико-політичної значущості проблематики забезпечення національної безпеки в цілому і, зокрема, інформаційної безпеки політичної комунікації України зумовило вибір теми дослідження.

Відомо, що питання інформаційної безпеки, захисту комп'ютерної інформації, забезпечення захищеності відомостей, що утворюють охоронювану законом таємницю, та інші подібні проблеми викликають серйозну заклопотаність як в Україні, так і в усьому світі. Дані питання безпосередньо пов'язані із забезпеченням національної безпеки держав, захистом конституційних прав і свобод людини і громадянина. Необхідність вдосконалення державної політики щодо протидії злочинам у сфері інформаційних технологій підтверджується тим, що останнім часом дані злочини стали глобальною міжнародною проблемою, багато з цих злочинів мають транскордонний характер.

Результати дослідження спеціальної літератури свідчать, що на цей момент існує досить велика кількість робіт, в яких розглядаються окремі аспекти боротьби з кіберзлочинністю. Зокрема, цій проблематиці присвячено роботи Д. С. Азарова, Ю. М. Батуріна, П. Д. Біленчука, В. М. Бутузова, Д. В. Пашнєва, В. С. Цимбалюка, В. П. Шеломенцева та ін. Проблемам боротьби з інформаційними злочинами в сучасному суспільстві присвячені дослідження В.М. Боєр, В.П. Іванського, Ю.В. Калініної, Р. Клебанова, С.Н. Кпенова, М.Ю.Костенко, С.В. Кузьміна, П.У. Кузнєцова, А.А. Левіна, С.І. Ушакова, А.С. Шийко.

Разом з тим проблема інформаційної безпеки системи політичної комунікації досі залишається у вітчизняній політичній науці маловивченою і потребує свого подальшого комплексного дослідження.

Об’єкт – державна інформаційна політика

Предмет – кіберзлочинність, як виклик. Суть особливості кіберзлочинності серед викликів державної інформаційної політики.

Мета роботи – визначити кіберзлочинність, як виклик щодо державної інформаційної політики, а також встановити заходи протидії кіберзлочинності на міжнародному та національному рівнях.

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

- визначити сутність та принципи реалізації державної інформаційної політики;
- дослідити кіберзлочинність як явище та його передумови виникнення, розвиток;
- вивчити світовий та вітчизняний досвід державної політики у протидії кіберзлочинності;
- проаналізувати механізми та принципи реалізації державної політики у сфері кібербезпеки;
- надати практичні рекомендації щодо моделі попередження кібрезлочинності.

Методологія і методика дослідження. Методолічна база дослідженння зумовлена поставленою метою і особливостями його предмету, грунтується на використанні діалектичного методу вивчення соціальних процесів і явищ. Характер поставлених дослідницьких завдань визначив необхідність використання також таких методів, як порівняльно-історичний, порівняльно-правовий, метод системного аналізу і конкретно-соціологічний метод.

Джерельну базу для дослідження склали:

Основні документи з питань попередження кіберзлочинності в міжнародній сфері:

- Окінавська хартія інформаційного суспільства 2000 року;
- Європейська конвенція з кіберзлочинів від 2001 року;
- Резолюція ООН щодо попередження злочинності та кримінального правосуддя;
- Конвенція про забезпечення міжнародної інформаційної безпеки (концепція).

Структура роботи визначається метою та завданнями дослідження. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи – 94 сторінки, з них основного матеріалу – 81 сторінка.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ

1.1. Державна інформаційна політика: суть та принципи реалізації

В умовах формування глобального інформаційного простору, найважливішим компонентом життєдіяльності та об'єктом державного управління в суверенній державі стає інформаційна сфера. Інформаційна сфера – це сукупність усього обсягу інформації, об'єктів інформаційної інфраструктури, суб'єктів, які здійснюють збір, формування, розповсюдження і використання інформації, а також системи регулювання виникаючих при цьому суспільних відносин. Ця сфера становить матеріально-технічну основу інформаційного суспільства. Розвиток інформаційних і телекомунікаційних технологій змушує розглядати її як елемент в системі соціального управління [7, с. 104].

Особливе значення цього об'єкта управління визначається тим, що інформація є основою для розвитку особистості кожного члена суспільства, взаємодії між членами суспільства, формування громадянського суспільства і його інституційних структур. Без обміну інформацією неможливий розвиток ні соціальної, ні економічної, ні політичної сфер життя суспільства. У зв'язку з цим, умовою сталого розвитку держави, збереження його єдності й цілісності є рівень ефективності організації інформаційної взаємодії між громадянським суспільством і державною владою, між адміністративно-територіальними та національними утвореннями, між структурами влади. Інформація є вихідним ресурсом для розробки державної політики та здійснення державного управління в будь-якій сфері життєдіяльності суспільства і держави.

Державна інформаційна політика – діяльність системи державної влади і управління по створенню умов для успішного, стійкого і безперервного розвитку системи соціально-політичних відносин суспільства в умовах інтенсивного впливу зовнішніх і внутрішніх факторів, що здійснює як стабілізуючий, так і деструктивний інформаційно-психологічний вплив на систему.

Ефективність державної інформаційної політики – здатність державної інформаційної політики забезпечити:

- успішність розвитку системи соціально-політичних відносин суспільства, тобто отримання системою нових якостей в оптимальні (з точки зору безперервності процесу розвитку системи) терміни з мінімальними витратами матеріальних та інтелектуальних ресурсів;
- безперервність процесу розвитку системи соціально-політичних відносин суспільства;
- стійкість процесу розвитку системи соціально-політичних відносин суспільства по відношенню до впливу зовнішніх деструктивних факторів і процесів;
- незворотність процесу розвитку системи соціально-політичних відносин суспільства, тобто набуття в процесі розвитку нових якостей, які раніше в системі були відсутні, і гарантія колишніх якостей, втрачених системою в процесі її розвитку;
- інтенсивність процесу розвитку системи соціально-політичних відносин суспільства, тобто здатність системи підтримувати методами внутрішнього регулювання необхідний темп (інтенсивність) власного розвитку для набуття системою нових якостей, що мають для неї життєво важливе значення (в першу чергу – якостей, що забезпечують подальший розвиток системи).

Інформаційна політика як засіб впливу влади на суспільство за допомогою поширення масової інформації, що забезпечує механізм функціонування всієї соціально-політичної системи, вимагає серйозного переосмислення. Це пов'язано з масштабною трансформацією соціально-політичних відносин в Україні, з військоювю агресією на сході України з боку Росії, з прагненням наукової спільноти зрозуміти, якими якостями повинна відрізнятися масова інформація в умовах глобалізації світового інформаційного простору [13, с. 25].

Очевидно, що національна інформаційна політика повинна забезпечувати сталий розвиток країни на основі принципу відкритості та гласного обговорення всіх проблемних питань. Поза цими умовами Україна, як і раніше, ризикує залишитися в ролі «наздоганяючої» країни. При відсутності такої політики, яка створюється з

урахуванням інтересів влади і суспільства, залишається ймовірність того, що відносини між цими сторонами виявляться односторонніми (побудованими за принципом «згори вниз») і ніколи не перейдуть в русло конструктивного діалогу. Це не означає, що інформаційна політика може реалізовуватися тільки в країнах з розвиненими політичними інститутами, громадянським суспільством і законодавчо гарантованими свободами в галузі засобів масової інформації.

Однак в автократичних державах, де знижені можливості плюралістичного мислення і цивільних ініціатив, інформаційна політика найчастіше залежить від волі одного або обмеженого числа осіб і не гарантує розвиток суспільства на основі шанобливого ставлення сторін одна до одної. Звернена на всіх членів суспільства національна інформаційна політика сама по собі не забезпечує більш високі економічні показники розвитку тієї чи іншої держави. Однак, як показує сучасна міжнародна практика, країни, де досягається консенсус взаємодії влади і суспільства, демонструють стабільні результати свого розвитку в цілому, створюють соціальні гарантії своїм громадянам, в тому числі гарантію на висловлення своєї думки в ЗМІ з найгостріших питань.

Таким чином, проведену інформаційну політику в національному масштабі людина схильна сприймати як своєрідний барометр загальнополітичного курсу. Розглядаючи інформаційну політику в рамках цілісної політики, необхідно зробити застереження: остання сприймається, перш за все, стосовно соціальної діяльності, яка визначається відповідальністю владних інститутів за реалізацію прав громадян, з урахуванням базових цінностей життя всього суспільства. Це сприйняття в певній мірі носить ідеалістичний характер, оскільки в повсякденному житті нерідко виникає дисбаланс між потребами влади і суспільства [23, с. 25].

Однак прагнення до консенсусу між державними структурами і суспільством, як зазначалося вище, є сьогодні очевидним в більшості найбільш розвинених в економічному відношенні країн, які гарантують своїм громадянам реалізацію їх основних політичних і соціальних прав. Необхідність існування цього консенсусу береться за основу і при оцінці можливостей здійснення інформаційної політики в Україні.

Визнаючи недосконаліть політичних і правових норм, що реалізуються сьогодні в нашій країні, тим не менше ідея громадянської активності населення, без якої позначена вище інформаційна політика відбутися не може, починає поступово поширюватися на суспільну свідомість і розвивати громадські ініціативи. Це проявляється не тільки в формі активних політичних протестів, але і в більш усвідомленому, ніж ще кілька років тому, прагненні громадян до відстоювання своїх соціальних, юридичних прав в рамках локальних конфліктів і протиріч, в бажанні консолідувати свої інтереси на користь виконання «малих справ», важливих для повсякденного буття людей.

Інформаційне забезпечення діяльності системи органів державної влади, її своєчасне забезпечення достовірною інформацією є найважливішою умовою сталого та ефективного функціонування державного механізму, реалізації всіх стадій процесу державного управління, адекватного цілям і задачам розвитку і задоволення насущних потреб суспільства. Крім того, в умовах переходу до інформаційного суспільства держава не може претендувати на гідне місце у світовій спільноті не приділяючи особливої уваги інформаційній сфері і не проводячи активну цілеспрямовану державну інформаційну політику як всередині країни, так і на міжнародному рівні [16].

Таким чином, розробка і реалізація державної інформаційної політики (ДІП), що відповідає потребам та інтересам суспільства, та її практична реалізація шляхом ефективного державного регулювання інформаційної сфери є актуальною комплексною проблемою державного управління.

У зв'язку з цим необхідне теоретичне обгрунтування самого поняття «державна інформаційна політика». Наприклад, така міжнародна організація, як ЮНЕСКО бачить мету інформаційної політики в тому, щоб «дати право всім громадянам суспільства на доступ і використання інформації і знань». При цьому акцентуються вигоди для суспільства від такого широкого підходу: «Вигоди від інформації для громадського доступу легше описати в неекономічних визначеннях. Для інформації, виробленої урядами, можливо, найбільша неекономічна цінність, пов'язана з розміщенням інформації для громадського доступу, – прозорість управління і

просування демократичних ідеалів. Надмірна секретність створює тиранію. Відкрите і необмежене поширення громадської інформації також підвищує громадське здоров'я і безпеку, і загальний соціальний добробут, оскільки громадяни приймають більш інформативні рішення щодо свого життя, навколишнього середовища і майбутнього» [93].

Науковець В. Роговець трактує її як здатність і можливість суб'єктів політики впливати на свідомість, психіку людей, їх поведінку і діяльність в інтересах держави і громадянського суспільства за допомогою інформації [73, с. 10]. В даному випадку акцентується увага на управлінському аспекті інформаційної політики, з урахуванням того, що інформація вже стала невід'ємним атрибутом соціального управління. Відповідно до цього формування інформаційної політики як системи управління інформаційними процесами і ресурсами сприймається як запорука економічного добробуту та безпеки країни [73, с. 11].

Запропоновану В. Роговцем інтерпретацію інформаційної політики можна сприйняти як найбільш раціональний варіант. Перш за все тому, що придушення психіки людей неминуче веде до посилення конфліктності як такої і, по суті, до заперечення в яких би то не було формах політичної дискусії. В даному випадку можна говорити лише про інформаційну політику, засновану на приниженні значущості одних суб'єктів політичної взаємодії на догоду іншим, що є антиподом паритетних відносин між владою і суспільством. Ось чому таку політику не можна прийняти як соціально відповідальну, націлену на формування громадянських відносин в суспільстві.

Більш зважені оцінки від М. Мельник, який стверджує, що інформаційна політика є окремим напрямком державної політики, що охоплює не тільки регламентацію діяльності з управління інформаційними ресурсами, розвитку інформаційно-комунікативної сфери і оптимізації взаємодії із засобами масової інформації, а й інформаційне забезпечення діяльності влади у всіх сферах суспільного життя [39].

Це судження представляється також і більш перспективним для з'ясування суті досліджуваного питання, тому що в контекст розвитку інформаційної політики

включена вся інформаційно-комунікативна сфера, а не тільки механізм інформаційного управління, що створюється владою для задоволення своїх інтересів. Запропоноване О. Литвиненко сприйняття інформаційної політики дозволяє трактувати її як стратегію і одночасно сферу повсякденної діяльності, засновану на діалогових відносинах між суб'єктами політичної діяльності [37, с. 10].

Державну інформаційну політику, – пише Ю. Іванченко – слід розглядати як сукупність цілей, що відображають національні інтереси в інформаційній сфері, стратегій, тактик, завдань державного управління, управлінських рішень і методів їх реалізації, що розробляються і реалізуються державною владою для регулювання і вдосконалення як власне процесів інформаційної взаємодії в усіх сферах життєдіяльності суспільства і держави, так і процесів забезпечення такої взаємодії. Вибір тієї чи іншої державної інформаційної політики – політичний акт. Таке політичне рішення, яке має довгострокове політичне значення для розвитку країни, повинне прийматися на найвищому рівні [24, с. 15].

Автор Ю. Іванченко виділяє наступні завдання державної влади з вироблення державної інформаційної політики:

- формування концепції;
- забезпечення нормативно-правового регулювання;
- організаційно-технологічне забезпечення процесів державного регулювання інформаційної сфери [24, с. 17].

Об'єктами ДІП вчений визначає:

- друковані засоби масової інформації (газети, журнали, книговидання);
- електронні засоби масової інформації (телебачення, радіо, Інтернет);
- засоби зв'язку;
- інформаційне право;
- інформаційна безпека.

Як предмет інформаційної політики ним називаються тенденції, закономірності розвитку інформаційної сфери, суспільних інформаційних відносин, інформаційних

процесів, методи аналізу і прогнозу їх розвитку, виявлення ефекту впливу ЗМІ на масову свідомість, на громадянське суспільство і державу [22, с. 18].

Мета інформаційної політики – забезпечення інформаційної безпеки громадян і країни; інформаційно-аналітичний супровід державної політики, доведення прийнятих державою рішень, програм до населення як головного масового суб'єкта управління.

Основними цілями державної інформаційної політики є:

- розвиток орієнтованого на інтереси людей, відкритого правового інформаційного суспільства, в якому у кожного була б можливість створювати інформацію і знання, мати доступ до них;
- використання потенціалу інформації для досягнення цілей соціально-економічного та культурного розвитку країни, підвищення якості життя людей;
- зміцнення єдиного інформаційного простору країни, мінімізація регіонального «цифрового розриву» на базі інформаційної інтеграції регіонів;
- подолання «цифрового розриву» між різними групами і верствами суспільства [33, с. 25].

Досягнення цих цілей повинно здійснюватися на основі наступних принципів державної інформаційної політики:

- поширення і використання інформації і знань у всіх сферах життєдіяльності для забезпечення гармонійного, справедливого і рівноправного розвитку людини;
- універсальність, неподільність і взаємозв'язок всіх прав людини і основних свобод, включаючи право на інформацію;
- сприяння культурному і мовному різноманіттю;
- підвищення рівня безпеки інформації;
- створення сприятливого середовища для розвитку інформаційної діяльності;
- забезпечення незалежності, плюралізму і різноманітності форм поширення масової інформації;
- розвиток людського потенціалу в області створення і використання інформації;

- використання науково-технічних досягнень і потенціалу інформаційно-комунікаційних і мультимедійних технологій для розвитку інформаційної діяльності;
- сприяння регіональному та міжнародному співробітництву в інформаційній сфері.

На думку І. Драч, інформаційна політика побудована на діях трьох суб'єктів. Це політика як така, державна влада (в особі трьох основних її гілок – виконавчої, законодавчої та судової), ЗМІ, чия діяльність базується на функціонуванні різних видів масової інформаційної діяльності – журналістики, PR, реклами, і суспільство – в особі груп за інтересами, інститутів і партій [17, с. 103].

Таким чином, інформаційна політика є складним поняттям і побудована на врахуванні інтересів усіх суб'єктів політичного простору. На основі цього циркулюють і базові інформаційні потоки. Інформаційна політика, крім того, враховує положення ЗМІ в суспільстві, яке визначається історичними закономірностями їх еволюції, особливостями їх взаємодії з державними структурами, політичними інститутами і суспільством в цілому, а також правовими та етичними нормами, що діють у сфері масової інформації.

Інформаційну політику слід сприймати як цілеспрямовану взаємодію політики, правового забезпечення, організаційних заходів з боку держави і єдиних, поділюваних суспільством і журналістським співтовариством принципів здійснення діяльності ЗМІ [18, с. 119].

Зазначений вище принцип прийняття різних підходів до інформування якраз і дозволяє налагодити діалог суб'єктів політики, що є основою побудови ефективних відносин між владою і суспільством в сучасній державі. Саме такі відносини, на наш погляд, здатні уберегти країну від революційних потрясінь і (або) загострення соціальної конфліктності.

Головними напрямами та способами державної інформаційної політики в Україні є:

- розвиток інформаційного простору України;
- створення системи державних стратегічних комунікацій;

– інформаційна реінтеграція тимчасово непідконтрольних територій Луганської та Донецької областей, а також тимчасово окупованої території Криму;
– популяризація України та її цінностей у світі.

Модель, зазначена на Рис.1.1, дозволяє уникнути ризиків (фінансових втрат від неповної і нескоординованої експлуатації інформації, втрачений час, невдачі інновацій і втрати репутації; забезпечити прозорість процесу, високу продуктивність використання інформаційних технологій.

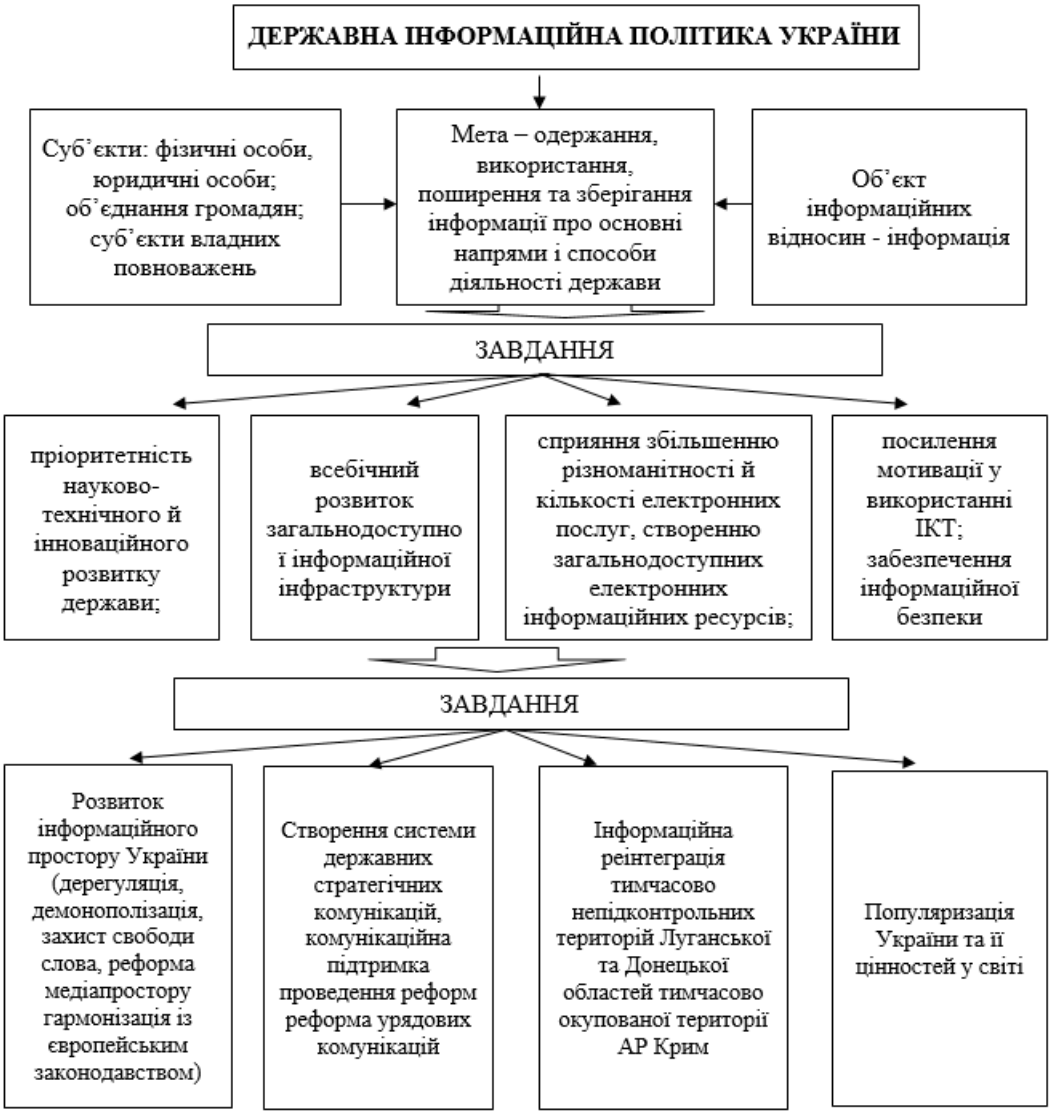


Рис. 1.1. Модель реалізації державної інформаційної політики України [17, с. 104]

Ефективність державної політики залежить від концептуального базису, що визначає перспективи розвитку конкретної сфери життєдіяльності суспільства і держави; законодавчого закріплення правил, умов та необхідних обмежень діяльності в певній сфері; організаційного, технологічного, фінансового забезпечення.

1.2. Інформаційна політика в структурі політики держави

Серед глобальних тенденцій розвитку світового співтовариства відбувається зростання значення інформації і знань. Інформація є однією з базових людських потреб і фундаментом будь-якої соціальної організації. Вона є сьогодні найважливішим ресурсом для досягнення цілей соціально-економічного розвитку країни в цілому, включаючи державне управління, підприємництво, охорону здоров'я, освіту, доступне житло, розвиток сільського господарства, охорону навколишнього середовища та запобігання катастроф, успішну боротьбу з екстремізмом і тероризмом.

Україна, як частина світової цивілізації, знаходиться на шляху становлення інформаційного суспільства, яке надає необхідні можливості по створенню і використанню інформації і знань, розширенню людських комунікацій, призводить до формування нової інформаційної, інноваційної економіки – найважливішого чинника стійкого підвищення добробуту людей.

Разом з тим, процеси глобалізації інформаційних ринків, недоступність всього обсягу необхідної інформації, особливо в мережі Інтернет, для більшості українських громадян, монополізм на внутрішніх ринках інформаційних послуг, обмеженість, низька якість масової інформації, порушення прав авторів, а також проблеми інформаційної безпеки вимагають від держави більшої уваги до формування та реалізації державної інформаційної політики. З огляду на перехідний характер процесів соціально-економічного розвитку в країні, успішно вирішувати зазначені проблеми можна тільки за участю держави. Вона повинна визначити свої пріоритети і напрямки діяльності в інформаційній сфері [22, с.58].

Необхідність розробки стратегії державної інформаційної політики визначається також потребою в координації зусиль органів влади, приватного сектору та громадянського суспільства, всіх учасників інформаційної діяльності зі створення умов розвитку інформаційного суспільства, підвищення рівня і якості використання інформації. Підвищення ефективності інформаційної діяльності на базі відповідної державної політики може стати потужною рушійною силою зростання конкурентоспроможності української економіки, створення нових робочих місць, а головне – поліпшення якості життя для всіх громадян. Розвиток інформаційного виробництва має забезпечити в економіці країни збалансованість ефекту від використання сировинних ресурсів і інтелектуальних ресурсів.

Особливі умови реалізації державної інформаційної політики - умови, в яких державна інформаційна політика не здатна в повній мірі забезпечити хоча б одну з умов власної ефективності за допомогою наявних на даний момент в її розпорядженні інструментів і механізмів політичного регулювання. [22, с.63].

Особливі умови – потенційно небезпечні для суб'єкта глобальні і довгострокові зміни стану зовнішнього середовища існування даного суб'єкта, що відбуваються переважно під впливом факторів зовнішнього середовища, які від суб'єкта (і його дій) практично не залежать. Подальше існування і сталий розвиток суб'єкта в особливих умовах можливо тільки при адекватній адаптації до них його системної структури і дій.

До особливих умов можна віднести тільки ті соціальні явища і процеси, які призводять до докорінних змін системи соціально-політичних відносин суспільства, які, в свою чергу, вимагають зміни державної інформаційної політики на концептуальному рівні. Поява таких умов призводить до виникнення нової галузі державної інформаційної політики – інформаційної політики в особливих умовах, мета якої – методом неминучих проб і помилок виробити правові механізми та інструменти правового регулювання, що дозволяють системі соціально-політичних відносин суспільства ефективно пристосуватися до нових зовнішніх умов, не знижуючи при цьому темпу і якості свого розвитку.

У сучасному суспільстві до особливих умов реалізації інформаційної політики відносяться:

- формування інформаційного суспільства;
- політична, соціальна, культурна, інформаційна, психологічна глобалізація;
- геополітична конкуренція в інформаційно-психологічному просторі;
- інформаційно-психологічна війна.

Процес формування глобального інформаційного суспільства, як особлива умова реалізації державної інформаційної політики, полягає в невідповідності темпів реагування організаційної та нормотворчої діяльності системи державних органів влади з модернізації державної інформаційної політики тих змін, які відбуваються в системі соціально-політичних відносин в процесі формування інформаційного суспільства.

Така невідповідність у швидкості розвитку системи державної інформаційної політики та системи соціально-політичних відносин сучасного суспільства, яке виражається, зокрема, в тому, що цілі сфери соціальних відносин в інформаційно-психологічному просторі неохвачени державним регулюванням, призводить до того, що деякі функції державного регулювання починають виконувати об'єкти державної інформаційної політики, такі як ЗМІ, в сучасних умовах справедливо називають «четвертою владою».

Політична, соціальна, культурна, інформаційна, психологічна глобалізація може бути віднесена до категорії особливих умов реалізації державної інформаційної політики в силу наступних основних причин.

В умовах відставання від провідних країн світу в темпах розвитку національного сегмента інформаційно-психологічного простору, виробництва знань-рішень і генерації високих технологій держава потрапляє в інформаційну залежність від країн-виробників інформаційних ресурсів і стає об'єктом політики інформаційного неоколоніалізму. Сучасна інформаційна політика не в змозі ефективно протистояти цьому негативному соціальному явищу, оскільки правове поле інформаційної політики на сучасному етапі розвитку здатне виявляти і давати юридичну кваліфікацію лише непрямим проявам і слідах діяльності держав –

інформаційних домінантів, послідовно проводять по відношенню до інших держав політику інформаційного неоколоніалізму. [23, с.21].

Геополітична конкуренція в інформаційно-психологічному просторі може бути віднесена до категорії особливих умов реалізації державної інформаційної політики в силу наступних причин:

- геополітична конкуренція в інформаційно-психологічному просторі пов'язана з виникненням нових принципів, пріоритетів та форм політичної боротьби, які не охоплюються і практично не регульованих існуючими нормами міжнародного права і національного законодавства;
- прихованість природи протікання інформаційно-психологічних процесів ускладнює регулювання даної категорії соціальних відносин інформаційним правом;
- відсутність міжнародного законодавства, що регулює зростання геополітичних суб'єктів в інформаційно-психологічному просторі, і, в першу чергу, правових норм і механізмів, що уповільнюють або перешкоджають формуванню геополітичних суб'єктів, спеціально створюваних для агресії по відношенню до інших держав, є причиною високої гнучкості і швидкості формування і зміни складу союзів і коаліцій в інформаційно-психологічному просторі, більшість з яких мають віртуальний характер і не вивчається діючої інформаційною політикою в якості предмета правового регулювання;
- можливість безконфліктного (з точки зору традиційного права) поєднання принципів мирного співробітництва і агресивного протиборства в зовнішній політиці суб'єкта геополітичної конкуренції по відношенню до одного й того ж суб'єкту геополітичних відносин призводить, при розгляді інформаційного протиборства в рамках чинного міжнародного права, до виникнення численних юридичних колізій;
- широке поширення практики використання в мирний час арсеналу сил, засобів і методів інформаційно-психологічної війни в політичних цілях відбувається, в першу чергу, завдяки відсутності правових механізмів, що накладають обмеження на безконтрольне застосування цих сил і засобів.

Інформаційно-психологічна війна може бути віднесена до категорії особливих умов реалізації державної інформаційної політики в силу особливої соціальної небезпеки даного явища, щодо якої суспільством ще не вироблена ефективна система організації протидії.

Державі належить ключова роль в становленні інформаційного суспільства: вона повинна стати не тільки каталізатором змін, що відбуваються, а й координатором зусиль різних суб'єктів суспільства, механізмом примирення протиріч бізнесу і соціальних інститутів, законодавцем, здатним забезпечити умови для конкуренції в інформаційній індустрії, встановити баланс між конкуренцією і регулюванням, побудувати правовий фундамент інформаційного суспільства [22, с. 36].

Відповідно до запропонованого підходу, інформаційна політика розглядається як стратегічний об'єкт соціальної інформаціології. Остання – це наука про логіку існування, розвиток, функціонування соціальної інформації, інформації про соціум і всередині соціуму, де відбувається обмін нею за допомогою комунікації [23, с.28].

Структурно-функціональна модель інформаційної політики включає кілька взаємопов'язаних елементів, основним з яких є ідеологічний блок (або місія) організації, що виступає змістовною базою для здійснення будь-якої інформаційної діяльності. Слідом за цим блоком, що виробляється на стратегічному рівні управління, йде адаптація і постановка конкретних завдань для різних цільових груп, які є об'єктами інформаційного впливу.

Оскільки основна мета, яка ставиться при формуванні інформаційної політики, полягає в забезпеченні ефективності управління, то, виходячи з цього, відбір цільових груп будується на основі їх впливу на досягнення даної мети. Після постановки завдань для різних цільових груп, інформаційна політика передбачає визначення форм контактів (і каналів комунікації), які дозволили б здійснити донесення необхідних повідомлень до кожної з цих груп, а також адекватних методів взаємодії.

Заключним елементом є контрольно-координаційна функція, основне завдання якої полягає в розподілі обсягів уваги до кожної групи і оцінки ефективності застосовуваних методів взаємодії. Така модель дозволяє виділити кілька

функціональних і змістовних блоків, які вимагають досить жорсткої регламентації [32].

На рівні ідеологічного блоку йдеться про чітке оформлення, з одного боку, цінностей, на основі яких будує свою роботу орган влади (при цьому мова може йти не стільки про ідеологію, скільки про те, які риси, імідж повинна мати влада), а з іншого – як ці цінності повинні бути адаптовані до специфіки різних цільових груп.

Наступні блоки фіксують специфіку тих видів діяльності, які спрямовані на оформлення і поширення цих цінностей (іміджевих характеристик) до різних цільових груп. При цьому можна виділити окремі функції, які необхідні для реалізації інформаційної політики. До їх числа відносяться «планування», «виробництво повідомлень», «поширення», «аналіз ефективності», «координація і контроль».

Такий аналіз дозволяє говорити про завдання, які може вирішувати держава, керуючи своєю інформаційною політикою:

Завдання оперативного управління.

- Збереження соціально-економічної і політичної стабільності.
- Забезпечення ефективності реалізації управлінських рішень.
- Залучення інвестицій

Завдання стратегічного управління.

- Формування лояльності населення до влади, міста, країни, держави через формування ефективного комунікаційного середовища, здатного знизити ступінь соціальної конфліктності.
- Формування патріотичних цінностей і способу життя, заснованого на них.
- Поділ відповідальності за соціально-економічні та політичні процеси з бізнесом і представниками «третього сектора» [43, с. 111].

На жаль, в умовах сучасної української дійсності інформаційна політика здійснюється за допомогою реалізації технологій односпрямованого впливу влади на суспільство з метою лобіювання потрібних їй рішень, без врахування важливості реалізації взаємодії між владою і суспільством як двома основними суб'єктами політичних відносин. В першу чергу, це пов'язано з відсутністю реально діючої концепції державної інформаційної політики, нормативно-правової бази, як на

державному рівні, так і на регіональному, бази, яка визначала б і ціннісні орієнтири змісту ДІП, джерела фінансування та матеріального забезпечення тощо.

Інша, важлива причина полягає в тому, що сьогодні немає адекватної організаційної моделі формування і управління інформаційною політикою, особливо якщо розглядати її як елемент загальної стратегії розвитку держави. Безумовно, фактично на всіх рівнях влади є прес-служби (прес-секретарі) або відділи по зв'язках з громадськістю. Однак існуючі структури працюють тільки на вирішення завдань оперативного управління. У певному сенсі вони – «пожежна команда», чия діяльність в основному полягає в швидкому реагуванні на пов'язані з роботою адміністрації проблеми. Говорити тут про комплексне вирішення стратегічних завдань не доводиться. Причому причини не в рівні кваліфікації даних фахівців, а в тій організаційної моделі та поточних завданнях, які перед ними ставляться.

Відсутність продуманої концепції державної інформаційної політики як комплексу спільних дій влади, суспільства і ЗМІ в комунікаційному просторі може призводити до того, що ця політика сприймається виключно як система цілеспрямованого впливу державних структур на ЗМІ. Сама влада сприймає цей процес невід'ємним від технічних умов інформатизації (звідси необхідність їх розвитку, який, як вже зазначалося, займає вагоме місце в офіційних документах). Тим часом проблема діалогу з владою виглядає як одна з найбільш гострих [32].

Змістовними пріоритетами інформаційної політики повинні виступати механізми і технології створення багатосторонньої (партиципарної) комунікації, результатом її здійснення якраз і може стати паритетна взаємодія всіх учасників комунікаційного процесу. В іншому випадку замість такої комунікації виникає нерівна інформаційна взаємодія між владою, суспільством і ЗМІ. В результаті формується інформаційний простір, при якому інтереси одних суб'єктів посилюються, а інших слабшають і навіть ігноруються.

Влада може активно впливати на ЗМІ, в різних формах примушуючи журналістів створювати картину світу на догоду інтересам державних структур і великих бізнес-монополій. ЗМІ, в свою чергу, різними способами в буквальному сенсі можуть нав'язувати суспільству ті чи інші погляди, мало піклуючись про плюралізм

думок, повазі інтересів різних соціальних і політичних груп. Суспільство, акумулюючи таку інформацію, транслює її, ще більше спотворюючи початковий «предмет обговорення». Таким чином, одні суб'єкти інформаційної політики неминуче підпадають під маніпулятивний вплив з боку інших суб'єктів.

Розвиток інформаційного суспільства, орієнтованого на інтереси людини, є спільною справою органів державної влади, приватного сектору та громадянського суспільства. Воно повинно здійснюватися на основі співробітництва і партнерських відносин між усіма зацікавленими сторонами.

Особливу роль тут відіграють автори і розповсюджувачі інформації (контенту): дослідники, аналітики, журналісти, працівники бібліотек, архівів, культурних і освітніх установ, видавці, інформаційні агентства, засоби масової інформації та інші системи поширення знань та інформації. Свобода їх позитивної діяльності повинна бути гарантована державною інформаційною політикою [33, с. 58].

Створювана і поширювана інформація повинна призначатися для різних груп і прошарків суспільства. Повинно мати місце різноманітність думок та інтерпретацій, при дотриманні законодавчих обмежень поширення окремих видів інформації. Все це є також необхідною запорукою успішного розвитку громадянського суспільства.

1.3. Правове забезпечення інформаційної політики

Основою проведення державної політики і основним механізмом реалізації державного управління в будь-якій сфері життєдіяльності суспільства і держави є нормативне правове регулювання, суть якого полягає в прийнятті управлінських рішень у формі нормативно-правових актів. Базу нормативно-правового регулювання складають акти національного законодавства. Тому наступним головним завданням державної влади в проведенні інформаційної політики є формування та розвиток її законодавчої бази – національного інформаційного законодавства, структурованого за рівнями законодавства, методам нормативного регулювання відносин і рівня охоплення предмета регулювання, яка включає як спеціальні акти, присвячені

питанням правового регулювання в інформаційній сфері, так і окремі норми з даного предмету в інших правових актах [43, с. 111].

При цьому слід підкреслити, що акти інформаційного законодавства, які повинні в принципі бути актами прямої дії, не тільки складають законодавчу базу, а й самі є певними управлінськими рішеннями, спрямованими на проведення тієї чи іншої інформаційної політики. Тому законодавче поле також є областю безпосереднього формування і проведення державної інформаційної політики (далі – ДІП).

У національному інформаційному законодавстві повинні бути максимально повно відрегульовані відносини, включаючи права, обмеження прав, обов'язки і відповідальність, об'єктів і суб'єктів правового регулювання в інформаційній сфері. Наявність концепції і законодавчої бази є необхідною, але не достатньою. Для здійснення ДІП повинні бути також створені організаційно-технологічні умови для практичної реалізації процесів державного регулювання інформаційної сфери. При цьому правила, умови та порядок формування і функціонування організаційно-технологічного забезпечення процесів державного регулювання інформаційної сфери також повинні бути визначені на основі відповідних актів інформаційного законодавства.

Основою формування організаційно-технологічного забезпечення проведення ДІП є чіткий розподіл прав, обов'язків і відповідальності за реалізацію такої політики в системі органів державної влади [43, с. 112].

Національна інформаційна політика України визначається Конституцією України, Законами України “Про наукову і науково-технічну діяльність”, “Про інформацію”, “Про науково-технічну інформацію”, “Про захист інформації в автоматизованих системах”, “Про друковані засоби масової інформації”, “Про авторське право та суміжні права”, “Про національний архівний фонд і архівні установи”, “Про телебачення і радіомовлення”, “Про Концепцію Національної програми інформатизації”, “Про Національну програму інформатизації”, а також іншими чинними нормативними актами загального і спеціального змісту, в яких

визначені співвідношення верховенства міжнародних норм і національні пріоритети у вказаній сфері.

Відповідно до фундаментальних положень Доктрини інформаційної безпеки України [15] забезпечення інформаційного суверенітету, запобігання інформаційній агресії, експансії та інформаційній блокаді України з боку іноземних держав, організацій, груп та осіб є пріоритетним завданням політикуму нашої країни. Інформаційна безпека держави є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки, яка характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз і являє собою сукупність інформаційно-психологічної (психофізичної) та інформаційно-технологічної безпеки держави [15].

Законом України "Про національну безпеку" визначено, що одним з головних пріоритетів України є прагнення побудувати орієнтоване на інтереси людей, відкрите для усіх і спрямоване на розвиток інформаційне суспільство, в якому кожен міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, щоб надати можливість кожній людині повною мірою реалізувати свій потенціал, сприяючи суспільному і особистому розвиткові та підвищуючи якість життя [48].

Водночас ступінь розбудови інформаційного суспільства в Україні порівняно із світовими тенденціями є недостатнім і не відповідає потенціалу та можливостям України, оскільки створення інфраструктури для надання органами державної влади та органами місцевого самоврядування юридичним і фізичним особам інформаційних послуг з використанням мережі Інтернет відбувається повільно. Так, система виконавчої влади і сьогодні залишається доволі закритою для громадян і бізнесу. Результати наукових та соціологічних досліджень стану системи державного управління також свідчать про низьку ефективність державної влади, корумпованість державного апарату, падіння довіри громадян до державних інститутів і державних службовців [43, с. 112].

Тому держава приймає заходи, спрямовані на реформування адміністративної системи з метою підвищення ефективності державного управління та кардинального поліпшення діяльності органів виконавчої влади на основі переходу на масове використання інформаційних комунікативних технологій (ІКТ).

У зв'язку з цим розроблено концептуальні офіційні документи, в яких визначені основні положення державної політики у галузі інформатизації органів державної влади України, закони України: "Про Національну програму інформатизації"; "Про Концепцію Національної програми інформатизації"; "Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації"; "Про електронний цифровий підпис"; "Про адміністративні послуги" [9]; "Про електронні документи та електронний документообіг" та ін.

У цих концептуальних документах сформульовані базові положення державної політики у галузі вдосконалення діяльності органів державної влади та підвищення її ефективності на основі використання автоматизованих систем та інформаційних комунікаційних технологій: цілі та завдання, принципи та основні напрями.

Так, в Рішенні Ради РНБО від 28 квітня 2015 року Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» зазначається, що державна політика інформатизації формується як складова частина соціально-економічної політики держави загалом і спрямовується на раціональне використання промислового та науковотехнічного потенціалу, матеріально-технічних і фінансових ресурсів для створення сучасної інформаційної інфраструктури в інтересах виконання комплексу поточних та перспективних завдань розвитку України, як незалежної демократичної держави з ринковою економікою [64].

Особливе місце для ефективної роботи органів державної вдади посідає Закон України "Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації" [50]. Він, відповідно до Конституції України [27], визначає порядок всебічного і об'єктивного висвітлення діяльності органів державної влади та органів місцевого самоврядування

засобами масової інформації і захисту їх від монопольного впливу органів тієї чи іншої гілки державної влади або органів місцевого самоврядування, і є складовою частиною законодавства України про інформацію. У цьому законі зазначається, що засоби масової інформації України відповідно до законодавства України мають право висвітлювати усі аспекти діяльності органів державної влади та органів місцевого самоврядування.

Органи державної влади та органи місцевого самоврядування зобов'язані надавати засобам масової інформації повну інформацію про свою діяльність через відповідні інформаційні служби органів державної влади та органів місцевого самоврядування, забезпечувати журналістам вільний доступ до неї, крім випадків, передбачених

Водночас варто зазначити, що підвищення ефективності державної системи управління суспільством на основі використання інформаційних технологій є структурною складовою комплексної постійно оновлюваної форми реалізації державної інформаційної політики.

Одним із самостійних її елементів є створення інформаційної технології "Електронне урядування". У сучасних словниках з мовознавства визначення термінів "електронне урядування" та "електронний уряд" відсутнє, тому лінгвістично його визначити неможливо, оскільки вживання слова "електронне" при поєднанні зі словами "урядування, "уряд" вибране з великим ступенем умовності, як і інші поняття: "електронна інформація", "електронний документ", "електронний підпис" і усі інші видові назви, що позначають нові різновиди продукції цифрової цивілізації третього тисячоліття.

Натомість у розпорядженні Кабінету Міністрів України "Про схвалення Концепції розвитку електронного урядування в Україні" зазначається, що електронне урядування є одним з інструментів розвитку інформаційного суспільства, впровадження якого сприятиме створенню умов для відкритого і прозорого державного управління [61].

Електронне урядування – це форма організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів

державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян. Головною складовою електронного урядування є електронний уряд – єдина інфраструктура міжвідомчої автоматизованої інформаційної взаємодії органів державної влади та органів місцевого самоврядування між собою, з громадянами і суб'єктами господарювання [61].

Відповідно до цього Розпорядження, основними принципами електронного урядування є:

– прозорість і відкритість;

– конфіденційність та інформаційна безпека;

– єдині технічні стандарти і взаємна сумісність;

– орієнтованість на інтереси і потреби споживачів послуг.

З урахуванням переваг технологій електронного урядування завданнями із забезпечення розвитку електронного урядування в Україні є:

– забезпечення захисту прав громадян на доступ до державної інформації;

– залучення громадян до участі в управлінні державними справами;

– удосконалення технології державного управління;

– підвищення якості управлінських рішень;

– подолання "інформаційної нерівності", зокрема за допомогою створення спеціальних центрів (пунктів) надання інформаційних послуг, центрів обслуговування населення (кол-центрів), веб-порталів надання послуг;

– організація надання послуг громадянам і суб'єктам господарювання в електронному вигляді з використанням Інтернету та інших засобів, насамперед за принципом "єдиного вікна";

– надання громадянам можливості навчатися протягом усього життя;

– деперсоніфікація надання адміністративних послуг з метою зниження рівня корупції у державних органах;

– організація інформаційної взаємодії органів державної влади та органів місцевого самоврядування на основі електронного документообігу з використанням електронного цифрового підпису;

– забезпечення передачі і довгострокового зберігання електронних документів у державних архівах, музеях, бібліотеках, підтримки їх в актуалізованому стані та надання доступу до них.

Висновки до Розділу 1

Державна інформаційна політика – це сукупність основних напрямів і способів діяльності держави по одержанню, використанню, поширенню та зберіганню інформації.

Головними напрямами і способами державної інформаційної політики є:

- забезпечення доступу громадян до інформації;
- створення національних систем і мереж інформації;
- зміцнення матеріально-технічних, фінансових, організаційних, правових і наукових основ інформаційної діяльності;
- забезпечення ефективного використання інформації;
- сприяння постійному оновленню, збагаченню та зберіганню національних інформаційних ресурсів;
- створення загальної системи охорони інформації;
- сприяння міжнародному співробітництву в галузі інформації і гарантування інформаційного суверенітету України;
- сприяння задоволенню інформаційних потреб закордонних українців.

Стан будь-якої інформаційної сфери також впливає і рівень політичної боротьби в країні. При цьому інформаційне суспільство можна розглядати як продовження революції індустріального та постіндустріального суспільства, де спостерігається швидке зростання секторів створення та споживання інформації, що перетворюється на один із найважливіших ресурсів, поряд з енергією та корисними копалинами. За ступенем споживання цього стратегічного ресурсу нині у світі оцінюється ступінь розвинутості країни, її економічний та політичний потенціал.

Інформаційні відносини в Україні реалізовуються на принципах:

- гарантованості права на інформацію;
- відкритості, доступності інформації, свободи обміну інформацією;
- достовірності і повноти інформації;
- свободи вираження поглядів і переконань;
- правомірності одержання, використання, поширення, зберігання та захисту інформації;
- захищеності особи від втручання в її особисте та сімейне життя.

РОЗДІЛ 2. КІБЕРЗЛОЧИННІСТЬ – ЗАГРОЗА ДЕРЖАВНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРУ

2.1. Кіберзлочинність як явище: передумови виникнення та розвиток

Парадокс розвитку людства полягає в тому, що протягом усього свого розвитку людина використовувала, накопичувала, передавала інформацію. Безперервний процес інформатизації суспільства охоплює всі сфери діяльності людини і держави: від вирішення проблем національної безпеки, охорони здоров'я та управління транспортом до освіти, фінансів, і навіть просто міжособистісного спілкування. У міру розвитку технологій електронних платежів, «безпаперового» документообігу, серйозний збій локальних мереж може паралізувати роботу цілих корпорацій і банків, що може привести до значних матеріальних збитків і колосальних збитків.

Історія кіберзлочинів – це новітня історія, яка стосується всіх нас. В даний час проблема кіберзлочинності переросла в масштаби світової спільноти.

Термін «кіберзлочинність» в даний час часто вживається поряд з терміном «комп'ютерна злочинність», причому нерідко ці поняття використовуються як синоніми. Дійсно, ці терміни дуже близькі один одному, але все ж таки не синонімічні. Поняття «кіберзлочинність» (в англомовному варіанті – *cybercrime*) ширше, ніж «комп'ютерна злочинність» (*computer crime*), і більш точно відображає природу такого явища, як злочинність в інформаційному просторі. Так, Оксфордський тлумачний словник [96] визначає приставку «cyber-» як компонент складного слова. Її значення - «*що відноситься до інформаційних технологій, мережі Інтернет, віртуальної реальності*». Таким чином, «cybercrime» – це злочинність, пов'язана як з використанням комп'ютерів, так і з використанням інформаційних технологій і глобальних мереж. У той же час термін «computer crime» відноситься тільки до злочинів, що здійснюються проти комп'ютерів або комп'ютерних даних.

Згідно з рекомендаціями експертів ООН термін «кіберзлочинність» охоплює будь-який злочин, який може відбуватися за допомогою комп'ютерної системи або мережі, в рамках комп'ютерної системи або мережі або проти комп'ютерної системи

або мережі [21]. Таким чином, до кіберзлочинів може бути віднесено будь-який злочин, скоєний в електронному середовищі.

Злочин, скоєний в кіберпросторі – це протиправне втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні дії, вчинені за допомогою комп'ютерів, комп'ютерних мереж і програм [21].

Рис.2.1. Класифікація кіберзлочинів [21]

Сьогодні кіберзлочинність – масштабна проблема, а шкідливі програми пишуться з метою незаконного отримання грошей. Розвиток інтернету став одним з ключових чинників, що визначили ці зміни. Компанії та окремі користувачі вже не уявляють без нього своє життя, і все більше фінансових операцій проводиться через інтернет. Кіберзлочинці усвідомили, які величезні можливості для «заробляння» грошей за допомогою шкідливого коду з'явилися останнім часом, і багато з сучасних шкідливих програм написані на замовлення або з метою подальшого продажу іншим злочинцям.

У конвенції Ради Європи зазначається про чотири типи комп'ютерних злочинів, які визначаються, як злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем [93]:

1. незаконний доступ – ст. 2 (протиправний умисний доступ до комп'ютерної системи або її частини);

2. незаконне перехоплення – ст. 3 (протиправне умисне перехоплення не призначених для громадськості передач комп'ютерних даних на комп'ютерну систему, з неї або в її межах);

3. втручання в дані – ст. 4 (протиправне пошкодження, видалення, порушення, зміна або припинення комп'ютерних даних);

4. втручання в систему – ст. 5 (серйозне протиправне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, порушення, зміни чи припинення комп'ютерних даних).

Крім трансформації самої кіберзлочинності, змінюються також і характеристики хакера: якщо спочатку це були люди, які мали знання, вміння, які спрямовували свої дії не стільки на протизаконні цілі, скільки на пошук нового, то в даний час за злочинними діями стоїть кримінальний бізнес. Спостерігається розшарування зловмисників на осіб, які мають високі знання в даній специфічній сфері, яких можна віднести до категорії «Elite», і осіб, які отримали в свої руки готовий алгоритм, що забезпечує виконання певного порядку дій, маючи при цьому дуже загальне уявлення про процеси, що відбуваються в інформаційних системах [93].

Перша категорія кіберзлочинців, а саме вони представляють сьогодні найбільшу загрозу, має цілком характерні, яскраво виражені риси. До таких можна віднести:

- здатність здійснювати злочинні діяння анонімно, таємно;
- злочинні діяння найкращими є в умовах транскордонної дії юрисдикції різних держав;
- високі професійні та інтелектуальні здібності хакера;

- наявність можливості об'єднання розрізнених комп'ютерів в єдиний механізм здійснення злочинних дій в автоматизованому режимі;
- відсутність, або з тривала тимчасова затримка, усвідомлення потерпілою стороною факту скоєння по відношенню до неї злочинного впливу;
- наявність великої кількості потерпілих при здійсненні хакерської атаки;
- відсутність необхідності хакеру вступати в безпосередній контакт з жертвою своєї протиправної дії.
- Появу кіберзлочинності можна відраховувати з моменту появи комп'ютера, так званої епохи ЕОМ. Історію кіберзлочинів можна розділити на два періоди: перший – з моменту створення першої ЕОМ до 1990 року і з 1990 року по даний момент часу. Справа в тому, що починаючи з 1990 року інтернет почав поширюватися по світу з величезною швидкістю.

Перша згадка про використання комп'ютера з метою скоєння злочину була оприлюднена у 1960-х роках, коли комп'ютери були великі універсальні комп'ютери, ЕОМ. Після Другої світової війни в 1946 році кілька компаній почали працювати над комерційними ЕОМ і до 1951 року UNIVAC випускає перший комерційний комп'ютер, створений в Сполучених Штатах, і третій комерційний комп'ютер у світі (після німецького Z4 і британського Ferranti Mark 1), який не був призначений для використання в наукових дослідженнях з розробки зброї. Перший екземпляр UNIVAC був офіційно проданий Бюро перепису населення США. Всього за період з 1951 по 1958 роки було створено 46 екземплярів UNIVAC. Вони були встановлені в урядових установах, приватних корпораціях і в трьох університетах США [22, с. 142].

Електронні вакуумні лампи виділяли велику кількість тепла, поглинали багато електричної енергії, були громіздкими, дорогими і ненадійними. Комп'ютери першого покоління, побудовані на вакуумних лампах, мали низьку швидкість і невисоку надійність.

У 1947 р. співробітники американської компанії «Белл» Вільям Шоклі, Джон Бардін і Уолтер Бреттейн винайшли транзистор. Транзистори виконували ті ж функції, що і електронні лампи, але використовували електричні властивості напівпровідників. У порівнянні з вакуумними трубками транзистори займали в 200

разів менше місця і споживали в 100 разів менше електроенергії. У той же час з'являються нові пристрої для організації пам'яті комп'ютерів – ферритові сердечники. З винаходом транзистора і використанням нових технологій зберігання даних в пам'яті з'явилася можливість значно зменшити розміри комп'ютерів, зробити їх більш швидкими і надійними, а також значно збільшити ємність пам'яті комп'ютерів [29, с. 2].

У 1954 році компанія Texas Instruments оголосила про початок серійного виробництва транзисторів, а в 1956 році вчені Массачусетського технологічного інституту створили перший, повністю побудований на транзисторах комп'ютер ТХ.

У 60-ті роки минулого століття з'явилося третє покоління ЕОМ, в яких вперше стали використовуватися інтегральні схеми (мікросхеми). В цей же час з'являється напівпровідникова пам'ять, яка і до цього дня використовується в персональних комп'ютерах в якості оперативної. У ці роки виробництво комп'ютерів набуває промисловий розмах. Компанія IBM першою реалізувала сімейство ЕОМ – серію повністю сумісних один з одним комп'ютерів від самих маленьких, розміром з невелику шафу (менше тоді ще не робили), до найбільш потужних і дорогих моделей.

Ще на початку 60-х з'являються перші мінікомп'ютери – невеликі малопотужні комп'ютери, доступні за ціною невеликим фірмам або лабораторіям. Мінікомп'ютери представляли собою перший крок на шляху до персональних комп'ютерів, пробні зразки яких були випущені тільки в середині 70-х голів. Разом зі стрімким розвитком комп'ютерної сфери починає свій розвиток кіберзлочинність [29, с.10].

Але комп'ютерна злочинність 1960-х і 1970-х років відрізнялася від кіберзлочинності сьогодні. По-перше, в той час ще не з'явився Інтернет, по-друге, ЕОМ не були об'єднані в мережу. У 1960 році типова ЕОМ коштувала кілька мільйонів доларів, займала площу однієї кімнати і вимагала спеціальної системи кондиціонування повітря, щоб комп'ютер не згорів. У той час тільки певне коло дослідників і вчених могли використовувати ЕОМ у своїй роботі.

Обмежене використання ЕОМ і відсутність з'єднання з іншими комп'ютерами різко скорочувало шанси здійснення комп'ютерних злочинів, і якщо такі відбувалися, то тільки людьми, які обслуговували ЕОМ. Всі злочини того часу зводилися до

злочинів, пов'язаних з фінансовими вкладеннями в ЕОМ. Це тривало до появи і всесвітнього поширення мережі Інтернет, що відкрило нові можливості для злочинців.

Історію кіберзлочинів можна розглядати в рамках історії розвитку хакерства. Хакер – це висококваліфікований IT-фахівець, людина, яка розуміє тонкощі роботи ЕОМ. Розрізняють два види IT-хакерів: «White hat» і «Black hat». «Black hat» називають кіберзлочинців, тоді як «White hat» – інших фахівців з інформаційної безпеки (зокрема фахівців, що працюють у великих IT- компаніях) або дослідників IT-систем, які не порушують закон [42].

Другий етап розвитку комп'ютерних злочинів починається з середини 90-х років минулого століття, це був період, коли Інтернет поширювався зі стрімкою швидкістю. Це був час, коли персональні комп'ютери та Інтернет стають доступнішими для загального використання. У грудні 1995 року, за деякими оцінками, було зареєстровано 16 мільйонів користувачів Інтернету в усьому світі, а вже до травня 2002 року ця цифра зросла до 580 мільйонів, що становило майже 10 відсотків від загального населення планети (NUA, 2003). Потрібно відзначити, що поширення Інтернету по світу було нерівномірно, наприклад, більше 95 відсотків із загального числа Інтернет-з'єднань розташовувалися в США, Канаді, Європі, Австралії та Японії. Саме в цей час в історію злочинів був введений новий вид злочинів, який мав назву «злам».

На початковому етапі розвитку кіберзлочинів дуже часто використовується термін «злам», хоча пізніше злам буде визначено як один із злочинів, що входить в поняття кіберзлочини. Саме злам характеризує протизаконні дії хакерів.

Кіберзлочинність є не тільки технічною і правовою, а й соціальною проблемою, ефективне рішення якої вимагає, перш за все, системного підходу до розробки основ забезпечення безпеки життєво важливих інтересів громадянина, суспільства і держави в кіберпросторі.

За механізмами і способами скоєння злочину в сфері комп'ютерних технологій вони мають високий рівень латентності. Найбільшу суспільну небезпеку становлять злочини, пов'язані з неправомірним доступом до комп'ютерної інформації.

Аналізовані правопорушення мають дуже високу латентність, яка, за різними даними, становить 85-90%. Більш того, факти виявлення незаконного доступу до інформаційних ресурсів на 90% мають випадковий характер [65, с.89].

Ці дані свідчать про те, що працівники правоохоронних органів часто просто не розуміють, як розслідувати ці злочини і як доводити їх в суді. Звідси неможливість якісно проводити розслідування, традиційні методи організації і планування розслідування не спрацьовують в даних умовах, необхідно підвищувати ефективність правоохоронної діяльності, підвищувати рівень вимогливості до рівня професіоналізму співробітників правоохоронних органів, їх морально ділових якостей. Не можна допускати їх формального ставлення до звітності про результати боротьби з комп'ютерною злочинністю.

Ще однією проблемою, з якою найчастіше стикаються слідчі під час розслідування злочинів у сфері комп'ютерних технологій, є встановлення факту вчинення злочину. Це пов'язано з тим, що часто комп'ютерні злочини скоюються в так званому «кіберпросторі», вони не знають кордонів, дуже часто злочини скоюються не виходячи з дому, за допомогою свого персонального комп'ютера. Крім того, незаконне копіювання інформації найчастіше залишається непоміченим, введення в комп'ютер вірусу зазвичай списується на ненавмисну помилку користувача, який не зміг його «відловити» при контактуванні з зовнішнім комп'ютерним світом. Також ставлення постраждалих до скоєного проти них посяганню не завжди адекватне. Замість того, щоб повідомити правоохоронними органам про факт незаконного втручання в комп'ютерну систему, постраждалі не поспішають цього робити, побоюючись підриву ділової репутації. Зазвичай, в якості потерпілої сторони від комп'ютерних злочинів виступають локальні мережі, сервери, фізичні особи [73, с.10].

Слід підкреслити, що професійні комп'ютерні злочинці як об'єкт злочину вибирають локальні мережі та сервери великих компаній, в свою чергу «дилетанти» зазіхають на інформацію комп'ютерів фізичних осіб і рідше «зламують» провайдерів Інтернет послуг, як правило, для «безкоштовного» доступу в Інтернет.

Примітний той факт, що потерпіла сторона, в особі великих корпорацій, що є власником системи, неохоче повідомляє (якщо повідомляє взагалі) в правоохоронні органи про факти вчинення комп'ютерного злочину. А оскільки вони становлять більшість, то саме цим можна пояснити високий рівень латентності комп'ютерних злочинів.

Крім того, в розкритті факту скоєння злочину дуже часто не зацікавлені посадові особи, в обов'язки яких входить забезпечення комп'ютерної безпеки. Визнання факту несанкціонованого доступу в підвідомчу їм систему ставить під сумнів їх професійну кваліфікацію, а неспроможність заходів з комп'ютерної безпеки, прийнятих керівництвом, може викликати серйозні внутрішні ускладнення.

Банківські службовці, як правило, ретельно приховують виявлені ними злочини, які вчинені проти комп'ютерів банку, так як це може згубно позначитися на престижі банку та призвести до втрати клієнтів. Деякі жертви бояться серйозного компетентного розслідування, тому що воно може розкрити непристойну або навіть незаконну механіку ведення справ [74, с.140].

Є ще одна проблема, пов'язана з ефективністю розслідування комп'ютерних злочинів та доведення їх до суду. Це громадська думка, яка не вважає комп'ютерні злочини серйозним злочином внаслідок того, що комп'ютерні злочинці, навіть якщо розслідування доведено до кінця і винесено вирок суду, відбуваються легкими покараннями, найчастіше – умовними вироками. Звідси – правовий нігілізм, з одного боку злочинців, які відчувають себе безкарно, а з іншого боку, потерпілих, які не хочуть звертатися в правоохоронні органи із заявами про несанкціонований доступ, тому що розуміють, що належного покарання для злочинців вони все одно не доб'ються.

2.2. Сутність та особливості кіберзлочинів

Стрімкий розвиток комп'ютерних, в тому числі інтернет-технологій, їх активне використання в усіх сферах економічної діяльності стали найважливішою тенденцією розвитку сучасного суспільства. Зростаюче застосування інтернет-технологій для організації торгівлі цінними паперами, розширення сфери електронних розрахунків,

інтернет-комерції, автоматизації багатьох функцій в сфері бізнесу створюють і нову специфічну область кримінальної активності. В умовах нарощування в світі процесів глобалізації та формування "інформаційного суспільства" в якості самостійного фактора, здатного загрожувати економічній безпеці, стала виступати комп'ютерна злочинність.

Активне впровадження інформаційних технологій в усі сфери діяльності привели до зміни і переліку злочинів, що відносяться до економічних. До цих злочинів стали відносити комп'ютерні злочини, які заподіюють шкоду економіці держави, її окремим секторам, підприємницькій діяльності, а також економічним інтересам окремих груп громадян. За оцінками фахівців, в США щорічно втрати корпорацій від злочинності перевищують 200 млрд, а від комп'ютерних злочинів – 6 млрд дол. У Великобританії комп'ютерні злочини обходяться в 2 млн ф. ст. на день [90].

За оцінками ряду досліджень, кожну секунду в світі жертвами кіберзлочинців стають 12 осіб і ця цифра з кожним роком зростає [90]. Можна виділити наступні фактори, що впливають на зростання числа кіберзлочинів:

- глобальна інформатизація всіх сфер життя суспільства не підвищує, а знижує ступінь його безпеки;
- прискорення науково-технічного прогресу збільшує ймовірність застосування злочинцями в якості засобів ураження суто мирних технологій, причому можливість "подвійного" їх використання часто не тільки не передбачається, але і не усвідомлюється творцями технології;
- тероризм все більше стає інформаційною технологією особливого типу, оскільки: по-перше, терористи все ширше використовують можливості сучасних інформаційно-телекомунікаційних систем для зв'язку і збору інформації; по-друге, реалією наших днів стає так званий "кібертероризм"; по-третє, більшість терористичних актів зараз розраховані не тільки на заподіяння матеріального збитку і загрозу життю і здоров'ю людей, а й на інформаційно-психологічний шок, вплив якого на великі маси людей створює сприятливу обстановку для досягнення терористами своїх цілей;

– "цифрова нерівність" і поява країн, які програли інформаційну гонку можуть стати причиною терористичної активності проти окремих держав як засіб асиметричної відповіді.

Основними об'єктами кіберзагроз є громадяни, бізнес-структури та держава (таблиця 2.1).

Таблиця 2.1

Об'єкти і види кіберзагроз [94]

Громадяни	Вплив на особистість шляхом збору персональних даних та атак на персональні комп'ютери і мобільні пристрої громадян, витік і оприлюднення приватної інформації, шахрайство, поширення небезпечного контенту
Бізнес	Вплив на системи інтернет-банкінгу, вплив на інформаційну інфраструктуру, блокування систем онлайн-торгівлі, геоінформаційних систем і хакерські атаки на сайти компаній
Держава	Атаки на ключові державні системи управління (електронний уряд, сайти державних структур), економічна блокада (масштабне відключення платіжних систем, систем бронювання), апаратні атаки на персональні комп'ютери і критично важливу інфраструктуру державних підприємств

Суб'єктами злочинів, які активно використовують високі технології, поряд з особами, які виконують професійні функції в організаціях і на підприємствах, стають практично будь-які особи. При цьому їхня мета, використовувані методи та наявні можливості практично не відрізняються від тих, які притаманні злочинцям за родом зайнятості. Основним мотивом кіберзлочинців виступає отримання матеріальної вигоди [94].

Кіберзлочинці використовують свій арсенал інформаційної зброї, що представляє собою сукупність засобів, призначених для порушення (копіювання, спотворення або знищення) інформаційних ресурсів на стадії їх створення, обробки, поширення і зберігання. До основних видів інформаційної зброї відносять такі:

- *бекдор* (backdoor, від англ. Back door – чорний хід). Даний інструмент передбачає прихований метод в системі, який дозволяє отримати доступ до захищеної області;
- *комп'ютерні "віруси*" – спеціальні програми, які впроваджуються в програмне забезпечення комп'ютерів, знищують, спотворюють або дезорганізують його функціонування. Вони здатні передаватися по лініях зв'язку, мережі передачі даних, виводити з ладу системи управління і т.п. Крім того, "віруси" здатні самостійно розмножуватися;
- *"логічні бомби"* – програмні закладні пристрої, які заздалегідь впроваджують в інформаційно-керуючі центри інфраструктури, щоб по сигналу або у встановлений час привести їх в дію;
- *програмні продукти типу "троянський кінь"* – програми або утиліти, які після установки виконують заявлені функції в фоновому режимі;
- *нейтралізатори тестових програм*, що забезпечують збереження природних і штучних недоліків програмного забезпечення;
- *аналізатори трафіку (sniffer*) – програми або пристрої, які контролюють дані, що передаються по мережі. Традиційно використовуються для законних функцій мережевого управління, вони можуть застосовуватися і під час кібератак з метою крадіжки інформації;
- *DDos-атаки* – призначені для порушення доступу до мережі, як правило, за допомогою виконання мільйонів запитів кожну секунду, в результаті чого доступ до мережі ускладнюється або порушується;
- *E-mail Spoofing* – це метод відправки електронної пошти з підміною джерела, використовується для того, щоб змусити одержувача надати конфіденційну інформацію;
- *Keylogger* є програмним або апаратним засобом, який призначений для контролю натискання клавіш на клавіатурі комп'ютера, для отримання пароля, пін-коду або іншої інформації [92].

На Землі існує дуже мало місць, де неможливо отримати доступ до Інтернету. У більшості країн є, як мінімум, один постачальник Інтернет-послуг, який надає мережеву інфраструктуру (апаратне забезпечення, таке як обладнання, кабелі та бездротовий доступ) для великих міст. Навіть в районах, де немає місцевих постачальників Інтернет-послуг, глобальні супутникові мережі можуть забезпечити доступ до Інтернету для віддалених районів. Широкосмугова технологія в країнах, що розвиваються, впроваджується повільними темпами, в результаті чого населення цих країн для доступу в Інтернет використовує мобільні технології [72].

Завдяки доступності Інтернет-послуг через мобільні пристрої, використання Інтернету неухильно зростає [72]. Смартфони стають все менш дорогими і включають в себе все більше функцій, а постачальники послуг мобільного зв'язку забезпечують більш надійний доступ в Інтернет через менш дорогі мережі стільникового зв'язку. Це сприяє збільшенню рівня проникнення Інтернету в багатьох країнах. 2016 рік став першим роком, коли більшість користувачів Інтернету у всьому світі для виходу в Інтернет стали використовувати мобільні пристрої [72].

Рівень проникнення Інтернету означає відсоток від загальної чисельності населення даної країни або регіону, який використовує Інтернет.

У 2018 році рівень проникнення Інтернету в світі оцінюється в 64% [72]. Таким чином, приблизно половина населення світу має доступ до Інтернету і можливість користуватися Інтернетом (Рисунок 2.2 із зазначенням рівня проникнення Інтернету з розбивкою по регіонах)

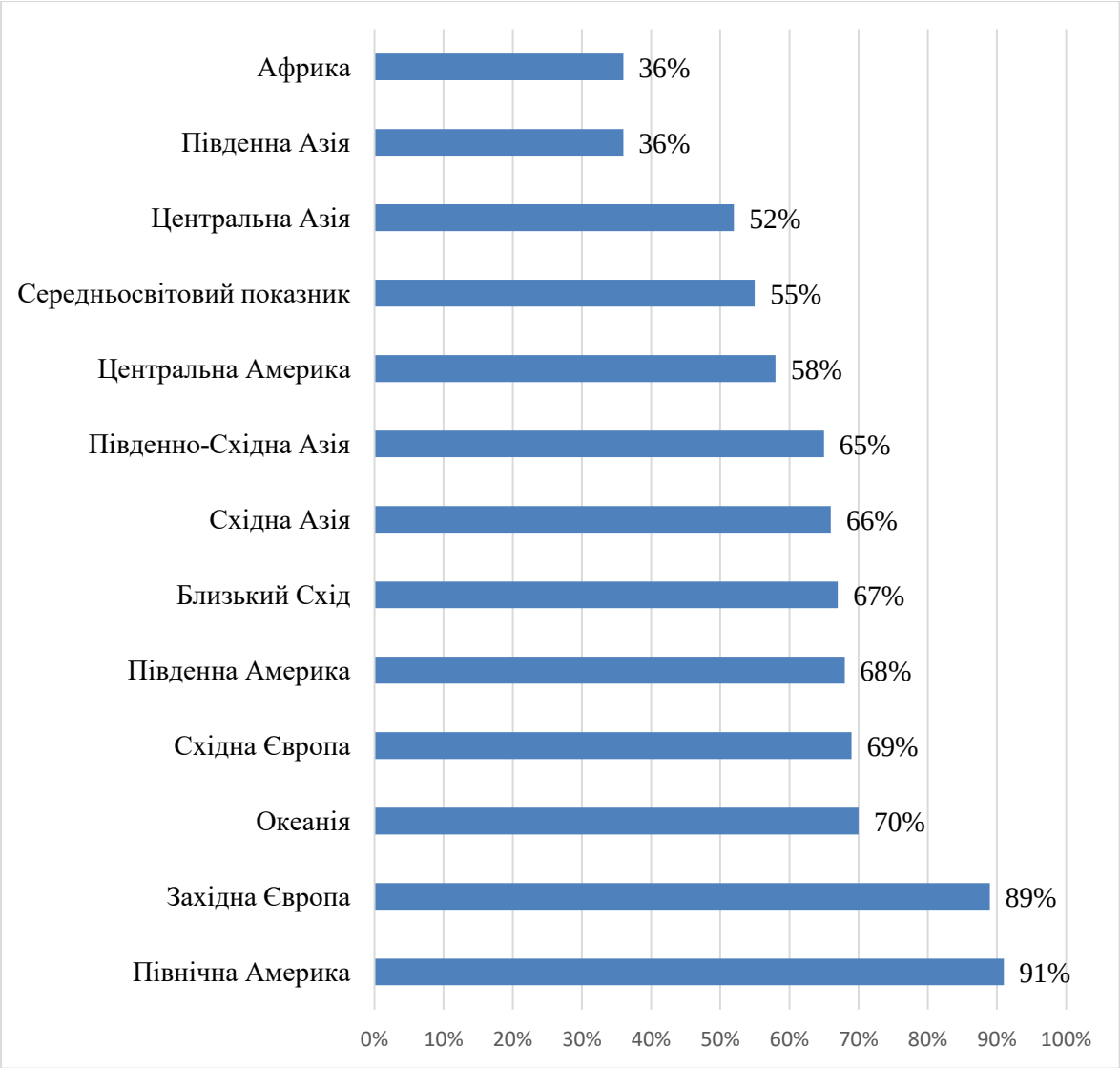


Рис. 2.1. Рівні проникнення Інтернету в світі за станом на вересень 2018 р., з розбивкою по регіонах [72]

У міру підвищення надійності доступу в Інтернет і збільшення кількості людей, що підключаються до Інтернету, зростає кількість важливих послуг, що надаються в режимі онлайн. Наприклад, підключення до Інтернету є дуже швидким і дуже надійним в Південній Кореї. За оцінками Організації економічного співробітництва і розвитку (ОЕСР) в 2018 році рівень проникнення Інтернету в домогосподарствах в Південній Кореї склав 99,5% [88].

При такій великій кількості людей, підключених до Інтернету, корейський уряд і комерційні структури пропонують все більше онлайнових послуг. Наприклад, якщо ви отримуєте квитанцію на оплату штрафу за перевищення швидкості (автоматично

з підключенням до Інтернету камери фіксації порушень швидкісного режиму), ви можете зайти на урядовий веб-сайт, щоб переглянути інформацію по своїй штрафній квитанції. Потім ви можете негайно сплатити штраф через систему банківських електронних платежів. Цей процес розрахунку може бути повністю безпаперовий. У деяких випадках кількість державних послуг, що надаються офлайн, менша за кількість онлайнових послуг.

В даний час в Китаї склалася схожа ситуація, тільки в ще більших масштабах. Згідно 41-му Статистичному звіту про розвиток Інтернету в Китаї, опублікованому в січні 2018 року, станом на кінець грудня 2017 року кількість користувачів Інтернету в Китаї досягла 772 мільйонів чоловік, збільшившись на 40,74 мільйонів у порівнянні з кінцем 2016 року. Рівень Інтернет-проникнення досяг 55,8%, що на 2,6% більше, ніж у кінці 2016 року. Число користувачів мобільного Інтернету в Китаї досягло 753 мільйонів осіб, що на 57,34 мільйонів більше порівняно з кінцем 2016 року [72].

До таких Інтернет-послуг, як миттєвий обмін повідомленнями, онлайн-платежі, онлайн-покупки, онлайн-доставка їжі або онлайн-бронювання поїздок, звертаються сотні мільйонів користувачів. Такі програми, як WeChat (інструмент для миттєвого обміну повідомленнями) і Alipay (система платежів на користь третіх осіб), стали важливими додатками практично для кожного смартфона.

Мобільні пристрої, мобільний Інтернет і ці додатки настільки популярні, що державні послуги, платежі, інвестиції, громадський і приватний транспорт і багато інших послуг повністю інтегровані з ними. В умовах, коли критично важливі послуги все частіше пропонуються в режимі онлайн, причому іноді це супроводжується скороченням кількості офлайнових послуг, також з'являється все більше можливостей для зловживання технологіями і вчинення злочинів.

Слід зазначити, що далеко не всі випадки порушення законодавства в галузі інформаційних технологій або із застосуванням технічних пристроїв нового покоління мають на меті збагачення. Так, з певною часткою ймовірності, можна припустити, що багато злочинців в інформаційній сфері використовують свої виключні навички для отримання для існування, але найчастіше, взломи, розкриття конфіденційних даних пов'язані зі спробою інформаційних активістів вплинути на

громадську думку, змінити хід політичних процесів, донести повідомлення до мас або поширити певну ідею.

Одним з яскравих прикладів, такого роду злочинів, є атака, здійснена на дипломатичні і політичні інформаційні мережі різних країн світу в 2009 році, тоді, в першу чергу, під атаку потрапили кілька комп'ютерів, розташованих в представництві тибетського уряду і особисто Далай Лами, операція була проведена за допомогою декількох пристроїв, розташованих на території США і КНР. Як стверджують фахівці, метою атак зловмисників стало отримання доступу до секретної інформації, шпигунство і отримання доступу до відеокамер і аудіомікрофонів представництв країн і недержавних органів по всьому світу. Операція отримала назву «Далай Лама під ковпаком» [84].

Так само, ще одним відомим випадком стала кібер-атака, вчинена з використанням вірусної платформи «Stuxnet», яка за неофіційними даними розроблена групою фахівців зі Сполучених Штатів Америки та Ізраїлю, створена спеціально для саботування Іранської ядерної програми.

Відмінною особливістю даного шкідливого ПЗ було те, що він міг нашкодити не тільки інформаційній та мережевій інфраструктурі, а й фізично пошкоджувати носії, перевантажуючи внутрішні механічні процеси технологічних пристроїв і в першу чергу жорсткі носії, які і були основними цілями даного вірусу. Крім цього, даний вірус зміг вивести з ладу більше 1 тисячі збагачувальних центрифуг на атомному об'єкті в м.Натанз.

Однак такий випадок далеко не єдиний, крім цього, такі міжнародні угруповання користувачів, які часто задовольняючи свої цілі, переступають законодавчо-зафіксовані норми «в ім'я загального блага». Тому, в рамках даного дослідження, необхідно відзначити найбільш яскравих представників з числа міжнародних злочинних угруповань, що діють та існують в межах інформаційних систем, що діють, досить імовірно, з політичних поглядів.

1. Перша хакерська група «Анонімний інтернаціонал» або як вона була названа для простоти освітлення спільнотою «Шалтай Болтай», оскільки всі повідомлення і

«зливи» інформації, що публікувалися в мережі учасниками даного об'єднання, публікувалися від імені казкового персонажу.

2. Наступним угрупуванням, що здійснювало політичні атаки була хакерська група під назвою «LulzSec» або «TheLulz Boat», початковим девізом якої було «сміємося над вашого захисту (кібер) з 2011 року». Незважаючи на свою порівняно невелику історію (учасники були затримані в червні 2011 року), угруповання створене спочатку «заради сміху» відзначилося серією гучних злочинів проти інформаційних мереж не тільки компаній, які вважалися захищеними на той момент, а й офіційних сайтів Сенату Сполучених Штатів Америки, сайту Центрального Розвідувального управління США, сайту компанії Sony (11 мільйонів облікових записів) і соціальної мережі для військовослужбовців (на якій вони зламали 170 тисяч особистих сторінок), а так само різні компрометуючі дані про чиновників і представників військової еліти США [96].

Учасники хакерського угруповання викладали всю відкриту конфіденційну інформацію в мережу, і так само відкрито підтримували засновника «WikiLeaks» Д.Ассанжа. В одному з інтерв'ю, учасник проекту «ЛулзСек», хакер під псевдонімом Вир, який називав себе «капітаном судна Лулзім», уточнив, що угруповання спочатку налічувала 6 фахівців, які спочатку діяли заради сміху, але після, перейшли на «політично мотивовані атаки».

3. Ще однією групою хакерів, які вчиняють злочини, виходячи зі своїх політичних поглядів є «Сирійська Електронна Армія» (Syrian Electronic Army). Появу цього угруповання пов'язують з початком громадянської війни в Сирії в 2011 році. Група фахівців, яка підтримує президента країни Башара Асада за заявами експертів причетна до багатьох гучних політичних випадків в інформаційному просторі серед яких: взлом сайтів новинних агентств «Нью-Йорк Таймс» і «Хаффлінгтон Пост» та інших значущих ЗМІ в 2014 році, акаунтів колишнього Президента США Б.Обами, і колишнього президента Франції – Ніколя Саркозі [101, с.25].

Крім цього угруповання причетне до взлому сайту корпусу морської піхоти США, на якому вона розмістила повідомлення про те, що Сирійська Армія не повинна бути ворогом США, навпаки – вона повинна стати їх союзниками, і блокування сайту

армії США і розміщенні повідомлень про зв'язок військових відомств Америки з підготовкою бійців опозиційної армії. Це робиться, за словами самих представників угруповання на їх офіційні звернення, для того, щоб підносити інформацію про конфлікт в Сирії з урядової точки зору, на противагу тій, яка підноситься західними політиками і ЗМІ.

4. Такими ж методами і засобами вчинення злочинів в інформаційному середовищі користується організація FancyBearz, цілями яких стають державні представники різних країн, включаючи США і Німеччину, а також Міжнародний Олімпійський Комітет, і антидопінгове агентство – WADA.

Дане угруповання звинувачується так само у взломі урядових інформаційних систем Німеччини, в отриманні доступу до серверів партії ХДС і особистому листуванні канцлера Німеччини Ангели Меркель. Німецькі фахівці відомчих служб відмовилися підтвердити зв'язок даних атак з російськими хакерами, проте, помічається, що дані хакери вже відомі своїми атаками на внутрішні мережі Бундестагу і, ймовірно, пов'язані з Головним Розвідувальним Управлінням ЗС Російської Федерації.

5. Слід зазначити, що навіть серед такого роду акторів відзначаються найбільш активні в прояві своєї позиції і найбільш серйозні в діях і методах спільноти, прикладом таких є група хакерів відома як Анонімні або Невідомі (Anonimous) – міжнародне угрупування, яке налічує численний склад учасників по всьому світу.

Фахівці цього угруповання злочинців діють досить давно, приблизно з 2003 року, і їх цілями стають урядові мережі, релігійні та корпоративні веб-сторінки, акаунти чиновників і громадських діячів. Дана група використовує всі методи здійснення кіберзлочини для просування політичних ідей і поширення свободи слова, захисту прав людини, свободи обігу інформації. Девізом цієї організації є поєднання пропозицій: «Нас багато, ми не забуваємо, ми не прощаємо, очікуйте нас» [103, с.407].

Неоднозначність поведінки даного угруповання дозволила утворитися масі чуток і легенд навколо їх істинних цілей, однак факти говорять про те, що даний рух на меті бачить свободу слова та інформації, розкриття корпоративної брехні і нерівності, а так само досягнення політичної правди, що робить дане угруповання

швидше «ідеєю руху» по всьому світу, особливо, з урахуванням закликів до участі, які «хактивісти» залишають після ряду атак.

Найгучнішими справами в рамках діяльності групи «Невідомих» також стали: злом інформаційних мереж компанії Booz Allen Hamilton, що співпрацює з міністерством оборони, розвідувальними службами і великими виробниками озброєнь, а так самих систем безпеки інформаційних структур для уряду США. Пірати виклали на своєму сайті PirateBay файл, який містить понад 90 тисяч електронних адрес, паролів, особисту інформацію, з метою підкреслити слабкості в системах захисту фірми, яка займається розробкою програмного забезпечення для запобігання кіберзлочинів і атак. Крім цього випадку, «Anonimous» відзначилися вельми неоднозначною дією, коли в листопаді 2015 року здійснили атаку акаунтів Ісламської Держави в різних соціальних мережах. У відповідь на теракти скоєні в Парижі раніше, «Anonimous» оголосили кібер-війну бойовикам ІГ, заявивши при цьому, що їх можливості щодо стримування Ісламської Держави в Інтернеті набагато вище, ніж у будь-якої держави світу, і вони спрямують всі зусилля щодо стримування активності терористів в мережі. Так само ЗМІ говорять про причетність групи «Anonimous» до взлому близько 500 сайтів на території КНР, включаючи урядові ресурси, із закликом до громадян Китаю приєднуватися до опору проти строгості режиму і контролю життя громадян. Крім цього на зламаних сторінках, «хактивісти» розміщували інформацію про те, як обходити цензуру в інтернет мережі [101, с.47].

Так само активісти цього угруповання на основі вивченої інформації можуть бути причетні до операцій, які в інформаційному середовищі отримали назви «Відплата» (Operation Payback) в 2010 році, коли у відповідь на заморозку платіжних систем переказів платежів сайту WikiLeaks, хакерські атаки обрушилися на платіжні системи Visa і MasterCard, а так же операції «Захопи Уолл-Стріт» (Occupy Wall Street) в 2011 році, за атакам на сайт Нью-Йоркської біржі в боротьбі проти соціальної і економічної нерівності в світі.

Крім перерахованих акцій слід відзначити, що даний рух має сторінки в різних соціальних мережах, де в різні періоди публікуються їхні заяви щодо будь-яких подій або особистостей. Так наприклад на їх сторінці містяться відео-міркування на тему

минулих виборів в США, які містять інформацію, ймовірно, здобуту нелегальним шляхом, що ганьбить честь і гідність Президента США Д. Трампа, зі звинуваченнями в хибності заяв, припущенні про майбутнє Сполучених Штатів Америки під час президентського терміну і відео-розслідування обставин смерті Аарона Шварца, інтернет-активіста і борця за вільне поширення інформації, до яких привели численні порушення конституції з боку представників влади, зі звіинуваченнями в «доведенні до самогубства», на додаток до цього, активісти зламали сайт Комісії з виконання покарань США, розмістивши там загрозливе повідомлення для співробітників.

Крім цього, в тому ж 2014 році, невідомими фахівцями була здійснена масова атака інформаційних мереж і серверів, що обслуговують державні органи Німеччини. Під час атаки був отриманий доступ до 14 парламентських серверів Бундестагу, які містили паролі і коди доступу до всіх урядових баз даних. Про те, яка інформація була викрадена з інформаційних мереж, питання залишається відкритим, але серед підозрюваних співробітники спецслужб Німеччини, в першу чергу, вказують російських хакерів, які, на їхню думку, намагалися отримати доступ до листування представників влади ФРН [73, с.11].

Ще одним яскравим прикладом є кібератака, виконана на інформаційні мережі представництва Демократичної Партії Сполучених Штатів Америки в 2016 році, тоді, в зв'язку з втручанням в роботу систем і серверів Національного Комітету, на сайті «Wikileaks», були опубліковані особисті листи, а так само інший цифровий контент, призначений для внутрішнього користування представників партії. Дана інформація, як стверджується дослідниками, могла стати причиною підриву довіри серед виборців до кандидата від Демократичної Партії США, і прямим чином вплинути на підсумки голосування.

Більш того, на хід цих виборів, як відображають дослідники і засоби масової інформації могла вплинути так само і інтернет-пропагангда, з розміщенням помилкових новин і розслідувань [102, с.58].

Представлений в дослідженні перелік лише частково відображає загальну тенденцію почастішання випадків проникнення, отримання незаконного доступу, взлому і використання інформаційних мереж урядів, представництв держав,

організацій, фондів і т.д. з метою зміни політичної ситуації, донесення певної позиції, впливу на політичні процеси.

2.3. Кіберзлочинність та кібертероризм в умовах діджиталізації

Кіберзлочини, зважаючи на їх відносну некараність, а також високу прибутковість, є досить привабливим видом діяльності. Ризики і витрати при здійсненні кіберзлочинів рівні з ризиками і витратами при здійсненні легальної трудової діяльності (виробничий травматизм, монотонність праці, стреси, ризик скорочення і т.д.) [21].

Поширення інтернету призвело до усунення національності кіберзлочинності, зробило її справді інтернаціональною. Хакер може мати громадянство однієї країни, перебувати на території іншої і при цьому працювати через сервер, розташований в третій країні. Транскордонність кіберзлочинності дає можливість для здійснення розкрадань і переведення в готівку грошей в абсолютно віддалених один від одного країнах.

Місце знаходження злочинця і факт вчинення злочинних дій, збір доказів є важким для правоохоронних органів, як і здійснення процесуальних дій. Тривалість самих атак при цьому варіюється в досить великому часовому інтервалі: від декількох секунд до діб і місяців. Завдяки попередньо запровадженому програмному забезпеченню, злочинці можуть використовувати при проведенні хакерських атак величезну кількість комп'ютерів (іноді рахунок йде на сотні тисяч).

Інформація, що знаходиться в корпоративних системах, стає все більш привабливою здобиччю не тільки для сторонніх хакерів, але і для власних співробітників компаній. Особливу небезпеку становлять системні адміністратори, які втратили лояльність до своєї компанії, тим більше така ситуація набуває широкого поширення в умовах економічної кризи. Сучасні кіберзлочинці, як будь-які професіонали, фінансово мотивовані, і продаж конфіденційних відомостей, особливо про юридичних осіб, став невід'ємною частиною економічної злочинності. Даний вид

злочинної діяльності став свого роду бізнесом, якому деякі готові присвятити все життя [26, с.47].

Кіберзлочинність поступово трансформувалася в великий, широко розгалужений бізнес з доходами, які можна порівняти з доходами від наркоторгівлі. У багатьох випадках хакери стали частиною організованої економічної злочинної діяльності, надавши свої знання, вміння в якості послуг різного роду шахраям, терористам, торговцям зброєю, наркотиками заради досягнення корисливих економічних цілей в особливо великих розмірах.

Форми кіберзлочинності видозмінюються і поширюються на все нові досягнення науково-технічного прогресу. Підвищену увагу спрямовано на соціальні мережі та мобільні пристрої – область, в якій користувачі менш інформовані про кіберзагрози. Хакерські атаки стали більш складними і професійними, спрямованими не тільки на окремих користувачів, а й промислові системи. У зв’язку з масовою діджиталізацією, кіберзлочинність набуває все істотнішого значення в сучасному світі.

Відбулася певна переорієнтація спрямованості кіберзлочинності на отримання переважно фінансового результату. На відміну від поширення вірусів, спрямованих на створення бот-мереж (поширення ботнетів - мереж інфікованих комп'ютерів), які здійснюють атаки незалежно від користувачів та завдають шкоди великій кількості користувачів, цільові атаки хакерів орієнтовані на конкретне підприємство або конкретного користувача. Такі дії пов'язані з попереднім вивченням хакерами свого об'єкта нападу. Сторона нападу здійснює атаку в несподіваний момент, після добірки необхідних інструментів, і діє майже безслідно. Комп'ютерне шпигунство, операції з комп'ютерними системами не тільки складно зафіксувати і довести як протиправні дії, але і точно персоніфікувати порушника і його географічне місцезнаходження [23, с.58].

Досить легкою жертвою кіберзлочинності є підприємства малого і середнього бізнесу (МСБ). Зростання кіберзлочинності пов'язане переважно не з великими підприємствами, а саме з підприємствами типу МСБ. Такі підприємства в силу малого бюджету, відсутності кваліфікованих кадрів, прогалин в знаннях співробітників не

можуть на належному рівні забезпечити якісну інформаційну безпеку. Тим більше, що втрата даних або ж їх компрометація не впливають істотно на їх функціонування, положення на ринку, рівень довіри споживачів, нарешті, розмір одержуваного прибутку.

Питання, пов'язані з обсягом продажів, маркетингом, бухгалтерією, набагато в більшій мірі турбують власників підприємств малого і середнього бізнесу, ніж інформаційна безпека, яка фінансується, як правило, за залишковим принципом. Великі компанії, на відміну від малого та середнього бізнесу, не можуть дозволити собі зневажливу, епізодичну увагу до інформаційної безпеки в силу необхідності збільшення привабливості, підтримання належного рівня операційної ефективності бізнесу, постійного конкурентного тиску з боку ринку. Захист конфіденційної інформації, інтелектуальної власності має принципово важливе значення для успішного ведення бізнесу і вимагає розробки комплексної стратегії безпеки, виходячи з цілей діяльності компанії. Дані кроки повинні включати, в тому числі, надійні системи аутентифікації, моніторингу, обмін інформацією про загрози безпеки зі спеціалізованими компаніями [1, с.57].

Багато компаній не завжди афішують факт впливу на них комп'ютерних атак з побоювань втрати репутації. Багато жертв кіберзлочинців не звертаються за допомогою, в тому числі через відсутність надії знайти винних і компенсації заподіяної шкоди. Слабким місцем запобігання кіберзлочинів є відсутність обов'язкової вимоги про необхідність інформування правоохоронних органів про скоєні атаки. Об'єднання зусиль компаній по боротьбі з кіберзлочинністю, їх відкритість, встановлення єдиних пріоритетів безпеки і якості продукції може реально підвищити безпеку кіберпростору. Запобігання негативного впливу хакерських атак на компанії можливе лише в тому випадку, якщо самі компанії визначать кібербезпеку як найважливіший елемент стратегії свого розвитку.

Що стосується такого явища як комп'ютерний тероризм (кібертероризм), то це залякування громадян та органів влади з метою досягнення злочинних намірів. Це проявляється в загрозі насильства, підтримки стану постійного страху з метою досягнення певних політичних чи інших цілей, примусу до певних дій, привернути

увагу до особистості кібертерориста або терористичної організації, яку він представляє. Заподіяння або загроза заподіяння шкоди є своєрідним попередженням про можливість заподіяння більш тяжких наслідків, якщо умови кібертерориста не будуть виконані. Характерною особливістю кібертероризму і його відмінністю від кіберзлочинності є його відкритість, коли умови терориста широко сповіщаються [1, с.74].

Кібертероризм – це серйозна загроза людству, порівнянна з ядерною, бактеріологічною і хімічною зброєю, причому ступінь цієї загрози в силу своєї новизни не до кінця ще усвідомлений і вивчений. Досвід, який вже є у світової спільноти в цій області, з усією очевидністю свідчить про безсумнівну уразливість будь-якої держави, тим більше що кібертероризм не має державних кордонів, кібертерорист здатний в рівній мірі загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі.

Виявити і нейтралізувати віртуального терориста вельми складно через надто малу кількість його слідів, на відміну від реального світу, де слідів скоєного залишається все ж більше. Особливу заклопотаність у правоохоронних органів викликають терористичні акти, пов'язані з використанням глобальної мережі Інтернет, з відкритих джерел якої, як стверджує ФБР, можна отримати технологію виготовлення біологічної, хімічної і навіть ядерної зброї терористів [12, с.272]

Визначаючи сучасний стан кіберзлочинності в Україні, слід указати, що вона, як і будь-яке інше соціальне явище, піддається оцінюванню за допомогою певних критеріїв, що свідчать про її кількісні та якісні характеристики. Здійснити таке оцінювання можна через аналіз показників поширеності кіберзлочинності в Україні: її рівня, географії, структури, динаміки тощо.

Стосовно рівня кіберзлочинності та її динаміки варто зазначити, що у 2009 р. в України було зареєстровано 217 злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, у 2010 р. – 190, у 2011 р. – 131, у 2012 р. – 138, у 2013 р. – 595, у 2014 р. – 443, у 2015 р. – 598, у 2016 р. – 865, у 2017 р. – 2573, 2018 р. – 3021 злочинів (Рис.2.2).

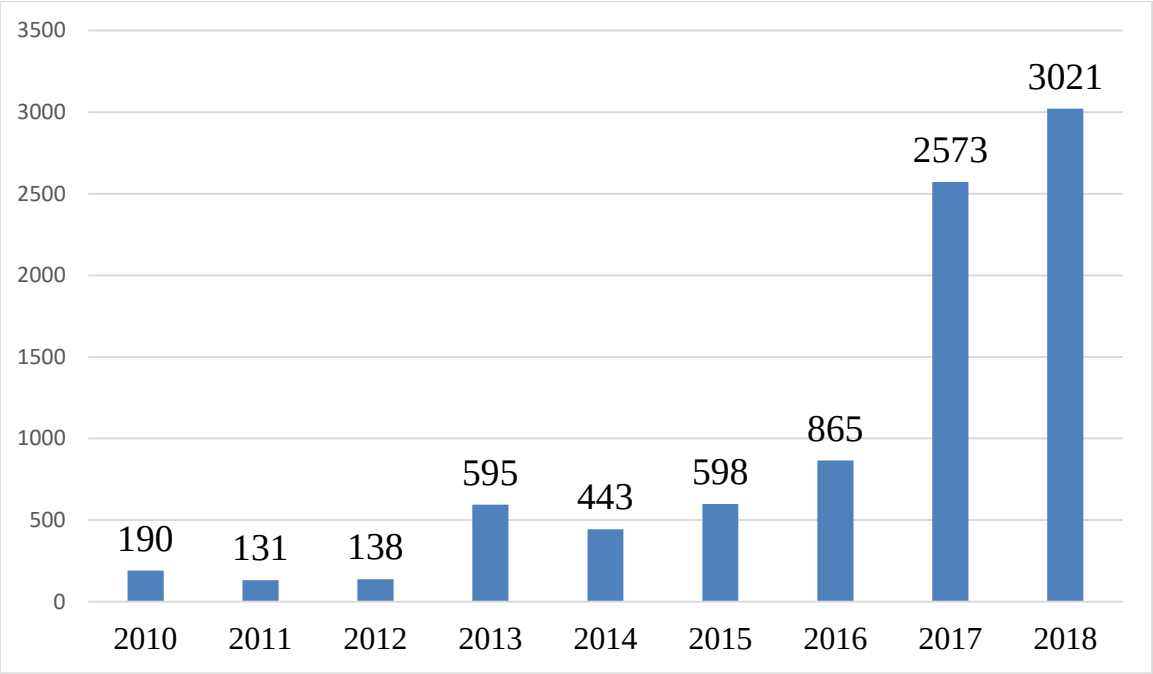


Рис. 2.2. Графічне зображення рівня та динаміки кіберзлочинності в Україні за 2010 – 2018 рр.. [6, с.11]

Суттєве збільшення кількості зареєстрованих у 2013 р. кіберзлочинів окремі вчені пов'язують із тим, що «зростання вказаного виду злочинності обумовлено щорічним зростанням користувачів Інтернет-ресурсу в Україні» [6, с. 10], інші пов'язують різницю в даних, що стосуються обліку зареєстрованих злочинів, з переданням права формувати державну статистику про стан злочинності в державі від МВС до прокуратури України.

Для розуміння природного перебігу речей та відсутності істотного коливання достатньо звернути увагу на питому вагу кіберзлочинів у загальній кількості зареєстрованих злочинів, що у 2013 р. відповідала 0,11 %. Аналогічні показники простежуються також у 2015 р., і навпаки, у 2014 р. відбулося зниження кількості зареєстрованих кіберзлочинів.

Разом із цим особливо відчутне зростання рівня кіберзлочинності відбулося у 2017 р. (більш ніж у чотири рази порівняно з 2013 р.), і це свідчить про наявність специфічних рис досліджуваного виду злочинів, пов'язаних з особливостями комплексу факторів його детермінації, як-то:

- стрімке розгортання процесу інформатизації суспільства (упровадження мережі третього покоління (3G) операторами мобільного зв'язку),
- освоювання кібертехнологій як засобу злочинної діяльності,
- об'єктивне відставання технічної складової правоохоронної системи (активна фаза реформування органів Національної поліції України, відсутність достатньої кількості фахівців та недостатнє фінансування) тощо.

Статистичний аналіз географічної поширеності кіберзлочинів в Україні за останні роки виявив залежність від фактору урбанізації. Найвища кіберкримінальна активність фіксується за ранжиром у Дніпропетровській області, м. Києві, а також у Харківській, Запорізькій та Черкаській областях; найнижча – в Чернівецькій, Херсонській, Сумській і Кіровоградській [6. с.12].

Відповідні географічні особливості вчинення кіберзлочинів в Україні слід розглядати не стільки через призму переважання на мапі кіберзлочинів східних областей порівняно із західними (що традиційно пояснюється низкою чинників, як-то: густота населення, яка на Сході нашої держави є вищою ніж на Заході, історичні та культурологічні передумови тощо), скільки через призму переважання промислово та фінансово розвинутих областей (центрів).

Саме технічний (відповідно, й фінансовий) розвиток є неможливим без залучення сучасних, перш за все інформаційних технологій, середовище яких і є середовищем кіберзлочинності. При цьому аналіз «географічних» особливостей окремих видів кіберзлочинів дозволив виявити таку специфіку. Деякі злочини мають традиційну «приналежність» за місцем вчинення переважно до великих міст.

Це такі злочини, як створення з метою використання, розповсюдження або збуту шкідливих програм чи технічних засобів, а також їх розповсюдження або збут; несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації та порушення правил експлуатації автоматизованих ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється.

Такий злочин, як несанкціоноване втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, маючи спочатку переважно приналежність до великих міст, останнім часом дедалі більше (в середньому 50 %) учиняється у містах та селищах міського типу.

Що стосується несанкціонованих дії з інформацією, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах і комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, то цей злочин порівняно з іншими кіберзлочинами має найбільш виражену тенденцію стрімкої «переорієнтації» на невеликі міста та сільську місцевість.

Статистичні дані, що характеризують показники злочинності в Україні за 2018 р., дозволяють зробити висновок, що кіберзлочинність становить 0,49 % (при цьому злочини проти волі, честі та гідності особи складають 0,18 %, а злочини проти статевої свободи та статевої недоторканості особи – 0,16 %) від загальної кількості злочинів, облікованих у звітному періоді [6, с.13].

Висновки до Розділу 2

Таким чином, виходячи з викладеного матеріалу, можна зробити висновки про те, що феномен кіберзлочинів, не є новим для сучасної науки, хоча, при цьому, і вимагає подальшого вивчення, особливо в питаннях точності і визначенні самого поняття. Була зроблена спроба визначення деяких суміжних понять, таких як ІКТ, «кіберзлочинність», «кібербезпека».

Основні характеристики, що відрізняють даний вид правопорушень від інших злочинних діянь: велика ймовірність приховування даних, складності при проведенні слідства, зважаючи на обмеженість інформації, неможливість уніфікації національних законодавств і підходів до слідства в даній області, складності в процесі збору даних, визначення складу злочину і ін. Більш того, автором відзначена тенденція до збільшення впливу такого аспекту, як транскордонність даних правопорушень.

Серед основних країн, які постраждали від кіберзочинності, відзначаються країни Північної Америки зокрема США, Канада, країни Європейського Союзу. Дана географія поширення безпосередньо пов'язана з рівнем технологічного розвитку держави, і інтенсивності використання інформаційних систем в бізнес-структурах, громадських інститутів, і особистого життя громадян, на території перелічених країн.

В розділі також було розглянуто низку резонансних випадків кіберзлочинів, які зачіпають політичні процеси в різних країнах, зокрема США, Ірані, Німеччині для підтвердження тези про те, що найчастіше кіберзлочини є «політично мотивованими». Таким чином, «політичні кіберзлочини» – це ті, що здійснюються за допомогою технічних засобів, пов'язаних між собою інтернетом і з політичних мотивів, протиправні діяння, спрямовані на технічні засоби та інформаційні системи державних органів і ЗМІ, з метою підриву, послаблення або зміни існуючого політичного режиму, державних інститутів або політичних процесів.

РОЗДІЛ 3. ЗАХОДИ ДЕРЖАВНОЇ ПОЛІТИКИ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ: СВІТОВИЙ ТА ВІТЧИЗНЯНИЙ ДОСВІД

3.1. Світовий досвід боротьби із кіберзлочинністю (на прикладі ЄС, НАТО та Інтерполу)

Кожна держава постійно балансує між принципами дотримання прав і свобод людини і громадянина, інтеграцією в міжнародне співтовариство, необхідністю забезпечення економічного зростання і національної безпеки, в тому числі за допомогою обмеження прав і свобод людини і громадянина, встановлення адміністративних форм обмеження підприємницької діяльності, захисту власних інтересів на міжнародній арені.

Вибір здійснює і населення, і органи публічної влади, однак в переліку сфер жодні внутрішні причини не повинні переважувати необхідність міжнародного співробітництва в боротьбі зі злочинами, яке повинно будуватися на принципах відкритості, взаємодопомоги, активності в розробці нових форм взаємодії. Міжнародне співробітництво в боротьбі з кіберзлочинністю необхідно здійснювати на основі участі всіх країн, що зумовлюється властивістю самої інформації, як об'єкта посягання, так і характером скоєних злочинів [70, с.21].

Дійсно, в сучасному світі всі сфери життєдіяльності знаходяться в прямій залежності від роботи обчислювальних і інформаційних мереж. Разом з тим широке використання для обробки інформації засобів обчислювальної техніки з програмним забезпеченням, що дозволяє порівняно легко модифікувати, копіювати і руйнувати інформацію, підвищує вразливість інформаційного простору [2, с. 4]

Користувачі інформаційних систем без достатніх для цього підстав вірять в відсутність кібератак, використовуючи інформаційний простір з незнанням обмежень і загроз безпеки системи [66, с.5-6].

У сучасному світі інформація виступає найважливішим компонентом розвитку суспільства. Перетворення постіндустріального суспільства в суспільство інформаційне означає, що інформація набуває глобального характеру, стає значущою

як для людини особисто, так для держави і суспільства в цілому, кожен може шукати, одержувати, зберігати, використовувати і поширювати інформацію будь-яким законним способом, не існує кордонів для її потоку. На даний момент інформація визнається однією з найважливіших цінностей, відповідно, її захист є не менш важливою діяльністю, ніж її отримання та передача, отже, в діджіталізованому суспільстві початку XXI ст. сфера прояву ризику змінюється [74, с.140].

Дуже важливо розуміти глобальність проблеми кіберзлочинності. Так, вже зараз кібератаки паралізують роботу не тільки приватних структур, а й державних органів, в світі не існує держави, яка було б захищене від подібного роду атак. В якості ймовірних джерел кіберзагроз розглядаються не тільки хакери або їх групи, але також окремі держави, терористичні, злочинні угруповання. При виробленні засобів і методів боротьби з кіберзлочинністю слід пам'ятати про латентність даного виду злочинів. За оцінками експертів, латентність «комп'ютерних злочинів» в США досягає 80%, у Великобританії – 85%, у ФРН – 75%, в Україні – понад 90% [72].

За даними міжнародної служби з забезпечення безпеки в області кіберзагроз Symantec Security, кожну секунду в світі жертвами кібератаки стають 12 осіб, а щорічно в світі реєструється близько 556 млн кіберзлочинів, збитки від яких становлять понад 100 млрд дол. США [4, с. 46].

Кіберзлочинність може порушувати інтереси як держави, так і окремої людини. Безперечно, особливості функціонування інформаційних систем, перш за все мережі Інтернет, вимагають, щоб на вирішення питань кібербезпеки були звернені спільні зусилля різних суб'єктів, як державних, так і приватних [73, с.11], однак саме держава може і повинна, а головне, тільки вона здатна ефективно здійснювати повномасштабну протидію скоєнню кіберзлочинів, створювати умови для того, щоб ті, хто в найбільшій мірі схильний до нападу кіберзлочинців (наприклад, банки, фізичні особи), могли вибудовувати більш надійну систему інформаційного захисту.

В даний час провідні країни світу активно розширюють і створюють в збройних силах і спецслужбах підрозділи, які повинні забезпечувати розвиток наступальних можливостей в кіберпросторі (Таблиця 3.1).

Таблиця 3.1

Підрозділи в спецслужбах країн з питань кібербезпеки [96]

Країна	Участь в Конвенції про кіберзлочинність	Розробка Конвенції ООН «Про забезпечення міжнародної інформаційної безпеки»	Основні організації в області кібербезпеки
Великобританія	+	-	Група безпеки електронної комунікації при Центрі правової зв'язку при МЗС; підрозділ Міністерства оборони щодо захисту від віртуальних загроз
Німеччина	+	-	Спеціальна група при МВС ФРН
Індія	+	-	Аналітичний і дослідницький відділи зовнішньої розвідки і розвідувальне бюро внутрішньої розвідки
Китай	-	+	Реалізація програми захисту від несанкціонованого підключення до комп'ютера
США	+	-	Центр національної кібербезпеки; Об'єднане кібернетичне командування Збройних сил США

Наприклад, в США поряд з уже функціонуючим Центром національної кібербезпеки (National Cyber Security Center) у складі Збройних сил сформовано Об'єднане кібернетичне командування (Unified US Cyber Command), яке в глобальному масштабі має координувати зусилля всіх структур Пентагону в ході ведення бойових дій, надавати відповідну підтримку цивільним федеральним установам, а також взаємодіяти з аналогічними за завданнями відомствами інших країн [86].

Разом з тим зазначені організації – частково підконтрольні відомства, оскільки верховною контролюючою структурою є Рада національної безпеки зі спеціальним

комітетом, до сфери відповідальності яких входить реалізація інформаційної стратегії [90, с.239], в тому числі по боротьбі і з кіберзлочинністю.

У Великобританії реалізуються програми зі створення кіберзброї, які забезпечать здатність влади протистояти зростаючим загрозам з кіберпростору [96].

В Австралії створено групу координації безпеки електронної пошти (ESCG). Основним завданням цієї групи є створення безпечного і надійного електронного оперативного простору як для суспільного, так і для приватного секторів [101, с. 84].

Діяльність з протидії вчиненню кіберзлочинів здійснюють не тільки окремі держави, але і їх блоки, зокрема НАТО. Так, важливість даної проблеми знаходить відображення у всіх керівних документах блоку, прийнятих в останні роки. В стратегічну концепцію НАТО вперше включено положення про кіберпростір як нову сферу військової діяльності альянсу [98].

Іншими словами, в боротьбі з транскордонними злочинами, до яких можна віднести і значну частину кіберзлочинів, особлива роль відведена державам, і тільки при добре скоординованій роботі правоохоронних органів різних країн можливо знизити кількість злочинів, скоєних правопорушень в даній сфері. Міжнародне співробітництво здійснюється за кількома напрямками і передбачає насамперед створення нормативних актів і вироблення загальних рекомендацій, а також впровадження ефективних моделей організаційної взаємодії між державами. При цьому слід враховувати, що традиційні механізми міжнародного співробітництва, включаючи запити, взаємодопомогу та інші подібні інструменти, що застосовувалися в XIX в. і раніше, є невідповідними в еру, коли злочини можуть відбуватися з будь-якої точки земної кулі зі швидкістю світла.

Правове регулювання питань боротьби з кіберзлочинами є базисом всієї системи протидії кіберзлочинності. Складність вироблення міжнародних актів в цілому в ситуації, що розглядається, ускладнюється ще й тим, що існуючі закони важко застосовувати, коли мова йде про не піддаються локалізації атаках в планетарних масштабах, докази яких розкидані і віртуальні [66, с.4].

Міжнародне співтовариство на різних рівнях виробило ряд актів, що мають значення для боротьби з кіберзлочинністю, причому особливу роль відіграють

регіональні акти, оскільки загальносвітові документи в даний час створити важко. Разом з тим не можна не відзначити спроби держав поширити норми глобальних міжнародних договорів на боротьбу з кіберзлочинністю або укласти нові договори. Наприклад, так як в кіберпросторі поряд з окремими особами можуть діяти і організовані злочинні групи, існує можливість застосування до них міжнародних договорів, спрямованих на боротьбу з організованою злочинністю, зокрема Конвенції ООН проти транснаціональної організованої злочинності від 15 листопада 2000 р. [75].

Крім того, розроблена концепція Конвенції ООН про забезпечення міжнародної інформаційної безпеки, яка була представлена міжнародній спільноті в листопаді 2011 р. на конференції в Лондоні і включає преамбулу, 23 статті, об'єднані в основну частину, і заключні положення. Основна частина документа складається з п'яти розділів, зміст яких знаходиться в єдиній композиційній цілісності.

Важливо, що в ст. 4 Конвенції закріплені основні загрози міжнародному миру і безпеці в інформаційному просторі, з яких виділено 11 базових і 4 додаткових. Серед базових названі, наприклад, використання інформаційних технологій і засобів для здійснення ворожих дій і актів агресії; цілеспрямований деструктивний вплив в інформаційному просторі на критично важливі структури іншої держави; транскордонне поширення інформації, що суперечить принципам і нормам міжнародного права, а також національним законодавствам держав. Знову ж в документі не вказані такі реальні загрози міжнародній безпеці, як вчинення кіберзлочинів, розповсюдження наркотичних і психотропних засобів, їх аналогів, а також порнографії, в тому числі і дитячої. Крім цього, концепція Конвенції містить ст. 5, присвячену основним принципам забезпечення міжнародної інформаційної безпеки [75].

Аналіз представлених принципів дозволяє зробити висновок про те, що їх можна розділити на чотири групи:

- принципи участі держави в системі міжнародної інформаційної безпеки як члена міжнародного співтовариства;

- принципи, що дозволяють державі зберегти свій суверенітет в процесі міжнародного співробітництва в боротьбі з кіберзлочинністю;
- принципи забезпечення вільного інформаційного обміну між країнами
- четверта група принципів встановлює характер взаємодії держави і приватних суб'єктів в розглянутих відносинах.

Разом з тим знову доводиться констатувати, що в концепції Конвенції детально не прописані принципи міжнародного співробітництва в боротьбі з кіберзлочинами, крім спрямованої протидії терористичного характеру.

Позитивним слід визнати включення в концепцію Конвенції розділу 5 «Міжнародне співробітництво в сфері міжнародної інформаційної безпеки», однак заходи міжнародного співробітництва в даній сфері представляються недостатніми для ефективного функціонування системи міжнародної економічної безпеки, оскільки припускають лише обмін національними концепціями забезпечення безпеки в інформаційному просторі, оперативний обмін інформацією про кризові події і загрози в інформаційному просторі і вжиті заходи щодо їх врегулювання і нейтралізації, консультації з питань діяльності в інформаційному просторі, яка може викликати заклопотаність держав-учасників, і співпраця щодо врегулювання конфліктних ситуацій військового характеру. Разом з тим дані форми не враховують необхідність задоволення потреби в оперативній взаємодії правоохоронних органів з широкого кола питань. Таким чином, положення концепції Конвенції ООН про забезпечення міжнародної інформаційної безпеки мають досить компромісний характер і орієнтовані насамперед на попередження інформаційних воєн, тероризму [75].

Не можна не відзначити, що більшу частину спеціалізованих актів по боротьбі з кіберзлочинами складають акти Європейського союзу, який має одну з найбільш розвинених в світі систем забезпечення інформаційної безпеки. У 2001 Європейська комісія представила спеціальне повідомлення «Створення безпечного інформаційного суспільства за допомогою підвищення захищеності інформаційної інфраструктури і боротьби зі злочинами з використанням комп'ютерних засобів», в

якому містилися пропозиції правового та організаційного характеру щодо боротьби з кіберзлочинністю в Європейському союзі.

Програми Інтерполу будуються навколо підготовки операцій з боротьби з новими комп'ютерними погрозами. Вони спрямовані на:

- сприяння обміну інформацією між країнами-членами в рамках регіональних робочих груп та конференцій;
- підготовку навчальних курсів для створення і підтримки професійних стандартів;
- координацію та сприяння міжнародним операціям;
- створення глобального списку контактів для розслідування кіберзлочинів;
- надання допомоги країнам-членам у випадку кібератак або розслідування кіберзлочинів через бази даних;
- розробка стратегічного партнерства з іншими міжнародними організаціями та організаціями приватного сектору;
- виявлення нових загроз і передача розвідувальної інформації країнам-членам;
- забезпечення функціонування безпечного веб-порталу для доступу до оперативної інформації і документів [75].

Після техніко-економічного дослідження, проведеного соціологічною компанією Rand Corporation, Європейською комісією було прийнято рішення про створення в структурі Європейської поліцейської організації (Європолу) Європейського центру по кіберзлочинності (ЕС3) – European Cybercrime Centre (ЕС3). Центр покликаний виконувати функції координатора в боротьбі ЄС проти кіберзлочинності, сприяючи більш швидкій реакції на онлайн-злочини. Він надає підтримку державам-членам та інститутам Європейського союзу в побудові оперативного і аналітичного потенціалу для досліджень і співпраці з міжнародними партнерами. ЕС-3 офіційно почав свою діяльність у січні 2013 року з мандатом для вирішення поліцейських завдань в наступних областях кіберзлочинності:

- злочини, вчинені організованими групами з метою вилучення великих злочинних доходів, таких як онлайн-шахрайства;

- злочини, які заподіюють серйозної шкоди жертві, такі як сексуальна експлуатація дітей онлайн;
- злочини, які впливають на критичні інфраструктури та інформаційні системи в країнах Європейського союзу [94].

ЕС-3 прагне стати координаційним центром в боротьбі ЄС проти кіберзлочинності шляхом створення оперативного і аналітичного потенціалу для досліджень і співпраці з міжнародними партнерами у створенні простору ЄС, вільного від кіберзлочинності. Європейський центр кіберзлочинності розміщується в Гаазі (Нідерланди), і таким чином ЕС-3 може спиратися на існуючу інфраструктуру Європолу та мережу правоохоронних органів. Рада Програми ЕС-3 допомагає урядам країн ЄС в процесі управління подоланням кіберзлочинності.

Членами Ради Програми ЕС-3 в даний час є:

1. EUCTF (цільова група Європейського союзу з кіберзлочинності).
2. CIRCAMP (проект COSPOL щодо дитячої порнографії в Інтернеті).
3. ENISA (Агентство Європейської мережевої та інформаційної безпеки).
4. ECTEG (Європейська навчальна та освітня група з кіберзлочинності).
5. CEPOL (Європейський поліцейський коледж).
6. EUROJUST (Європейська організація судової співпраці).
7. CERT-EU (Європейська Команда відповідальності за комп'ютерну безпеку).
8. Міжнародна організація кримінальної поліції - Інтерпол.
9. Європейська комісія.
10. EEAS (Європейська служба зовнішніх дій) [91].

Подолання наслідків кіберзлочинності і її профілактика є дуже запитуваною темою для публічних послуг. Сьогодні не всі держави-члени досягли рівня ноухау, необхідного для початку ефективної боротьби з кіберзлочинністю. Кіберпідрозділи поліції в більшості країн ЄС часто не мають апаратного і програмного забезпечення, необхідного для виконання навіть простих судових експертиз.

ЕС-3 сприяє розвитку потенціалу держав-членів шляхом ув'язки фінансування ЄС з правоохоронними органами країн - членів Євросоюзу. Високий рівень підготовки фахівців з боротьби з кіберзлочинами буде наріжним каменем нового

проекту. ЕС-3 буде активно координувати розвиток технологій і підготовки фахівців в рамках програми Horizon-2020 [93].

Розслідування шахрайства в Інтернеті, жорстокого поводження з дітьми та іншими злочинами регулярно відкриває Європі сотні нових жертв від злочинців в різних частинах світу. Операції такого масштабу не можуть бути успішно завершені національними поліцейськими силами в поодинці. Саме тут Європейський центр кіберзлочинності має значну цінність.

Європол є спільнотою фахівців в Європі для оперативної підтримки, координації та експертизи в області кіберзлочинності. Європейський центр кіберзлочинності забезпечує більш широкі спільні заходи у співпраці з державами - членами ЄС, з іншими ключовими зацікавленими сторонами; країн, що не входять в ЄС; з міжнародними організаціями; з керівними органами та постачальниками інтернет-послуг, з компаніями, що займаються інтернет-безпекою фінансового сектора; з академічними експертами; з організаціями громадянського суспільства.

Іншими словами, сучасною тенденцією міжнародної протидії кіберзлочинності є розширення сфери взаємодії держав. Реальністю стає оперативне співробітництво правоохоронних органів з боротьби з кіберзлочинами (Інтерпол, Європол, Євроюст), створення і використання єдиної бази даних про кіберзлочинців, про вчинені і плановані кіберзлочини (перш за все працює в режимі 24/7). Відзначимо, що робота Інтерполу в плані оперативності обробки інформації менш ефективна, ніж спеціалізованих організацій меншого масштабу.

3.2. Механізми та принципи реалізації державної політики у сфері кібербезпеки

Державна політика в сфері національної безпеки і оборони спрямована на захист громадянина, а саме: його життя, честі і гідності, конституційних прав і свобод, створення безпечних умов життєдіяльності. Крім того, з огляду на складові національної безпеки, можемо відзначити, що така політика повинна забезпечувати захист суспільства і його демократичних цінностей, стійкий його розвиток, а також

держави. Це в свою чергу передбачає захист конституційного ладу, суверенітету, територіальної цілісності і недоторканності держави, навколишнього природного середовища і т.д.

Загрози національній безпеці України і відповідні пріоритети державної політики в сферах національної та громадської безпеки визначаються в Законі України «Про національну безпеку України», Стратегії національної безпеки України, Стратегії воєнної безпеки України, Стратегії кібербезпеки України та інших документах, які стосуються питань національної безпеки і оборони і визначаються Радою національної безпеки і оборони України, а також затверджуються указами Президента України.

Слід зазначити, що відповідно до цілей Стратегії розвитку системи Міністерства внутрішніх справ України до 2020 року (далі - МВС) планується створення безпечного середовища для існування і розвитку вільного суспільства. Передбачається, що досягнення цієї мети можливе за рахунок реалізації наступних заходів:

- формування і реалізації державної політики в сфері внутрішніх справ;
- зміцнення довіри до органів системи МВС з боку суспільства;
- забезпечення розвитку України як безпечної європейської держави, базис якого складають інтереси її громадян і висока ефективність всіх складових системи МВС [74, с. 140].

Реалізація цих заходів для України – серйозний етап в її розвитку, так як дана Стратегія сприятиме впровадженню євроінтеграційної політики в сфері внутрішніх справ. Таким чином, Україна досягне показників, необхідних для набуття повноправного членства України в Організації Північноатлантичного договору.

Проаналізувавши положення даної Стратегії, необхідно зазначити, що підходи (сервісні, соціально орієнтовані і т. д.), за допомогою яких буде забезпечуватися реалізація її цілей, вимагають уточнення в зв'язку з декларативністю принципів, які вони включають. Йдеться про те, що служіння суспільству (вказане як одне із завдань системи органів МВС) вже закріплено в Конституції України, і в даній Стратегії є апріорним постулатом. Положення цієї Стратегії вимагають доопрацювання у

напрямку приведення їх у відповідність з нормами Закону України «Про національну безпеку України» [48]. Так, в цьому Законі дається визначення національної безпеки як стану захищеності національних інтересів особистості, суспільства і держави. Разом з тим, Стратегія розвитку системи МВС України до 2020 року передбачає створення безпечного середовища та усунення негативного впливу сучасних викликів особистісної та суспільної безпеки.

Сучасні практики управління та інформаційна діяльність, які будуть впроваджуватися в ході виконання Стратегії, вимагатимуть значних фінансових вкладень.

На думку її розробників, джерелом поповнення витрат на реалізацію заходів у сфері створення безпечного середовища, забезпечення збалансованої міграційної політики і т.д., будуть кошти державного бюджету, а також міжнародна технічна допомога та інші джерела, не заборонені законодавством. В такому випадку необхідно приділити більше уваги в ході реалізації Стратегії підходам, які мають на меті залучення суспільства до процесу створення безпечного середовища, збільшення нетерпимості до корупції і розвиток демократичного цивільного контролю. Це повинно сприятливо позначитися на фінансуванні реалізації вищевказаних заходів, а також забезпечить їх підтримку з боку суспільства, що, в свою чергу, спричинить зміцнення довіри до органів системи МВС в цілому.

В українському законодавстві у Кримінальному кодексі України (далі – ККУ), у розділі XVI «злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку» кіберзлочинами визнано такі діяння [28]:

1) несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361);

2) створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 3611);

3) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах),

автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 3612);

4) несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362);

5) порушення правил експлуатації електроннообчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363);

6) перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 3631) злочин, визначений статтею 361 ККУ, це «класичне» зламування комп’ютерної системи, тобто самочинне, без належного дозволу проникнення у комп’ютерні системи чи мережі з протиправним умислом, що спричинило певні негативні наслідки (витік, втрату, підробку, блокування інформації тощо). Зазвичай злом супроводжує інше суспільно небезпечне діяння, таке як, наприклад, крадіжкав, тобто є допоміжним засобом у вчиненні багатьох інших злочинів.

Стаття 3611 ККУ передбачає дії, що полягають у створенні, розповсюдженні чи збуті шкідливого програмного забезпечення (далі – ПЗ) – певної програми або сукупності програм, що перешкоджає функціонуванню комп’ютера, пошкоджує дані на ньому або призводить до інших небажаних наслідків в комп'ютерній системі [28].

Шкідливе ПЗ може мати різноманітну форму (віруси (програми, здатні до самокопіювання з одночасним завдаванням шкоди комп’ютеру), троянська програма (шкідлива програма, що видає себе за безпечну, яка заважає роботі, шпигує за ним, використовує ресурси комп'ютера для якої-небудь незаконної діяльності і т. д.,) тощо), і може застосовуватись як допоміжний засіб у зламі та інших кіберзлочинах. відповідно до статті 3612 ККУ, злочином є несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в комп’ютерах або інших носіях

інформації. при цьому не обов’язково, щоб збут і розповсюдження такої інформації стали наслідком вчинення злочинів, зазначених вище. «комп’ютерна» інформація з обмеженим доступом поділяється на конфіденційну і таємну [28].

Конфіденційна інформація містить відомості, які перебувають у володінні, користуванні або розпорядженні окремих осіб, поширюється за їх бажанням згідно з передбаченими ними умовами. до таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі. згідно зі статтею 362 ККУ кіберзлочином є несанкціоновані зміна, знищення або блокування комп’ютерної інформації. Також карається за цією статтею несанкціоновані перехоплення або копіювання комп’ютерної інформації, якщо це призвело до її витоку. при чому, суб’єктом цього злочину є тільки особи, що мають право доступу до такої інформації [28].

Статтею 363 ККУ передбачено такі злочинні діяння, як порушення правил експлуатації комп’ютерів (що може виражатися у невиконанні або неналежному виконанні обов’язків із виконання правил експлуатації комп’ютерів (наприклад, правил апаратного забезпечення або правил експлуатації їх програмного забезпечення)) і порушення порядку чи правил захисту інформації (невиконання або неналежне виконання встановлених нормативно-правовими актами вимог (організаційних чи технічних) захисту інформації), якщо це заподіяло значну шкоду, вчинені особами, які відповідають за таку експлуатацію чи захист.

У ст. 3631 ККУ передбачено відповідальність за умисне масове розповсюдження повідомлень, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи комп’ютеру. повідомлення, про які йде мова – це так званий «спам», тобто масове розповсюдження попередньо не обумовлених електронних листів. через масовий характер спамових повідомлень останні утруднюють роботу інформаційних систем і ресурсів, створюючи для них зайве перевантаження, що може бути причиною їх виходу з ладу. «Спам» також може стати носієм згаданих раніше шкідливих програм і вірусів [8].

Інформаційні злочини, відповідно до українського законодавства, можуть мати різноманітну форму та способи вчинення. крім того, можна сказати, що вчинювані кіберзлочинцями дії можуть мати комплексний характер, тобто становити сукупність кіберзлочинів, що супроводжують і забезпечують один одного.

Суспільну небезпечність кіберзлочинів та актуальність цієї проблеми ілюструє таке явище, як кібератака. Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій та спрямовані на досягнення таких цілей:

- порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів;
- порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем;
- використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [9].

Кібератаки, в силу своєї специфіки, дуже часто спрямовані на автоматизовані та інформаційні системи, що мають державне значення. прикладом цього можуть слугувати відомі кібератаки на енергетичні компанії України 23 грудня 2015 року, коли зловмисникам вдалось успішно атакувати комп'ютерні системи управління трьох енергопостачальних компаній України, або кібератака 17-18 грудня 2016 року, коли була виведена з ладу підстанція «Північна» енергокомпанії «Укренерго», що мало наслідком залишення без струму споживачів певних районів Києва [33, с. 25].

З огляду на все вище сказане, можна зробити висновок, що кіберзлочини дійсно мають високу ступінь суспільної небезпечності, тому що дії, які складають такі злочини, є досить складними для реалізації, оскільки потребують спеціальних знань в сфері комп’ютерних технологій. Це означає, що і використання існуючих способів захисту від них також потребує певного рівня обізнаності в даній сфері. Отже, одна з проблемних сторін явища кіберзлочинності полягає у низькому рівні ІТ-освіченості населення різних країн, зокрема, України. Складність полягає в тому, що комп’ютерні

технології є досить складними в освоєнні, тому дуже важливо для пересічного громадянина знати хоча б найпростіші способи захисту, що не потребують глибоких специфічних знань.

Повертаючись до державного регулювання емерджентних технологій у контексті реалізації функції держави слід визначити низку основних ключових моментів. По-перше, мова повинна йти про забезпечення реалізації основної функції держави – загальної безпеки суспільства, особливо це стосується правових норм, що забороняють певні дії насамперед стосовно заздалегідь деструктивних технологій.

Основна проблема полягає у неочевидній деструктивності і можливих помилок в оцінці суті технологій. Так на сьогодні, досить неоднозначна ситуація із правовими обмеженнями у сфері використання технологій генної модифікації. Широка кампанія проти генномодифікованих організмів спирається на не до кінця встановлені факти, а уявно випереджувальна функція правових норм заборони може лише загальмувати технологічний прогрес в окремих державах. По-друге, регулювання державою відносин стосовно використання емерджентних технологій має обмежуватися реалізацією економічної функції держави, яка полягає у забезпеченні економічної багатоманітності як це визначено у ст. 15 Конституції України [27].

Мова повинна йти про заохочення вільного ринку і державний вплив на недопущення зловживання монопольним станом та обмеження економічної конкуренції. По-третє, надання різноманітних пріоритетів та преференцій повинно бути обґрунтованим і випливати із реально існуючої необхідності. На жаль у чинному вітчизняному законодавстві норми стосовно розвитку інноваційної діяльності, а також відповідні заохочення багато у чому мають суто декларативний характер.

Зазначене дозволяє прийти до наступних загальних висновків стосовно загального впливу комп’ютерних технологій на кіберзагрози. По-перше, серед інформаційно-компютерних технологій можливо виділити певну їх частину під умовною назвою «емерджентні технології», які проявляються у багатьох галузях науки і техніки. Під «емерджентною технологією» у контексті розгляду питань правового регулювання відповідних суспільних відносин пропонується розуміти таку технологію, що є радикально новою, швидкозростаючою, узгодженою з існуючими

технологіями, яка при цьому здійснює значний вплив на суспільне життя у різноманітних сферах, які неможливо передбачити наперед.

Досить значна кількість технологій, що застосовуються в інформаційній сфері зумовлює виникнення і розвиток таких «емерджентних технологій» та їх стрибкоподібний і глобальний вплив. По-друге, найбільш яскраво зазначені вище фактори проявляються у таких прикладах як: технології Інтернету речей, технології розподіленої обробки (грід-технології, «хмарні технології», DL-технології), технології криптографії. Для емерджентних технологій, що застосовуються в інформаційній сфері і діють у кіберпросторі характерні тісний взаємозв'язок та взаємний вплив. По-третє, загрози, що існують у кіберпросторі за весь час його існування модифікуються та інтенсифікуються за умови використання емерджентних технологій, при цьому такі технології мають потенціал їх збільшення. По-четверте, у питанні правового регулювання як реалізації функцій держави, зокрема щодо забезпечення кібербезпеки та протидії кіберзагрозам слід виходити насамперед з загальної безпеки суспільства, особливо це стосується правових норм, що забороняють певні дії – зокрема, стосовно заздалегідь деструктивних (руйнівних) технологій [36, с. 54].

3.3. Ефективна модель попередження кібрезлочинності: практичні рекомендації

Для України входження в новий етап суспільного розвитку означає безальтернативну ситуацію, за якої лише вдосконалення організації використання інформаційної основи розвитку української нації і держави – об'єднаної системи вітчизняних інформаційних баз, а також розвитку інформаційного виробництва та систем соціальних інформаційних комунікацій, що в сукупності складають ресурсну базу вітчизняного інформаційного простору, – може забезпечити належні позиції у міжнародному співробітництві.

Запорукою цього розвитку є організація безпеки національного інформаційного суверенітету для України і як для об'єкта глобальних інформаційних

впливів, і як для повноправного суб'єкта міжнародної діяльності, міжнародних інформаційних обмінів має надзвичайно велике значення. Гарантом існування і розвитку національних інформаційних ресурсів в умовах глобальних впливів є ефективна інформаційна безпека нашого суспільства [36, с. 112].

Процеси глобалізації, каталізатором яких в останні десятиріччя стала інформатизація на основі електронних технологій, крім свого позитивного значення для розвитку прогресу зумовлюють появу нових викликів і загроз для інформаційної інфраструктури, для національного інформаційного суверенітету, самобутності, самосвідомості, а для цивілізації – багатоваріантних можливостей подальшого розвитку. І тому робота з нейтралізації кіберзагроз як важливої складової забезпечення інформаційної безпеки є запорукою ефективного використання і перспективного розвитку суверенних для кожної держави, нації масивів інформації.

Розвиток ефективних інструментів забезпечення інформаційного суверенітету є важливою умовою суспільного розвитку і першочерговим завданням сьогодення. Питання забезпечення кібернетичної безпеки є надзвичайно важливими для української держави на сучасному етапі, що, насамперед, обумовлено необхідністю протистояти протиправним посяганням на інформаційний простір України, збереження інформаційних ресурсів, захисту населення від негативного інформаційного впливу тощо.

Окрім цього, стратегічно визнаним пріоритетом зовнішньої політики України є європейська інтеграція, що вимагає удосконалення нормативно-правової бази забезпечення кібернетичної безпеки України, яке б відповідало не лише міжнародним стандартам, а передусім українським національним інтересам в інформаційній сфері [42].

Поразка в інформаційній, в тому числі кібернетичній, війні може неминуче призвести до розпаду будь-якої держави. У сучасних умовах багато важливих систем промислового і оборонного сектора економіки, наприклад система управління повітряним сполученням, підприємствами енергетичної й атомної галузі та електромережі, що працюють на основі інформаційнокомунікаційних технологій, становлять потенційні об'єкти ризику через уразливості їх для вторгнення ззовні.

Таким чином, до зовнішніх загроз кібернетичному просторі відносяться і власне хакерські атаки, що здійснюються з територій інших держав, які мають на меті порушення роботи комп'ютерних систем, розкрадання інформації конфіденційного характеру та ін. [79, с.12].

Боротьба з кіберзлочинністю повинна носити системний характер, виходячи із сучасних ризиків та викликів у кіберпросторі, а інституційне середовище забезпечення кібербезпеки постійно вдосконалюватися. Ефективність заходів у цій сфері повинно досягатися завдяки здійсненню оцінки загроз організованої кіберзлочинності, що дозволить визначати сучасні загрози та ризики у кіберпросторі. У сучасному глобалізованому світі Україна потребує створення адекватної системи кібернетичної безпеки.

Активність з боку провідних держав світу у кіберпросторі, глибинні зміни відношення до внутрішньої інформаційної політики та формування потужних транснаціональних злочинних груп, що спеціалізуються на кіберзлочинах обумовлюють необхідність виробленні пріоритетів трансформації вітчизняного кібербезпекового сектору з урахуванням вищезазначених тенденцій.

Варто зазначити, що у швидкоплинному перебігу подій суспільного життя, з революційними процесами у розвитку інформаційних технологій значна частина чинних нормативних актів як внутрішньодержавних, так і міжнародних поступово втрачає актуальність, відповідність процесам, які ними нормуються, і потребує уточнень або ж перегляду. Розвиток інформаційної діяльності створює необхідність правового урегулювання нових аспектів цієї діяльності.

Потребує досконалого правового обґрунтування питання організації ефективного протистояння кібертероризму в умовах активізації глобальних впливів, нових інформаційних технологій. Комплекс відповідних правових актів має постійно вдосконалюватися із урахуванням відповідного міжнародного законодавства, його еволюції і вітчизняної законотворчої практики, що має бути на варті інтересів національної інформаційної діяльності.

У питанні правового регулювання як реалізації функцій держави, зокрема щодо забезпечення кібербезпеки та протидії кіберзагрозам слід виходити насамперед з

загальної безпеки суспільства, особливо це стосується правових норм, що забороняють певні дії – зокрема, стосовно заздалегідь деструктивних (руйнівних) технологій. Основна проблема полягає у неочевидності деструктивності і можливих помилок в оцінці суті технологій, тому пошук можливих шляхів вирішення зазначеної низки проблем є перспективним для подальших досліджень у галузі правової науки [84, с.312].

Окрім цього, регулювання державою відносин стосовно використання емерджентних технологій має обмежуватися реалізацією економічної функції держави, яка полягає у забезпеченні економічної багатоманітності як це визначено у ст. 15 Конституції України. Мова повинна йти про заохочення вільного ринку і державний вплив на недопущення зловживання монопольним станом та обмеження економічної конкуренції. Водночас, надання різноманітних пріоритетів та преференцій повинно бути обґрунтованим і випливати із реально існуючої необхідності.

Так як інформаційні технології, що існують на даний момент, дозволяють як приховувати розташування, так і використовувати дані інших, то , слід виробити наступні кроки.

На національному рівні:

- виступати і брати участь в розробці міжнародної стратегії з протидії кіберзагрозам і створенні єдиних міжнародно-правових механізмів регулювання віртуального простору;

1) спільною метою і напрямом Стратегії кібербезпеки забезпечити віртуальну безпеку особистості, організації і держави шляхом визначення системи пріоритетів, принципів і заходів в області внутрішньої і зовнішньої політики, в якій повинні бути відображені: всі складові кіберпростору, при яких забезпечується захист від максимально можливого числа загроз і впливів з небажаними наслідками;

2) конкретними / приватними напрямками стратегії необхідно визначати стандарти співпраці суб'єктів інформаційного суспільства - особистості, організацій і держави – в області забезпечення кібербезпеки; це норми дотримання балансу між встановленням відповідальності за недотримання вимог КБ, з одного боку, і

введенням надлишкових обмежень - з іншого; пріоритетність ризиків КБ відповідно до можливостей реалізації кіберзагроз та розмірів негативних наслідків від інцидентів КБ; актуалізація засобів і методів забезпечення кібербезпеки з метою протистояння постійно змінюваним кіберзагрозам [85, с.244].

– виробити і впровадити багаторівневу інституційну систему кібербезпеки, яка б включала:

1) науково-аналітичний рівень, який би вивчав ризики кібербезпеки відповідно до можливостей реалізації кіберзагроз і розмірами негативних наслідків; актуалізував засоби і методи забезпечення кібербезпеки. Це одна з найважливіших завдань.

Так як проблема полягає в складності класифікації загроз, що виходять з території держави і безпосередньо від неї. Внаслідок даної тенденції необхідно наголосити на необхідності для будь-якої держави виробити вжиття заходів стосовно ідентифікації кіберзагроз, а також їх своєчасного виявлення, запобігання, захисту, а також мінімалізації наслідків;

2) виконавчий рівень, який би здійснював координацію за двома напрямками – внутрішньому (між національними структурами, відповідальними за виявлення і протиборство кіберзагрозам) і зовнішньому, коли координація здійснюється між національними структурами і схожими іноземними регіональними / міжнародними установами;

– нарощувати потужності в інформаційній сфері з протиборства електронних атак.

Необхідно посилити заходи внутрішньополітичного характеру щодо стимулювання розвитку технологічної складової кібербезпеки для збереження балансу сил і складання противаги іншим імовірнісним «супротивникам» в області кібербезпеки;

– виступати, впроваджувати та реалізовувати регіональне, міжнародне співробітництво в сфері кібербезпеки, відстеження діяльності злочинних, терористичних груп і окремих хакерів, які діють в кіберпросторі;

- виступати і брати активну участь у розвитку міжнародного співробітництва в області та структурах, спрямованих на виявлення кіберзагроз, своєчасно виявляти, запобігати, захищати, а також мінімізувати наслідки.

На міжнародному рівні:

- виробити і впровадити міжнародну угоду в сфері запобігання та розслідування кіберагресії, а також оновити вже існуючі нормативно-правові акти;
- створити міжнародний орган з регіональними представництвами. Цей орган повинен бути еквівалентом ООН в кіберпросторі - КіберООН (далі - КООН), в ньому повинні бути кілька структур, наприклад: науково-аналітичний рівень, виконуючий функції, які повинні бути ті ж, що і на національному рівні

Виконавчий рівень може бути на міжнародному, регіональному та на національному рівні. Регіональний рівень дозволить, в разі кіберагресії, вчасно включитися в протидію, національний рівень дозволить нарівні з місцевими національними представниками включати в розслідування регіональних і міжнародних представників КООН. Також потрібно, щоб діяльність КООН повинна бути здійснена 12 адміністраторами, що обираються щорічно з членів КООН, на відміну від ООН тут не повинно бути привілейованих членів, з правом на вето або постійних. У разі кіберагресії КООН створить комісію для розслідування з міжнародних, регіональних, національних представників. Висновки комісії з відповідними доказами будуть направлятися в міжнародний суд. Винні покарання у вигляді санкцій і штрафів, щоб відшкодувати збитки.

Висновки до Розділу 3

Кібербезпека все частіше розглядається, як стратегічна проблема державного рівня, яка охоплює всі верстви суспільства. Не виключенням є і нинішній етап розвитку України, як і багатьох держав світу, який характеризується максимальною інформатизацією всіх сфер її життєдіяльності. В той же час перенесення багатьох процесів, зокрема й тих, що стосуються критичної інфраструктури, у т.з. кіберпростір,

несе в собі разом з позитивними, також й негативні наслідки: уразливість цих процесів перед численними кіберзагрозами.

Забезпечення безпеки у кіберпросторі є на сьогодні актуальним для нашої держави з огляду на те, що проти неї ведеться гібридна війна, одним з проявів якої є кібератаки на українські державні органи та установи, а також об’єкти критичної інфраструктури. З огляду на це, державі слід приділяти питанню кібербезпеки максимальну увагу.

Не дивлячись на те, що розвиток технологій в сучасному світі не тільки дозволяє людству вирішувати безліч проблем його прогресивної еволюції, але одночасно з цим породжує нові виклики і загрози в області віртуального кібернетичного простору, яке в більшості випадків дослідники називають інформаційним і якими в більшості випадків віддається перевага терміну «інформаційна безпека». Про такі підходи зазначалося у попередньому розділі. Однак відмінності між кібернетичної безпекою і інформаційною безпекою, на думку авторів, цілком очевидні.

ВИСНОВКИ

На основі проведеного дослідження зроблені наступні висновки:

Визначено, що інформаційна політика – це сукупність напрямів і способів діяльності компетентних органів держави з контролю, регулювання та планування процесів у сфері одержання, зберігання, оброблення, використання та поширення інформації. Виділено три основні напрямки інформаційної політики: урядове створення і поширення інформації, розробка, регулювання і використання інформаційної інфраструктури, інституційна та юридична інфраструктура.

Встановлено, що кіберзлочинність – це наслідок глобалізації інформаційно-комунікаційних технологій і появи міжнародних комп'ютерних мереж. На відміну від інших видів економічної злочинності, кіберзлочинність в даний час є найбільш швидкозростаючим сегментом, що пов'язано зі збільшенням чисельності користувачів комп'ютерів, підключених до глобальної мережі Інтернет, постійним підвищенням рівня професіоналізму кіберзлочинців, стійким розвитком і вдосконаленням інформаційних технологій. Будь-які інформаційні і технічні новації значно розширюють сферу кіберзлочинності і створюють умови для підвищення ефективності хакерських атак. Тому кіберзлочинність зростає більш швидкими темпами, ніж всі інші види злочинності і є одним з головних викликів по відношенню до інформаційної політики як України, так і інших держав світу.

За останні роки злочинність в інформаційному середовищі помітно посилила активність. Почастішали випадки скоєння кіберзлочинів за політичними мотивами і переконаннями, крім звичних економічних мотивів. На сьогоднішній день, багато нових акторів активно виходять на світову арену, беручи на себе передові технології, в тому числі і кіберзлочинність. Помітно так само стала кількість випадків, коли вчинення кіберзлочинів з політичних міркувань проводилося не окремо взятими правопорушниками, а в складі організованих груп, причому цілями ставали як ЗМІ, так і окремі діячі політики, зокрема президенти країн, громадські організації, військові і судові відомства різних країн

Виявлено, що розвиток вітчизняного законодавства у сфері забезпечення кібербезпеки відбувався поступово із врахуванням документів міжнародно-правового характеру у розрізі резолюцій Генеральної асамблеї ООН щодо культури кібербезпеки у сучасних умовах. Стан та ступінь загроз у кіберпросторі зумовили реагування держави у документах стратегічного характеру у сфері національної безпеки і оборони України. Агресія проти України у 2014 році, що відбувалась з активним використанням бойових дій проти нашої держави у кіберпросторі, а також посилення загальносвітових загроз кібербезпеці, зумовили формування відповідного законодавства, а також перегляду вже існуючих актів.

Найбільш активно зазначений процес відбувався останні два роки. 8 травня 2018 року набув чинності Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року. Цей Закон є комплексним спеціальним законодавчим актом у сфері забезпечення кібербезпеки. Попри деякі неоднозначні формулювання у тексті законодавчого акту і можливі питання з його практичним застосуванням, слід зазначити, що період формування національного законодавства у сфері кібербезпеки розпочатий, а основний акт спеціального законодавства, що започатковує відповідну систему законодавства, ухвалений.

У подальшому має бути сформований відповідний масив нормативно-правових актів, що складатимуть безпосереднє законодавство у сфері забезпечення кібербезпеки. Одночасно повинен відбуватись процес узгодження положень нового законодавства кібербезпеки з нормами права, насамперед, у галузі кримінального, адміністративного, цивільного права

Форми реалізації державної інформаційної політики різноманітні, вдосконалення їх повинно проходити постійно, комплексно, з урахуванням розвитку інформаційних технологій та специфіки різних галузей народного господарства і людської життєдіяльності. Такий підхід може гарантувати системну, своєчасну і ефективну реалізацію державної інформаційної політики, забезпечити соціальну спрямованість інформаційної політики, перетворити її з модного доважку в системі державного і муніципального управління в реально діючий механізм підвищення ефективності управління в різних галузях

Необхідно підвищити освіченість громадян України у сфері кібербезпеки. Це можна зробити на рівні державної пропаганди через ЗМІ, інформуючи населення про загальний стан справ в сфері кібербезпеки держави, стимулюючи населення до самоосвіти. Але перш за все, потрібно здійснити якісні зміни у системі освіти щодо цього питання, оскільки всім відомо, що у непрофільних навчальних закладах, таких як загальноосвітні школи, такі предмети, як інформатика (яка і дає базові знання учням у сфері інформаційних технологій, зокрема, щодо кібербезпеки) має низький рівень якості викладання.

З урахуванням всієї складності і небезпеки кіберзлочинів необхідне вироблення спільних дій вчених-юристів, перш за все законодавців та фахівців в області комп'ютерних інформаційних технологій, спрямованих на боротьбу зі злочинами в глобальних інформаційних мережах. Оскільки впровадження нормативних актів як національного, так і міжнародного характеру – недостатній крок на шляху вирішення проблеми боротьби з кіберзлочинністю, в даному випадку необхідні спеціальні знання в області інформаційних технологій і програмного забезпечення. Наслідком спільної роботи має бути створення єдиного глобального акту, що регламентує порядок протидії кіберзлочинів, не вироблено, проте міжнародне співтовариство в рамках регіонального співробітництва вживає заходів щодо законодавчого регулювання дій суб'єктів в кіберпросторі, по боротьбі з кіберзлочинами, а також створення принципово нового органу, який повинен займатися кіберзлочинами на міжнародному рівні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження): моногр. К.: Атіка, 2007. 304 с.
2. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти: монографія; за загальною редакцією д-ра юрид. наук, проф. Бандурки О. М.. Харків: Вид-во Ун-ту внутр. Справ, 2015. 368 с.
3. Бєляков К. І. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення: моногр. К.: КВІЦ, 2014. 576 с.
4. Бельський Ю. Щодо визначення поняття кіберзлочину // Юридичний вісник. 2014. № 6. С. 414–418.
5. Бутузов В. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): моногр. / В. Бутузов. – К.: КИТ, 2010. – 148 с.
6. Березовська І. Р. Державна інформаційна політика України та основні напрями її вдосконаленн// Міжнародні відносини. Серія «Економічні науки». 2019. № 4. С.10-18.
7. Бурячок В. Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства// Сучас. спец. техніка. 2011. № 3 (26). С. 104–114.
8. Богуцький П. Нелінійна раціональність системи права// Право України. 2018. № 6. С. 182-195.
9. Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека: Термінологічний навчальний довідник. Київ: ООО «Д.В.К.», 2014. 508 с.
10. Горбань О. Ю. Інформаційна війна проти України та засоби її ведення// Вісн. НАДУ. 2015. №1. 136–141.
11. Галлін Д. С., Манчіні П. Сучасні медіа-системи: три моделі відносин ЗМІ та політики / Пер. з англ. О.Насика. К.: Наука, 2008. 320 с.
12. Гаман Т. В. Проблемні питання нормативноправового забезпечення інформаційної діяльності органів державного управління (регіональний аспект) // Університетські наукові записки. 2015. № 1–2 (13–14). С. 272–276.

13. Гібридна війна: Російська Федерація проти країн Балтії: огляд. вид. упоряд.: С.Л. Фальченко, В.М. Гребенюк. Київ : Нац. акад.. СБУ, 2018. 164 с.
14. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. К.: НІСД, 2014. С. 36.
15. Доктрина інформаційної безпеки України: Затверджена Указом Президента України від 25 лютого 2017 року № 47/2017. [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/laws/show/47/2017?lang=ru.
16. Дзялошинский И. М. Коммуникационные матрицы прикладной политической коммуникативистики [Електронний ресурс] – Режим доступу: http://www.hse.ru/data/ 2012/12/04/1301970655/коммуникационные%20матрицы.pdf.
17. Драч І. Інформаційна політика України: Доп. на міжнар. конгресі у Києві "Інформаційне суспільство в Україні – стан, проблеми, перспективи"// Укр. проблеми. 2011. № 20. С. 103-107.
18. Дубов Д. В. Стратегічні аспекти кібербезпеки України // Стратегічні пріоритети : [наук.-аналіт. щокварт. зб.] / Нац. ін-т стратег. дослідж. К. : НІСД, 2013. № 4 (29). С. 119–126.
19. Довгань О. Д. Система інформаційної безпеки України: онтологічні виміри// Інформація і право. 2018. № 1 (24). С. 89-103.
20. Европейская Конвенция по киберпреступлениям (преступлениям в киберпространстве) Будапешт, 23 ноября 2001 г. [Електронний ресурс] – Режим доступу: http://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/rms/0900001680081580.
21. Злочини, пов'язані з використанням комп'ютерної мережі. Десятий конгрес ООН з попередження злочинності та поводження з правопорушниками //A/CONF.187/10. [Електронний ресурс] – Режим доступу: http://www.un.org/russian/topics/crime/docs10.htm.
22. Інформаційна складова державної політики та управління : монографія / С. Г. Соловйов, О.Є. Бухтатий, Ю.В. Нестеряк [та ін.] ; за заг. ред. Н. В. Грицяк; Нац. акад. держ. упр. при Президентові України. К.: К.І.С., 2015. 319 с.

23. Інформаційне право: підручник В. Я. Настюк (кер. авт.кол.), Л. П. Коваленко та ін.; за заг. ред. В. Я. Настюка, Л. П. Коваленко Харків: Право, 2016. 280 с.

24. Іванченко Ю. М. Сутність, головні напрями та способи державної інформаційної політики в Україні// Державне управління: теорія та практика. 2005. № 2. С.15-18.

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

26. Інформаційне суспільство: аналіз політичних аспектів зарубіжних концепцій: монографія / Картунов О. В., Маруховський О. О. ; за заг. ред. Картунова Олексія Васильовича; Ун-т економіки та права "КРОК". К. : Ун-т економіки та права "КРОК", 2012. 343 с.

27. Конституція України: Прийнята на п'ятій сесії Верховної Ради України 28 черв. 1996 р. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

28. Кримінальний кодекс України від 28.11.2019, підстава - 263-IX, 284-IX. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/main/2341-14.

29. Конвенція про кіберзлочинність [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/main .

30. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Науководослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І.Вернадського. – К.: Видавничий дім «АртЕк», 2018. №1-12.

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

32. Красноступ Г. М. Основні напрями правового забезпечення державної інформаційної політик// Офіційний веб-сайт Міністерства юстиції України [Електронний ресурс] – Режим доступу: http://old.minjust.gov.ua/30768.

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

34. Комп'ютерна злочинність і інформаційна безпека. А.П.Леонов; під заг. ред. А. П.Леонова. Мінськ: АРІЛ, 2000. 552 с.

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

36. Ліпкан В. А. Національна безпека України: навчальний посібник. 2-ге вид. К. : КНТ, 2009. 576 с.

37. Литвиненко О. Інформаційні технології та Україна у світовому контексті // Людина і політика. 2001. № 1. С.10-17.

38. Лужецький В. А. Інформаційна безпека: навч. посіб. Вінниця: УНІВЕРСУМ-Вінниця, 2009. 240 с.

39. Мельник М. Сутність поняття «державна політика розвитку інформаційного суспільства»: узагальнення європейських та вітчизняних трактувань// Науковий вісник «Демократичне врядування». 2012. Вип. 9. [Електронний ресурс] – Режим доступу: http://www.lvivacademy.com/vidavnitstvo_1/visnik9/fail/Melnyk.pdf.

40. Москаленко А., Губерський Л., Іванов В. Основи масово-інформаційної діяльності. К., 2014. 71 с.

41. Моисеев Н. Информационное общество как этап новейшей истории// Свободная мысль. 2016. № 1. С. 81-83.

42. Нікулеско Д. Кібербезпека: вразливі моменти// Юридична газета. 14 травня 2019. [Електронний ресурс] – Режим доступу: http://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html.

43. Нестеряк Ю. В. Нормативно-правові основи державної інформаційної політики України в умовах розвитку інформаційного суспільства// Теорія та практика державного управління. 2016. Вип. 4 (39). С. 111–119

44. Окінавська хартія глобального інформаційного суспільства. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/998_163.

45. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій: наук.-практ. посіб. / [В.М. Болгов, Н.М. Гадіон, О.З. Гладун та ін.]. К.: Національна академія прокуратури України, 2015. 202 с.

46. Про інформацію: Закон України від 21.01.192.[Електронний ресурс] – Ре жим доступу: https://zakon.rada.gov.ua/laws/show/2657-12.

47. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7 вересня 2005 року № 2824-IV. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2824-15.

48. Про національну безпеку України: Закон України від 21.06.2018 № 964-IV. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19#n355

49. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19/conv

50. Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації: Закон України від от 23.09.1997 № 539/97-ВР.[Електронний ресурс] – Режим доступу:https://zakon.rada.gov.ua/laws/show/539/97-%D0%B2%D1%80

51. Про електронні довірчі послуги: Закон України від 05.10.2017 № 852-IV. [Електронний ресурс] – Режим доступу:https://zakon.rada.gov.ua/laws/show/2155-19

52. Про адміністративні послуги: Закон України від 06.09.2013 р. № 5203-VI .[Електронний ресурс] – Режим доступу:https://zakon.rada.gov.ua/laws/show/5203-17

53. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/851-15

54. Про авторське право і суміжні права: Закон України від 04.11.2018 №5142.[Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/3792-12

55. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 01.02.1993 №5412. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2782-12.

56. Про інформаційні агентства: Закон України від 01.06.1992 №7415 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/74/95-%D0%B2%D1%80.

57. Про Суспільне телебачення і радіомовлення України: Закон України від 17.04.2014 №1452. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/1227-18.

58. Про рекламу: Закон України від 03.07.1996 №5841. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80.

59. Про телебачення і радіомовлення: Закон України від 21 грудня 1993 року № 3759-XII. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/3759-12

60. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі: Указ Президента України від 31 лип. 2000 р. [Електронний ресурс] – Режим доступу:https://zakon.rada.gov.ua/laws/show/928/2000..

61. Про схвалення Концепції розвитку електронного урядування в Україні: Розпорядження Кабінету Міністрав України від 13 грудня 2010 р. № 2250-р. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/go/797-2017-%D1%80.

62. Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Закон України від 21 липня 2006 року № 23-V. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/23-16.

63. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України": Указ Президента України від 26 травня 2015 року № 287/2050. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/287/2015.

64. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Рішення РНБО від 28 квітня 2014 року. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/n0004525-14.

65. Погорецький М. Кіберзлочини: до визначення поняття// Вісник прокуратури. 2012. № 8. С. 89–96.

66. Пожуєв В. І. Формування державної інформаційної політики в умовах глобалізації// Гуманітарний вісник Запорізької державної інженерної академії. 2016. Вип. 43. С. 4–12.

67. Пахнін М. Л. Принципи, завдання та інструменти державної інформаційної політики України в сучасних умовах// Теорія та практика державного управління. 2014. Вип. 3(46). С.1–9.

68. Политология. Учебник Ю. В. Ирхин, В. Д. Зотов, Л. В. Зотова. М.: Юристъ, 2012. 511 с.

69. Проблеми української політики: аналітичні доповіді Інституту політичних і етноціональних досліджень ім. І.Ф.Кураса НАН України. К.: ІПіЕНД ім.І.Ф.Кураса НАН України, 2010. 410 с.

70. Почепцов Г. Г., Чукут С. А. Інформаційна політика: Навч. посібник. К.: Знання, 2016. 663 с.

71. Петров В. В. Щодо формування національної системи кібербезпеки України// Стратегічні пріоритети : [наук.-аналіт. щокварт. зб.] / Нац. ін-т стратег. дослідж. К. : НІСД, 2013. № 4 (29). С. 127–130.

72. Рівень проникнення Інтернету в світі за станом на вересень 2018 року з розбивкою по регіонах, Statista. [Електронний ресурс] – Режим доступу: https://www.statista.com/statistics/269329/penetration-rate-of-the-internetby-region/.

73. Роговець В. Інформаційні війни в сучасному світі: причини, механізми, наслідки // Персонал. 2015. № 5. С.10-17.

74. Рязанцева І. М. Проблемні питання розбудови національної системи кібербезпеки// Право і Безпека : наук. журн. 2014. № 2 (53). С. 140–144.

75. Резолюция принятая Генеральной Ассамблеей ООН // Двенадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию/ A/RES/65/230 1.04.2011. [Електронний ресурс] – Режим доступу: http://www.unodc.org/documents/justice-and-prison-reform/AGMs/A_RES_65_230r.pdf.

76. Радзієвський І. На шляху до інформаційного суспільства: державна інформаційна політика в умовах глобалізації.[Електронний ресурс] – Режим д оступу: http://www.guds.gov.ua/document/41970/2_2004_radziievs'kyi_red.doc.

77. Сологуб Р. Як захистити критичну інфраструктуру країни у кіберпросторі [Електронний ресурс] – Режим доступу:https://biz.nv.ua/ukr/experts/jakzakhistiti-najtsinnishu-informatsiju-u-kiberprostori-2510093.html.

78. Словник термінів з кібербезпеки. за заг. ред. О. Копатіна, Є. Скулишина.: АванпостПрим, 2012. 214 с.

79. Системний аналіз переходу від концепції національної інформаційної політики до доктрини інформаційної безпеки України. І. Горбенко, О. Потій, С. Черних, М. Прокофьєв// Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: науковотехнічний збірник. 2017. Вип. 5. С. 12-26.

80. Сучасні тренди кібербезпекової політики: висновки для України. Аналітична записка. [Електронний ресурс] – Режим доступу: http://www.niss.gov.ua/articles/294/.

81. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави : моногр. Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.

82. Токар О. Державна інформаційна політика: проблеми визначення концепту// Політичний менеджер. 2015. № 5. С.131–141.

83. Україна: інформація і свобода слова: Зб. законод. актів, нормат. док. та ст. фахівців Упоряд. А.М.Задворний. К.: Молодь, 2017. 832 с.

84. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення// Боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. № 1 (27). 312–320.

85. Ярема О. Г. Предмет правового забезпечення інформаційної безпеки в інформаційному праві// Науковий вісник Львівського державного університету внутрішніх справ. 2016. № 2. С. 244-252.

86. Department of Defense: Report on Strategic Communication. URL: http://www.au.af.mil/au/awc/awcgate/dod/dod_report_strategic_communication_11feb10.pdf.

87. Dimitriu G. R. Winning the story war: Strategic communication and the conflict in Afghanistan / G. R. Dimitriu // Public Relations Review. Vol. 38. Issue 2. 2018. P. 195–207.

88. Data: Internet access. OECD. URL: https://data.oecd.org/ict/internet-access.htm.

89. Freedman L. The Transformation of Strategic Affairs. Lawrence Freedman. The Adelphi Papers. London: Routledge, 2016. Vol. 45; Iss. 379.

90. Djerf-Pierre Monika. Squaring the Circle: Public Service and Cmmercial News on Swedish Television, 2018. Journalism Studies 1(2). P. 239 – 260.

91. Europol. Internet Organised Crime Threat Assessment 2018. URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organisedcrime-threat-assessment-iocta-2018.
92. Europol. Public Awareness and Prevention Guides. URL: https://www.europol.europa.eu/activities-services/public-awareness-and-preventionguides/online-sex.
93. European Convention on Cybercrime. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.
94. European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI). URL: http://www.ulapland.fi/home/oiffi/enlist/resources/HeuniWeb.htm.
95. Nandini Ramprashad. The National Research Council of India / Computers in danger. NewDelhi, 2017. 251 p.
96. Kessel J. M. and Mozur P. How China Is Changing Your Internet. New York Times. 2016. URL: https://www.nytimes.com/video/technology/100000004574648/chinainternet-wechat.html.
97. Krocker, Rachel. An Internet Connection does not equal Internet access. ICT Works. 2014. URL: https://www.ictworks.org/an-internet-connection-does-not-equal-internetaccess/.
98. NATO Strategic Communication: More to be Done? / Steve Tatham, Rita Le Page; National Defence Academy of Latvia Center for Security and Strategic Research. Rīga, 2014. URL: http://www.academia.edu/6808986/NATO_Strategic_Communication_More_to_be_done.
99. Oxford English Dictionary [Electronic recourse]. URL: http://www.askoxford.com.
100. Piattoni Simona. Clientelism, Interests and Democratic Representation: The European Experience in Historical and Comparative Perspective. Cambridge: – Cambridge University Press, 2015. 256 p.

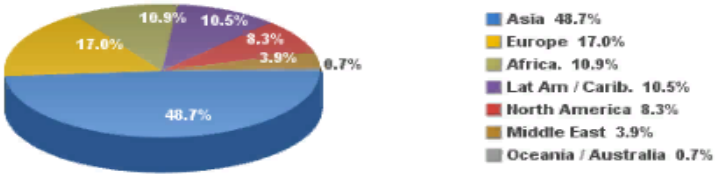
101. Sanders Karen, Canel Crespo María José and Holtz-Bacha Christina. Communicating Governments: A Three-Country Comparison of How Governments Communicate with Citizens // The International Journal of Press/Politics, 16(4). 2017. 547 p.
102. Tench Ralph, Yeomans Liz. Exploring Public Relations. Financial Times / Prentice Hall; 1 edition, 2016. 672 p.
103. Yar M. The Novelty of ‘Cyber crime’: An Assessment in Light of Routine Activity // Theory European Journal of Criminology. 2015. Volume 2 (4). P. 407–427.

ДОДАТКИ

ДОДАТОК А

Статистика використання Інтернет станом на 31 грудня 2017 року [72]

Internet Users in the World by Regions - December 31, 2017



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 4,156,932,140 Internet users in December 31, 2017
Copyright © 2018, Miniwatts Marketing Group

INTERNET USAGE STATISTICS
The Internet Big Picture
World Internet Users and 2018 Population Stats

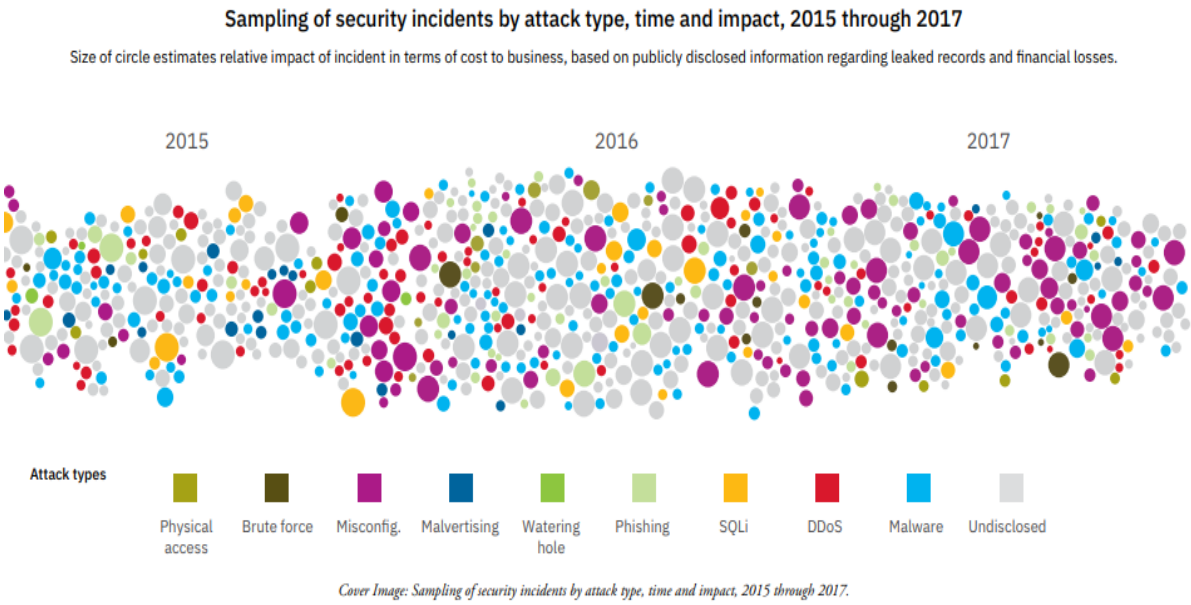
WORLD INTERNET USAGE AND POPULATION STATISTICS
DEC 31, 2017 - Update

World Regions	Population (2018 Est.)	Population % of World	Internet Users 31 Dec 2017	Penetration Rate (% Pop.)	Growth 2000-2018	Internet Users %
Africa	1,287,914,329	16.9 %	453,329,534	35.2 %	9,941 %	10.9 %
Asia	4,207,588,157	55.1 %	2,023,630,194	48.1 %	1,670 %	48.7 %
Europe	827,650,849	10.8 %	704,833,752	85.2 %	570 %	17.0 %
Latin America / Caribbean	652,047,996	8.5 %	437,001,277	67.0 %	2,318 %	10.5 %
Middle East	254,438,981	3.3 %	164,037,259	64.5 %	4,893 %	3.9 %
North America	363,844,662	4.8 %	345,660,847	95.0 %	219 %	8.3 %
Oceania / Australia	41,273,454	0.6 %	28,439,277	68.9 %	273 %	0.7 %
WORLD TOTAL	7,634,758,428	100.0 %	4,156,932,140	54.4 %	1,052 %	100.0 %

NOTES: (1) Internet Usage and World Population Statistics estimates in Dec 31, 2017. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the United Nations Population Division. (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, by local ICT Regulators and other reliable sources. (5) For definitions, navigation help and disclaimers, please refer to the Website Surfing Guide. (6) The information from this website may be cited, giving the due credit and placing a link back to www.internetworldstats.com. Copyright © 2018, Miniwatts Marketing Group. All rights reserved worldwide.

ДОДАТОК Б

Динаміка способів злочинів з 2015 по 2017 року, за даними IBM X-Force 2018 [72]



Cover Image: Sampling of security incidents by attack type, time and impact, 2015 through 2017.

ДОДАТОК В

Шкідливе ПЗ, яке принесло найбільші збитки за 2017 рік. IBM X-Force