Міністерство освіти і науки України
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Навчально-науковий інститут фінансів, економіки, управління та права
Кафедра фінансів, банківського бізнесу та оподаткування

Магістерська робота

на тему «Формування інформаційної безпеки України в умовах викликів та загроз»

Виконав: студент 6-го курсу, групи 601-УФБ
Спеціальності
072 «Фінанси, банківська справа та страхування»
за освітньо-професійною програмою «Фінанси, банківська справа та страхування»
другого (магістерського) рівня вищої освіти
Черевко Я.О.
Керівник: д.е.н., професор Варналій З.С.
Рецензент: директор Департаменту організації навчального процесу, акредитації та ліцензування О.С. Максименко

Засвідчую, що в цій роботі немає запозичень із праць інших авторів без відповідних посилань
Черевко Я.О.
Підтверджую достовірність даних, використаних у роботі
Черевко Я.О.

Полтава, 2022 року

АНОТАЦІЯ

Черевко Я.О. Формування інформаційної безпеки України в умовах викликів та загроз. Рукопис. Магістерська робота на здобуття другого (магістерського) рівня вищої освіти зі спеціальності 072 «Фінанси, банківська справа та страхування» за освітньо-професійною програмою «Управління фінансово-економічною безпекою», Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, 2022.

Робота містить 125 сторінок, 17 таблиць, 21 рисунків, список літератури складається із 106 найменувань.

Ключові слова: інформація, інформаційна безпека, виклики та загрози, державна політика, національна безпека країни.

Національна безпека в умовах зростаючих взаємозв'язків та взаємозалежності держав при збереженні та появі нових глобальних небезпек і загроз стає складовою загальної світової безпеки. Важливою складовою та сферою національної безпеки є інформаційна безпека. Із зростанням у сучасних умовах науково-технічного прогресу буде зростати значення інформаційної безпеки людини, суспільства, держави. Тому нині у зарубіжних країнах та в Україні питанням інформаційної політики та інформаційної безпеки приділяється особлива увага. Це обумовлює актуальність теми магістерської роботи.

Метою магістерської роботи є дослідження теоретичних та практичних аспектів формування інформаційної безпеки в умовах викликів та загроз.

Предметом дослідження є сукупність теоретичних та практичних аспектів формування інформаційної безпеки в умовах викликів та загроз та визначення стратегічних напрямів підвищення її рівня.

У теоретичній частині роботи розглянуто наукові підходи до визначення сутності поняття «інформаційна безпека». Виділено та охарактеризовано види ризики та загрози інформаційній безпеці держави.

Розглянуто методичні підходи до оцінювання стану та загроз безпеки інформаційних ресурсів. Охарактеризовано державну політику у напрямку забезпечення інформаційної безпеки в Україні та розглянуто світовий досвід.

У розрахунково-аналітичній частині роботи проведено оцінювання інформаційної безпеки держави. Визначено основні напрями державного регулювання сфери інформаційно-комунікаційної діяльності в системі економічної безпеки України.

Практична цінність магістерської роботи полягає в можливості використання запропонованих напрямів підвищення рівня інформаційної безпеки в Україні.

Інформаційною базою для написання даної роботи є законодавчі та нормативно-правові акти з питань забезпечення інформаційної безпеки в Україні; монографії; підручники та наукові статті з питань інформаційної безпеки держави; дані Державної служби статистики України.

SUMMARY

Cherevko Ya.O. Formation of Ukraine’s information security in the face of challenges and threats. Manuscript. Master's thesis for the second (master's) level of higher education in the specialty 072 "Finance, Banking and Insurance" under the educational and professional program "Management of Financial and Economic Security", National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, 2022.

The work contains 125 pages, 17 tables, 21 figures, the list of references consists of 106 titles.

Keywords: information, information security, challenges and threats, state policy, national security of the country.

National security in the context of growing interconnections and interdependence of states while maintaining and emerging new global dangers and threats is becoming part of global security. An important component and area of national security is information security. With the growth of scientific and technological progress in modern conditions, the importance of information security of man, society and the state will grow. Therefore, special attention is paid to the issues of information policy and information security in foreign countries and in Ukraine. This determines the relevance of the topic of the master's thesis.

The purpose of the master's work is to study the theoretical and practical aspects of the formation of information security in the face of challenges and threats.

The subject of research is a set of theoretical and practical aspects of the formation of information security in the face of challenges and threats and the definition of strategic directions for improving its level.

The theoretical part of the work considers scientific approaches to defining the essence of the concept of "information security". The types of risks and threats to the information security of the state are identified and characterized. Methodical

approaches to assessing the state and threats to the security of information resources are considered. The state policy in the direction of ensuring information security in Ukraine is described and the world experience is considered.

In the calculation and analytical part of the work, the information security of the state was assessed. The main directions of state regulation of the sphere of information and communication activity in the system of economic security of Ukraine are determined.

The practical value of the master's work lies in the possibility of using the proposed directions of improving the level of information security in Ukraine.

The information base for writing this work is the legislation and regulations on information security in Ukraine; monographs; textbooks and scientific articles on information security of the state; data of the State Statistics Service of Ukraine.

ЗМІСТ

ВСТУП

Національна безпека в умовах зростаючих взаємозв'язків та взаємозалежності держав при збереженні та появі нових глобальних небезпек і загроз стає складовою загальної світової безпеки. Важливою складовою та сферою національної безпеки є інформаційна безпека. Із зростанням у сучасних умовах науково-технічного прогресу буде зростати значення інформаційної безпеки людини, суспільства, держави. Тому дослідження питання інформації, яка стала чинником, який може призвести до значних технологічних аварій і катастроф, військових конфліктів та їх наслідків, дезорганізувати державне управління, фінансову систему, роботу наукових центрів, має актуальне значення.

Дослідження інформаційної безпеки України присвячені праці таких зарубіжних учених: Р. Андерсона, К. Веня, Л. Гордона, М. Гупти, Л. Кардгольма, Н. Кшетрі, Дж. Лі, М. Лоєба, Т. Мура, А. Сінгха, З. Сонні, Г. Стефанідеса, М. Столла, Т. Цякіса, Ю. Ши та ін. Це питання досліджували й вітчизняні вчені, зокрема, В. Бабенко, А. Бойко, Т. Васильєва, Г. Гайдур, І. Гонтарева, Р. Грищук, Т. Затонацька, А. Качинський, С. Лєонов, О. Кузьменко, В. Маргасова, С. Онищенко, Т. Полозова, О. Сороківська, В. Хаустова та ін. Останнім часом питання інформаційної політики та інформаційної безпеки набуло особливої актуальності.

Метою даної магістерської роботи є дослідження теоретичних та практичних аспектів формування інформаційної безпеки в умовах викликів та загроз.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

– визначити тенденції розвитку національної економіки у світлі формування цифрової економіки;

– дослідити наукові підходи до трактування «інформаційна безпека» та визначити її значення у системі національної безпеки держави;

– розглянути класифікацію викликів та загроз інформаційній безпеці;

– проаналізувати сучасні методи оцінювання стану та загроз безпеки інформаційних ресурсів;

– визначити індикатори та провести оцінювання рівня інформаційної безпеки України;

– дослідити військову агресія як найбільшу загрозу інформаційній безпеці України;

– обґрунтувати державну політику формування інформаційної безпеки в Україні в умовах викликів та загроз;

– дослідити взаємовідносини держави та інститутів громадського суспільства з питань забезпечення інформаційної безпеки України на сучасному етапі;

– проаналізувати світовий досвід забезпечення інформаційної безпеки держави;

– визначити напрями напрями формування інформаційної безпеки України з урахуванням сучасних викликів та загроз.

Об’єктом дослідження є процес формування інформаційної безпеки в Україні.

Предмет дослідження – сукупність теоретичних та практичних аспектів формування інформаційної безпеки в умовах викликів та загроз та визначення стратегічних напрямів підвищення її рівня.

Основними методами дослідження, використаними в даній роботі є: діалектичний метод пізнання, метод аналізу і синтезу, метод індукції та дедукції, порівняльний аналіз та інші.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

1.1. Тенденції розвитку національної економіки у світлі формування цифрової економіки

Базисом для розвитку суспільства є економіка, яка забезпечує всі сфери життєдіяльності людини, країни та світу. Вивченням проблем її формування, становлення та розвитку присвячено безліч наукових праць вітчизняних вчених та закордонних науковців. В контексті окремої держави основний акцент дослідження робиться на питаннях, пов'язаних із національною економікою, особливо її структурою, індикаторами виміру її стану, факторами впливу, етапами розвитку, тощо.

В останні роки відбувається поступовий розвиток економіки у напрямку подальшого зростання інформатизації, цифровізації та телекомунікації її сфер. Дані тенденції підтверджуються розрахунками, проведеними експертами ініціативи «Цифрова адженда України» [72, 67], які відображають прогнози показників цифровізації економіки України, хоча вони є занадто оптимістичними (табл. 1.1).

Таблиця 1.1

Прогнозні показники цифровізації економіки України

Показники	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Внутрішній ринок (споживання ІКТ), млрд дол.	2,0	2,5	3,0	4,5	6,0	8,0	10,0	12,0	14,0	16,0
Вплив на ВВП, % зростання	+0,5	+1,0	+2,0	+3,5	+4,5	+6,0	+7,5	+9,0	+11,0	+14,0
Частка цифрової економіки у загальному ВВП, %	3	5	8	11	15	20	28	40	52	65

У сучасних економічних умовах розвитку України відбувається збільшення рівня споживання інформаційно-комунікаційних технологій, що, своєю чергою, впливає на темпи їх модернізації в різних сферах економічної діяльності. Оскільки рівень фінансування в цій сфері низький порівняно з іншими сферами та іншими країнами, це відчувається в повільному зростанні ІТ-сектору в Україні. Експерти прогнозують, що 2030 року частка цифрової економіки в загальному ВВП зросте до 65%, що призведе до зростання на 14%. Це можливо лише завдяки припливу інвестицій закордонних компаній, зацікавлених у високо-технологічному виробництві, а також впровадженні сучасних технологій для забезпечення більш ефективного функціонування бізнес-процесів різних суб'єктів економіки.

В умовах бурхливого розвитку інформаційних технологій та глобалізаційних перетворень національна економіка та бізнес-середовище зазнає динамічних змін. Діджиталізація виступає каталізатором інноваційного розвитку, технологічні зміни призвели до появи таких можливостей, як гнучкість, реактивність та індивідуалізація продукції, однак разом із тим з'явилися й нові перешкоди, такі як швидкі технологічні перетворення, високий рівень складності, зміна переваг клієнтів та вимог законодавства.

Для розвинутих країн світу характерне проникнення діджиталізації в усі сфери життя суспільства. Масштабне поширення технологій зумовлює зменшення частки традиційної економіки поряд із діджиталізацією. Діджиталізація викликає структурні зміни в галузях, і її вплив є різноманітним, і виникає питання про вплив даного процесу на бізнес-моделі.

Діджиталізація сприяє розширенню інформаційного простору, створюючи нові інформаційні продукти, сприяє зниженню інформаційних витрат. Це істотно прискорює і спрощує пошук інформації, взаємообмін нею і сприяє посиленню співпраці між компаніями, що впливає на методи операційної діяльності суб'єктів господарювання, пошук людьми сприятливих умов для життєдіяльності, а також на якість взаємодії між населенням країни і її урядом. Зміни в господарських процесах, переорієнтація виробництва зі

створення матеріальних благ на надання послуг, глобалізація економіки відзначаються науковцями як найбільш фундаментальні ознаки розвитку нового типу суспільства в епоху становлення процесів інформатизації та діджиталізації.

Діджиталізація є необхідним процесом розвитку сучасних підприємств в умовах неоекономіки. Вона покликана спростити та прискорити роботу з великими базами даних, забезпечити автоматизацію усіх видів діяльності (основної та допоміжної операційної, інвестиційної, фінансових), покращення комунікації з клієнтами, постачальниками та партнерами та усіма інститутами зовнішнього середовища, формування нових засад взаємодії в межах підприємства – між підрозділами, працівниками, менеджментом, перехід до нових організаційних форм господарювання (мережева та віртуальна економіка).

Необхідність у діджиталізації обумовлюється прагненням до постійного підвищення рівня своєї конкурентоспроможності, що в свою чергу є передумовою виживання та розвитку бізнес-організацій в умовах неоекономіки.

Діджиталізація забезпечує підприємствам такі конкурентні переваги як: надання додаткової цінності товару через якісний сервіс; високий рівень зв’язку з клієнтами та цільовою аудиторією; підвищення іміджу компанії за допомогою швидкої комунікації з клієнтами; зниження ціни за допомогою автоматизації процесів та оцифровування бізнес процесів; прозорість внутрішніх та зовнішніх процесів підприємства; підвищення лояльності клієнтів до компанії.

Аналіз теоретичних концепцій дослідження розвитку цифрової економіки дозволяє виділити їхні основні переваги та недоліки. Їх сукупність представлена у таблиці 1.2.

Таблиця 1.2

Переваги та недоліки діджиталізації національній економіці

Переваги	Недоліки
- підвищення рівня конкурентоспроможності різних господарюючих суб'єктів; - спрощення роботи з інформацією; - економія фінансових ресурсів; - підвищення лояльності клієнтів; - зростання іміджу підприємств; - індивідуальний підхід до потреб клієнтів; - економія часу.	-необхідність залучення висококваліфікованих спеціалістів; - можливість втрати контролю через зовнішні втручання в роботу підприємств; - потреба у спеціальному обладнанні; - необхідність постійного вдосконалення функціонування відповідних систем.

Клаус Шваб переваги діджиталізації визначає наступним чином:

1. Безпрецедентне зростання інновацій – що стосується їх швидкості, об'єму та впливу. Це дасть значне покращення в ефективності, продуктивності та скороченні витрат.

2. Безпрецедентне зростання даних та можливостей їх використання для нових технологій вже дає краще залучення різних верств розробників – користувачів – клієнтів й сприятиме розвиткові в багатьох відношеннях.

3. Штучний інтелект стає реальністю – конкретні приклади ми вже бачимо від масової роботизації й до біотехнологій. В цілому, невблаганний перехід від простого оцифрування (третя промислова революція) до інновацій, заснований на комбінаціях технологій (четверта промислова революція), змушує компанії переглядати те, як вони ведуть бізнес. Керівники бізнесу і керівники вищої ланки повинні розуміти мінливе середовище, кидати виклик своїм операційним командам і невпинно, постійно впроваджувати інновації.

Удосконалення бізнес-процесів є інструментом управління, підвищення результативності та формування конкурентних переваг підприємства. Впровадження информаційно-комунікаційних технологій, Big Data, бізнес-аналітики, бізнес-планування, що передбачає автоматизацію бізнес-процесів, як слід, зростання продуктивності праці, економію поточних витрат, оперативну гнучкість бізнесу.

Застосування діджиталізації створює низку конкурентних переваг підприємства в розрізі операційних процесів, а саме підвищуючи їх рівень транспарентності та можливості, вчасно прийняти управлінське рішення, миттєвий обмін інформацією між компетентними співробітниками, здійснення маркетингових досліджень та створення системних підходів до реагування. Організаційні відповіді на сигнали ризикових змін за рахунок діджиталізації формуються на принципах узгодженості, вчасності, дієвості, запобіганні кризових становищ.

Проте, важлива роль діджиталізації як способу модернізації національної економіки не виключає її основні проблеми:

1. Недооцінка соціального та інших вимірів розвитку сучасної економіки, наприклад, неоднорідності розвитку українських регіонів. Швидше за все, цифровізація стане стратифікованою, а не однорідною.

2. Зниження продуктивності у сфері виробництва самих цифрових технологій і, в свою чергу, уповільнення інвестування в їх розвиток.

3. Зниження кваліфікації виробничого персоналу в умовах його перетворення у придаток оцифрованих виробництв, витіснення праці не тільки низької, а й середньої кваліфікації.

4. Зростання імовірності технологічних збоїв і техногенних катастроф, інформаційно-цифрових маніпуляцій і шахрайських операцій у невиробничій сфері.

5. Уповільнення зростання частки цифрової економіки у ВВП, що вже спостерігається в низці промислово розвинених країн.

6. Витіснення базових технологічних процесів, науково-технічних інновацій, а також економічних відносин, пов'язаних з соціальною орієнтацією економіки України.

7. Обмежені можливості урахування специфіки української економіки, співвідношення державного регулювання і ринку.

8. Загрози економічній безпеці країни, насамперед, її кібер- і військово-промисловій безпеці.

9. Вихід вітчизняних ІТ-компаній з-під державного контролю, оподаткування тощо.

10. Загострення соціальних суперечностей при масовому вивільненні працівників, зниження ступеня соціальної захищеності внаслідок розширення автономності учасників мережевої цифрової економіки, посилення соціальної нерівності, в т. ч. і внаслідок наявної цифрової нерівності, перетворення соціально-економічних суб'єктів у «гвинтики» технологічного прогресу.

Економічна трансформація бізнесу в поєднанні з технологічними змінами сприяє пришвидшенню процесів діджиталізації економіки. Основними зрушеннями, що відбуваються в сучасному світі та вливають на національну економіку є:

1) цифрова економіка досягла зрілості в розвинених країнах і знаходиться на етапі формування в країнах, що розвиваються;

2) виникає цифрова нерівність як між окремими індивідуумами, так і цілими державами;

3) усі галузі економіки зазнають цифрової трансформації;

4) споживач займає центральне місце в глобальній ринковій економіці;

5) прослідковується гіпершвидкість бізнес-операцій;

6) виникають нові моделі ведення бізнесу (віртуальні альянси, цифрові компанії);

7) пошук шляхів інноваційного розвитку набуває важливого значення на всіх рівнях господарювання;

8) оцінка цифрових ризиків та управління ними стають найважливішими чинниками для ефективного функціонування;

9) формується потреба у висококваліфікованих кадрах для управління цифровими технологіями;

10) значного поширення набувають гнучкі нетипові форми та способи зайнятості.

Цифрові інновації стимулюють розвиток цифрової економіки та суспільства, дають можливість застосування розробок у багатьох сферах і

призводять до трансформації економіки. У країнах з високим рівнем доходів на душу населення спостерігається тенденція до підвищення рівнів прибутковості секторів економіки, що забезпечують економію коштів унаслідок їх масштабної діджиталізації. Водночас у країнах з рівнем доходів вище середнього збільшення обсягів промислового виробництва, добробуту та зростання чисельності населення призводять до підвищення попиту на використання технологій.

У зв'язку зі зростанням впливу ІКТ на конкурентоспроможність бізнес-структур індикатори діджиталізації розраховуються також спеціалістами низки провідних міжнародних компаній. Наприклад, фахівці компанії «Huawei» розробили глобальний індекс мережевої взаємодії (Global Connectivity Index – GCI), котрий характеризує конкурентоспроможність, інноваційність і продуктивність економіки країни. Зокрема, зменшення/збільшення GCI на один пункт спричиняє відповідну динаміку продуктивності праці на 2,3 %, ступеня освоєння національних інновацій – на 2,2, конкурентоспроможності – на 2,1 %.

Як показує досвід розвинутих країн, діджитал-технології не лише здатні безпосередньо забезпечити економічне зростання, а й створюють самопідтримуючий синергетичний ефект за рахунок численних екстерналій, що поширюються на економічну, соціальну, технологічну, інтелектуальну й інфраструктурну складові розвитку. Наприклад, згідно з розрахунками експертів ЄС, у разі призупинення цифрової трансформації щороку втрачатиметься майже 600 млрд євро. Тому на рівні Співтовариства активно просуваються ідеї єдиного цифрового ринку, який до 2020 р. буде спроможний створити близько 6 млрд зв'язків фізичних осіб із інтернет-мережею.

Особливо дискусійним є питання вимірювання впливу діджиталізації на економіку країни. Глобальний інститут McKinsey у своїх дослідженнях використовує Індекс діджиталізації галузі (Industry Digitization Index) для вимірювання рівня діджиталізації окремих секторів економіки країни. Індекс включає три субіндекси:

1) витрати на цифрові активи (витрати на апаратне забезпечення, витрати на програмне забезпечення та ІТ-послуги, витрати на телекомунікаційне обладнання);

2) витрати на цифрові активи в розрахунку на одного працівника (витрати на апаратне забезпечення в розрахунку на одного працівника, витрати на програмне забезпечення та ІТ-послуги в розрахунку на одного працівника, витрати на телекомунікаційне обладнання в розрахунку на одного працівника);

3) нарощування цифрового капіталу (загальний обсяг апаратного забезпечення в розрахунку на одного працівника, загальний обсяг програмного забезпечення в розрахунку на одного працівника).

Результати на рівні секторів зважуються з урахуванням економічного розміру сектора та порівнюються з еталонним значенням, яким, на думку Глобального інституту McKinsey, є сектор ІКТ у США (табл. 1.3).

Таблиця 1.3

Рівень діджиталізації галузей економіки США та ЄС за даними Глобального інституту McKinsey, 2021 р.

Рівень діджиталізації	Галузі економіки США	Галузі економіки ЄС
Високий	інформаційно-комунікаційні технології, засоби масової інформації, сектор фінансових і страхових послуг	інформаційно-комунікаційні технології, засоби масової інформації, сектор фінансових послуг
Середній	високотехнологічна промисловість, оптова торгівля, роздрібна торгівля	гірничодобувна промисловість, сектор операцій з нерухомістю, сектор освітніх послуг
Низький	сектор охорони здоров'я, будівництво, сектор готельно-ресторанних послуг	сектор готельно-ресторанних послуг, будівництво, сільське господарство

Водночас низка досліджень Глобального інституту McKinsey присвячена сформованості цифрового сектора економіки ЄС. Оцінка

діджиталізації економіки відбувається за трьома групами країн. Перша група представлена десятьма країнами Центрально-Східної Європи (Болгарія, Хорватія, Чеська Республіка, Угорщина, Латвія, Литва, Польща, Румунія, Словаччина та Словенія). Ця група отримала назву «цифрових претендентів», оскільки зазначені країни демонструють великий потенціал розвитку галузі цифрових технологій. Друга група, так звані «цифрові лідери», складається з відносно невеликих за територіальним розміром країн з високими показниками діджиталізації: Бельгія, Данія, Естонія, Фінляндія, Ірландія, Люксембург, Нідерланди, Норвегія і Швеція. Третя група, що має назву «велика п’ятірка країн ЄС», включає Францію, Німеччину, Італію, Іспанію та Великобританію. У цих п’яти країнах показники діджиталізації є відносно високими, але нижчі, порівняно з «цифровими лідерами».

Сучасне народне господарство України та багатьох інших країн світу зазнає трансформації з урахуванням тенденцій залучення новітніх інформаційних і комп'ютерних технологій для розв'язання різного роду завдань, інтеграції їх у більшість сфер економічної діяльності. Зростання ІТ-компонентів у всіх галузях економіки в підсумку призведе до трансформації постіндустріального суспільства в цифрове. Таким чином, можна сказати, що сьогодні актуальним є саме цифровий варіант розвитку економіки, який забезпечуватиметься завдяки використанню економічних агентів інструментів впливу в різних сферах.

Водночас цифровий варіант розвитку економіки актуалізує питання формування інформаційної безпеки держави.

1.2. Інформаційна безпека в системі національної безпеки держави

В нинішній час інформація перетворилась у формуючий фактор матеріальної сфери життя людини, виступаючи у ролі інноваційних технологій, комп’ютерних програм тощо. Водночас вона використовується як основний засіб міжособистісної взаємодії, постійно виникаючи та

замінюючись у процесі переходу від однієї інформаційної системи до іншої. Таке становище інформації в суспільстві обумовлює необхідність відноситись до неї як до товару, що має певну цінність, зростаючу залежно від достовірності, корисності й доступності.

Термін інформація походить від латинського information і перекладається буквально: ознайомлення, роз'яснення, уявлення, поняття. Можна обмежитись даним визначенням терміну інформація оскільки в більшості наукових праць з проблем інформаційної безпеки, поняття інформація не формується [1].

На макрорівні інформація впевнено займає позиції головного фактора могутності держави, адже здатність країни мати у своєму розпорядженні найсучасніші інформаційні технології дозволяє ефективно управляти інформацією. Володіння державою такою здатністю – шлях до подальшого нарощування своєї економічної міцності.

На мікрорівні обсяг, достовірність, цілісність, якість обробки інформації визначає ефективність дій менеджменту як підприємства, так і держави в цілому, а тим самим актуалізує використання інформаційних технологій в управлінні валютно-фінансовими, соціально-економічними процесами. «Без необхідного обсягу та якості інформації неможливо забезпечити розвиток господарюючого суб'єкта на основі високотехнологічного виробництва, ефективних методів організації праці» [2].

Інформаційна безпека у 21 столітті виходить на перший план у системі національної безпеки держави, тому тільки ця держава може розраховувати на лідерство в економічній, військово-політичній та інших сферах, отримати стратегічну і тактичну перевагу, гнучкіше регулювати економічні витрати на розвиток озброєнь і військової техніки, підтримувати перевагу з ряду новітніх технологій, яка має лідерство у засобах інформації та інформаційної боротьби.

Аналіз наукових джерел свідчить про наявність у сучасній літературі багатьох визначень сутності інформації, серед яких виділяють різні принципові підходи.

Академік В. Глушков вважав, що інформація є атрибутом (невід'ємною властивістю) не тільки живих, розумних істот, але й усіх матеріальних тіл. Інформація у неорганічній природі існує об'єктивно, але як би в потенційній формі. З появою живих організмів, тобто споживачів інформації, починається використання інформації з метою пізнання й управління. Отже, інформація, будучи атрибутом матерії й руху, існує споконвічно в просторі й часі [3].

Засновник кібернетики Н. Вінер стверджував, що інформація є властивістю лише високоорганізованої, тобто живої матерії. Інформація й інформаційні процеси, на його думку, властиві тільки біологічній і соціальній формам руху матерії. Він вважав, що живі організми розвивають необхідну їм інформацію завдяки постійній взаємодії із природою, обміну з навколишнім середовищем [4]. При цьому інформації належить особлива інтегруюча роль, завдяки якій у живих істот й насамперед у людини, розвилися адаптаційні здібності. У такий спосіб інформація лежить в основі процесів саморегулювання у живій природі.

К. Шеннов пропонує функціональний підхід до розуміння сутності інформації, у рамках якого інформацію часто розглядають як властивість лише систем, що самоорганізуються, не тільки у живій природі, але й у техніці. До них, наприклад, відносять і живі істоти й кібернетичні системи, для яких характерні процеси саморегулювання завдяки передаванню, зберіганню й переробленню інформації [5].

В. Афанасьєв пропонує ще й соціальний підхід до інформації. Він розуміє інформацію як продукт життєдіяльності тільки соціальних форм матерії, людського суспільства. Інформація існує об'єктивно в процесі й часі, але проявляється лише в процесі пізнання людиною навколишнього світу [6].

Серед соціальних теорій інформації особливе значення має семіотична концепція. Основною проблемою зв'язків та інформаційних систем у суспільстві є проблема мови, яку можна розглядати як семіотичну систему знаків, символі і правил, за допомогою яких відображається й передається інформація.

Так, з позиції семіотики, будь-яка інформація (повідомлення) є не що інше як набір знаків й, отже, може розглядатися з позиції семантичних, синтаксичних і прагматичних характеристик.

Синтаксис визначає систему правил у мові, за якими із знаків побудовані речення і вислови. Семантика – це вчення про зміст слів. Зміст слова, як відомо, передається через поняття. Семантика вивчає точність відтворення в інформації сутності віддзеркаленого явища, тобто його змісту. У свою чергу, прагматика вивчає зв’язки між знаками й людьми, які ці знаки встановлюють і вживають. Вона встановлює зв'язок змісту повідомлення й мети діяльності або управління, корисність, важливість, роль і значення інформації для конкретних справ, тобто цінність.

Цим трьом частинам лінгвістики відповідають три аспекти інформації: формальний (синтаксичний), змістовний (семантичний) і ціннісний (прагматичний). Інформація, яка виходить від об’єкта-оригіналу й сприймається суб’єктом-споживачем в інтересах тієї чи іншої діяльності, кодується й передається людиною за допомогою мови що містить не тільки формальні (кількісні), але й змістовні (якісні) характеристики, віддзеркалені синтаксисом, семантикою й прагматикою. Відповідно до семіотичної теорії, тільки їхня єдність виражає сутність інформації. Таким чином, інформація є семіотикою – це кодовані за допомогою знакових систем і передані для використання в спілкуванні людьми відомості, повідомлення, дані в сполученні синтаксичних, семантичних і прагматичних характеристик.

У сучасній системі наукових знань мають місце й інші теорії, які пояснюють сутність інформації, що свідчить про граничну узагальненість, складність і багатогранність цього явища. Слід зазначити, що в системі наукових знань відсутнє універсальне поняття інформації. Відсутність єдиного розуміння даного явища призвело до безлічі його дефініцій, що наочно представлено у таблиці 1.4.

Таблиця 1.4

Узагальнені підходи до формулювання поняття «інформація»

Науковець	Коротка характеристика поняття
Н.Вінер	Інформація є інформація, не матерія й не енергія. Це позначення змісту, отриманого від зовнішнього світу в процесі пристосування до нього.
А.М. Яглов	Здатність знаків викликати образи.
Л. Бріллюєн	Повідомлення, освідомлення про положення справ, навчання, відомості про будь-що передані людьми.
К. Шеннон	Комунікація й зв'язок, у процесі якої усувається невизначеність.
У. Ешбі	Передача розмаїтості.
А.А. Моль	Оригінальність, новизна; міра складності структур.
А.М. Яглом	Здатність знаків викликати образи.
А.Д. Урсул	Передача відбиття розмаїтості в процесі й об’єктах.
Словник іншомовних слів	Повідомлення про якісь події, чиюсь діяльність; відомості, що є об’єктом зберігання, накопичення, переробки і передавання.

Це всього лише не значна частина визначень інформації, що розкривають ту або іншу грань даного феномена. На думку вчених, інформація має деякі загальні специфічні властивості: вона принципово не створюється й не знищується, а всього лише виникають (нові ідеї, знання), передається й приймається, так само як руйнується, губиться й забувається; при цьому вона може змінювати форму не змінюючи свого змісту.

Виходячи із наукових підходів і законодавчих актів України можна визначити інформацію як документовані або публічно оголошені відомості про події та явища, що відбувають у суспільстві, державі та навколишньому середовищі. Інформацією можна вважати дані, що знайшли власного споживача.

Вся інформація, що створюється і поширюється в нашій державі, незалежно від змісту, форм, часу й місця становить її інформаційні ресурси. Україна самостійно створює на своїй території інформаційні ресурси і вільно ними розпоряджається, за винятком випадків, передбачених положеннями законів і міжнародними договорами. Національні інформаційні ресурси є

основою інформаційного суверенітету України, який гарантується інформаційною безпекою.

Інформаційна безпека є невід'ємною складовою національної безпеки.

Поняття «інформаційна безпека» з'явилося наприкінці 80-х років у праці німецького вченого Я.М. Жаркова йдеться про важливий інформаційний компонент у міжнародній безпеці та робиться спроба розглянути проблеми безпеки, які пов'язані з інформаційними загрозами комплексно. А у вітчизняній літературі починаючи з кінця 1991 – початку 1992 року спостерігається тенденція до відкритого дослідження проблеми інформаційної безпеки як окремого питання [7].

Формування інформаційної безпеки як напряму розвитку інформаційних систем правомірно датувати кінцем 20-го сторіччя. Адже саме тоді у суспільстві та фінансово-господарській діяльності суб'єктів господарювання почали траплятися випадки втрати інформації через зовнішні та внутрішні джерела, що обумовлювалося створенням локальних мереж (рис. 1.1).

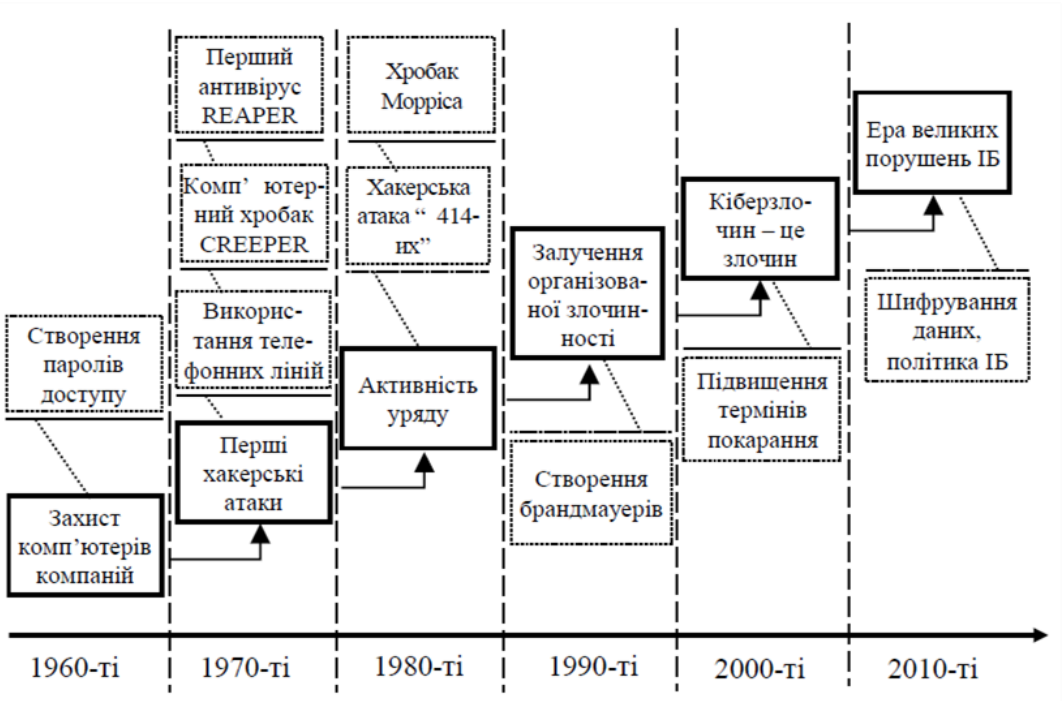

Рис. 1.1. Етапи розвитку інформаційної безпеки

Реалізація таких інцидентів призвела до необхідності впровадження нових інструментів захисту. Серед них головним було створення паролів доступу користувачів у відповідності із їх функціональними обов'язками.

Як загальнонаукову категорію «безпеку» можна визначити як такий стан розглянутої системи, коли вона здатна протистояти впливу зовнішніх і внутрішніх погроз, а також функціонування цієї системи не створює погрози для складової цієї ж системи й зовнішнього середовища.

Інформаційна безпека є невід'ємним напрямом розбудови інформаційного суспільства, розвиток якого повинен відбуватись не тільки через нарощування технологічних можливостей здійснення інформаційного обміну, але й через глибоке усвідомлення усіма суб'єктами інформаційних відносин – власниками інформації та її користувачами, виробниками інформаційних технологій і засобів, постачальниками послуг, державою – необхідності здійснення всіх заходів щодо інформаційних ресурсів та забезпечення інформаційної безпеки держави.

Розуміння поняття «інформаційна безпека» є важливим завданням наукового аналізу. Суть самого поняття виявляється у вираженні родового поняття, і таким є поняття безпеки, що в широкому сенсі характеризується як певний процес управління загрозами та небезпеками. Інформаційна безпека, відповідно, означає процес управління загрозами та небезпеками у сфері інформації [9].

Слід зазначити, що у науковій літературі поки бракує єдиного консолідованого погляду на зміст поняття «інформаційна безпека». Для одних воно відображає стан, для інших процес, діяльність, здатність, систему гарантій, властивість, функцію. Відтак постає необхідність в угрупуванні напрямів визначення аналізованого поняття, сучасні підходи до трактування якого містяться у таблиці 1.5.

Таблиця 1.5

Сучасні підходи до трактування поняття «інформаційної безпеки»

Науковець	Короткий зміст поняття
1	2
В. Богуш	Стан захищеності інформаційного середовища, який відповідає інтересам держави, за якого забезпечується формування, використання і можливості розвитку незалежно від впливу внутрішніх та зовнішніх інформаційних загроз.
В.А. Ліпкан, В.А. Авраменко	Стан захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації.
Р. Калюжний	Стан захищеності інформаційного простору, який забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави.
Н.Р. Нижник, Я.М. Жарков В.Т. Білоус	Стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни.
Б.А Кормич	Захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави.
О.І. Барановський	Стан захищеності національних інтересів України в інформаційному середовищі, за якого не допускається (або зводиться до мінімуму) завдання шкоди особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інформації й несанкціоноване її поширення та використання, а також через негативний інформаційний вплив та негативні наслідки функціонування інформаційних технологій.

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають.

При цьому інформаційну безпеку у найзагальнішому розумінні можна визначити як такий стан захищеності інформаційного простору держави, за якого неможливо завдати збитку властивостям об’єкта безпеки, що стосується інформації та інформаційної інфраструктури, і який гарантує безперешкодне

формування, використання й розвиток національної інформаційної сфери в інтересах оборони (рис. 1.2).

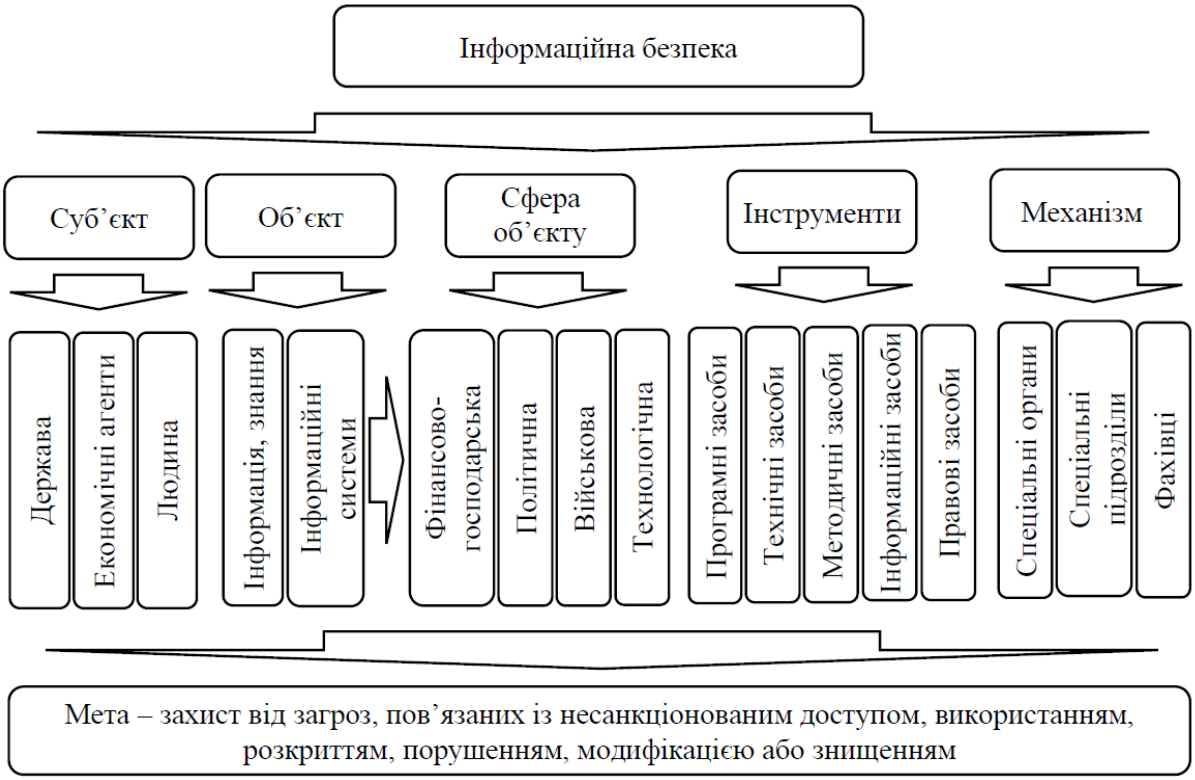

Рис. 1.2. Структура інформаційної безпеки

Основними характеристиками інформаційної безпеки на теперішній час залишаються такі:

– доступність – можливість використання інформації коли в цьому полягає потреба;

– цілісність – захищення інформації від несанкціонованих змін, забезпечення її точності та повноти;

– конфіденційність – властивість інформації не підлягати розголосові, надійність, секретність, гарантована приватність.

Інформаційна безпека як одна з характеристик стійкого розвитку виступає в якості базової цінності держави. Водночас, ціннісні орієнтації, що ґрунтуються на уявленнях про інформаційну безпеку у різних суспільних груп і окремих осіб, почасти не співпадають. Саме у цьому знаходить свій

безпосередній вираз вплив держави, яка за допомогою системи методів виражає загальні цінності у сфері інформаційної безпеки.

Виокремлюють два види інформаційної безпеки − інформаційна безпека особистості та інформаційна безпека держави.

Інформаційна безпека особистості – це захищеність психіки й свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до образ, самогубства тощо.

Інформаційна безпека держави характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) відносно небезпечних (дестабілізуючих) інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи.

Розрізняють внутрішні та зовнішні джерела інформаційної безпеки. Під внутрішніми джерелами розуміють відсутність історичного, політичного та соціального досвіду життя у правовій державі, що торкається процесу практичної реалізації конституційних прав та свобод громадян, в тому числі в інформаційній сфері. Е. Макаренко та В. Кирик вважають внутрішнім джерелом інформаційної безпеки посилення організованої злочинності та збільшення кількості комп'ютерних злочинів, зниження рівня освіченості громадян, що суттєво ускладнює підготовку трудових ресурсів для використання новітніх технологій, в тому числі інформаційних. Недостатня координація діяльності вищого державного керівництва, органів влади та військових формувань в реалізації єдиної державної політики забезпечення національної безпеки теж можна вважати таким джерелом. До цього слід додати і відставання України від розвинутих країн за рівнем інформатизації органів державної влади, юридично-фінансової сфери, промисловості та побуту громадян [10].

До зовнішніх джерел належать діяльність іноземних політичних, військових, економічних та розвідувальних структур в інформаційній сфері;

політика домінування деяких країн в інформаційній сфері; діяльність міжнародних терористичних груп; розробка концепцій інформаційних війн будь-якими структурами; культурна експансія у відношенні до конкретної країни.

Варто також окреслити і основні напрямами забезпечення інформаційної безпеки:

– у сфері міжнародної співпраці – інтеграція в міжнародну систему забезпечення інформаційної безпеки і співпраця по запобіганню протиправних дій в інформаційній сфері;

– у сфері оборони – вдосконалення системи моніторингу загроз та їх джерел, своєчасне інформування відповідних суб'єктів влади про стан інформаційного ресурсу і інформаційних систем оборонної сфери; засобів, методів і способів здійснення, спеціальних заходів і заходів інформаційного впливу; системи підбору і спеціальної підготовки користувачів.

Якщо проаналізувати зміст і напрями досліджень поняття інформаційної безпеки, то можна виокремити кілька підходів до визначення сутності цього явища (рис. 1.3).

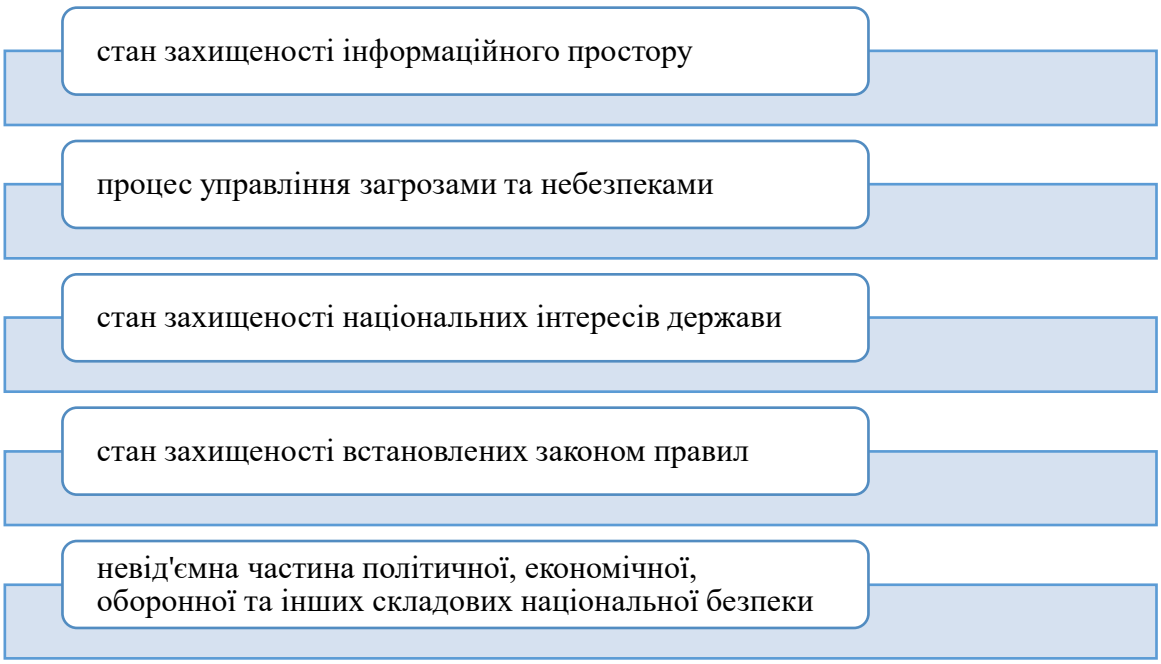

Рис. 1.3. Підходи до визначення сутності поняття «інформаційна безпека»

Проаналізувавши різні підходи до визначення поняття «інформаційна безпека» розуміємо недоцільність обрання тієї чи іншої позиції. Вищевказані підходи дають можливість зрозуміти це явище комплексно і системно. Крім того, інформаційна безпека не може розглядатися лише у якості окремого стану. Вона є властивістю та атрибутом інформаційного суспільства, діяльністю та результатом діяльності людини, яка спрямована на забезпечення безпеки в інформаційній сфері. Інформаційна безпека є не станом, а являється процесом, оскільки вона повинна враховувати майбутнє.

Інформаційну безпеку слід розглядати через єдність таких ознак як стан, властивість управління загрозами і небезпеками. Через ці ознаки забезпечується обрання оптимального шляху їх усунення та мінімізації впливу негативних наслідків, зокрема у сфері інформаційної діяльності держави. Тому можна виділити три основні аспекти визначення сутності «інформаційна безпека» (табл. 1.6) [11].

Таблиця 1.6

Існуючі аспекти визначення категорії «інформаційна безпека»

Аспект	Пояснення
1	2
1. Нормативно-правовий (ґрунтується на аналізі нормативно-правових актів)	Закон України «Про Концепцію Національної програми інформатизації» інформаційну безпеку розглядає як невід'ємну частину політичної, економічної, оборонної та інших складових національної безпеки. В Законі України «Про національну безпеку України» поняття «інформаційна безпека» не розкривається, увага фокусується на інформаційній сфері національної безпеки, при чому, не дається визначення навіть і даного поняття, а лише перераховуються загрози та напрями державної політики.
2. Доктрильний (виходячи з аналізу трактувань терміну в роботах дослідників, фахівців у цій галузі)	а) під інформаційною безпекою розуміють стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни; б) інформаційна безпека – безпека об'єкта від інформаційних загроз або негативних впливів, пов'язаних з інформацією та нерозголошення даних про той чи інший об'єкт, що є державною таємницею; в) інформаційна безпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства і держави.

Продовження табл. 1.6

1	2
3. Енциклопедичний (в основі – аналіз визначень, наведених у словниках, енциклопедіях)	Інформаційна безпека означає: законодавче формування державної інформаційної політики; гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України; створення і впровадження безпечних інформаційних технологій; охорону державної таємниці, а також інформації з обмеженим доступом; захист національного інформаційного простору України від розповсюдження спотвореної або забороненої для поширення інформаційної продукції

На підставі аналізу законодавчої, нормативно-правової бази та наукових підходів до аналізу інформаційної безпеки пропонується визначити її як захищеність встановлених законодавчо інформаційних процесів у державі, що забезпечують гарантовані Конституцією України умови розвитку людини, суспільства й держави, середовища суспільства, яке забезпечує її використання і розвиток на користь громадян, організацій, держави.

Інформаційну безпеку можна розглядати з позиції захисту не тільки інтересів держави, а насамперед особистості і суспільства. Окрім цього інформаційну безпеку, на думку В. Петрика, можна також досліджувати в контексті захисту інформаційних технологій, інформаційної інфраструктури держави, інформаційного ринку та створення безпечних умов для існування й розвитку інформаційних процесів [12].

1.3. Класифікація ризиків і загроз інформаційній безпеці

В процесі дослідження інформаційної безпеки важливим питанням виступає моніторинг загроз та ризиків, що можуть загрожувати її ефективності.

Загрози інформаційним ресурсам можна розглядати в найширшому розумінні як потенційні явища природного, технічного або антропогенного характеру, що можуть чинити небажаний вплив на інформаційну систему, а також на інформацію, яка в ній зберігається.

Головні загрози, які можуть спричинити порушення основних категорій інформаційної системи, а також негативно вплинути на компоненти інформаційної системи, спричинити збій їх функціонування, втрату чи навіть повне знищення, такі: розголошення інформації; витік інформації; несанкціонований доступ до інформації (рис. 1.4).

Рис. 1.4. Традиційні способи нанесення збитку інформаційній безпеці

Інформаційні загрози становлять небезпеку для індивіда, суспільства та держави. Реалізація ризиків та їх трансформація в загрозу свідчить про неефективність функціонування державної системи управління інформаційною безпекою [13]. Управління загрозами і ризиками сприяє їх усуненню.

Загрози інформаційній безпеці можна трактувати як сукупність внутрішніх та зовнішніх умов, які можуть нанести шкоду інтересам особистості та суспільства через небажані інформаційні атаки на відповідні об’єкти інформаційної інфраструктури держави.

Актуальність вивчення загроз інформаційній безпеці підтверджує у своїй роботі і Г. Сащук [14]: «…З огляду на той факт, що під впливом інформаційних атак можуть цілеспрямовано змінюватись світогляд і моральність окремих людей і суспільства загалом, нав’язуються інтереси,

мотиви та спосіб життя інших людей, аналіз сутності та форм прояву сучасних методи прихованого агресивного впливу, прояву завідомо агресивних дій, які суперечать інтересам національної безпеки, та вироблення механізмів протидії їм у всіх напрямах».

Виходячи з численних досліджень [2-4, 11] можна виділити наступні види загроз інформаційній безпеці:

1) загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;

2) загрози несанкціонованого та неправомірного впливу сторонніх осіб на інформацію та інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування та використання);

3) відмови обладнання (можуть виникнути під час блокування доступу до одного або декількох ресурсів інформаційної системи);

4) загрози інформаційним правам і свободам особистості (право виробляти, поширювати, шукати, одержувати, передавати та використовувати інформацію; право інтелектуальної власності на інформацію і речової власності на документовану інформацію; право на особисту таємницю; право на захист честі і достоїнства і т. ін.).

Фактори загроз за видовою ознакою поділяються на політичні, економічні та організаційно-технічні.

Під політичними факторами загроз інформаційній безпеці розуміють:

– зміни геополітичної обстановки внаслідок фундаментальних змін у різноманітних регіонах світу, зведення до мінімуму ймовірності світової ядерної війни;

– інформаційна експансія розвинених країн, які здійснюють глобальний моніторинг світових політичних, економічних, воєнних, екологічних та інших процесів, та розповсюджують інформацію з метою здобуття односторонніх переваг;

– становлення нової державності в пострадянських країнах на основі принципів демократії, законності, інформаційної відкритості;

– знищення колишньої командно-адміністративної системи державного управління, а також системи забезпечення безпеки;

– порушення інформаційних зв’язків унаслідок утворення на території колишнього СРСР нових держав;

– прагнення пострадянських країн до більш тісного співробітництва із закордонними країнами в процесі проведення реформ на основі максимальної відкритості сторін;

– низька загальна правова та інформаційна культура сторін.

Основними економічними факторами загроз безпеці інформації є:

– перехід на ринкові відносини в економіці, поява на ринку великої кількості вітчизняних та зарубіжних комерційних структур − виробників та споживачів інформації, засобів інформатизації та захисту інформації, включення інформаційної продукції в систему товарних відносин;

– критичний стан вітчизняних галузей промисловості, яка виробляє засоби інформатизації та захисту інформації;

– розширення кооперації із зарубіжними країнами в розвитку інформаційної інфраструктури.

Основними організаційно-технічними факторами загроз інформаційній безпеці є:

– недостатня нормативно-правова база у сфері інформаційних відносин, у тому числі в галузі забезпечення інформаційної безпеки;

– недостатнє регулювання державою процесів функціонування та розвитку ринку засобів інформатизації, інформаційних продуктів та послуг;

– широке використання у сфері державного управління та кредитно-фінансової сфери незахищених від витоку інформації імпортних технічних та програмних засобів для зберігання, обробки та передавання інформації;

– зростання обсягів інформації, яка передається відкритими каналами зв'язку;

– загострення криміногенної обстановки, зростання числа комп'ютерних злочинів, особливо в кредитно-фінансовій сфері.

Ієрархічна класифікація загроз інформаційній безпеці включає в себе глобальні, регіональні та локальні фактори.

До глобальних факторів загроз інформаційній безпеці відносяться: недружня політика іноземних держав у галузі глобального інформаційного моніторингу, розповсюдження інформації та нових інформаційних технологій; діяльність іноземних розвідувальних та спеціальних служб; діяльність іноземних політичних та економічних структуру, спрямована проти інтересів держави; злочинні дії міжнародних груп, формувань та окремих осіб.

Регіональні фактори загроз інформаційній безпеці включають в себе: використання інформаційної інфраструктури колишнього СРСР для передавання конфіденційної інформації; невідповідність інформаційного забезпечення державних та суспільних інститутів сучасним вимогам управління економічними, політичними та соціальними процесами; відставання від розвинених країн світу з темпів та масштабів розробки та впровадження нових інформаційних технологій; недопустимо високий рівень технологічної залежності держави від зарубіжних країн у зв’язку з широким використанням імпортних засобів обчислювальної техніки, систем телекомунікації, зв'язку та інформаційних технологій; розвиток зарубіжних технічних засобів розвідки та промислового шпигунства; зростання злочинності в інформаційній сфері; використання старих методів та засобів захисту національних інформаційних мереж; широке розповсюдження комп'ютерних вірусів, призначених для ураження систем управління та зв'язку; відсутність ефективної системи забезпечення цілісності, незмінності та схоронності нетаємної інформації, у тому числі такої, що є інтелектуальною власністю.

До локальних факторів загроз інформаційної безпеки включають: перехоплення електронних випромінювань; застосування підслуховуючих пристроїв або закладок; дистанційне фотографування; розкрадання носіїв

інформації; копіювання носіїв інформації з подоланням заходів захисту; незаконне приєднання до апаратури та ліній зв’язку; упровадження та використання комп'ютерних вірусів і т. ін.

Загрози самі по собі не виникають, носіями загроз безпеки інформації є джерела загроз. Джерелами загроз можуть бути:

– суб’єкти (особи);

– об’єктивні прояви.

Причому джерела загроз можуть міститися і перебувати як усередині організації, що захищається, – внутрішні джерела, так і поза нею – зовнішні джерела.

Усі джерела загроз безпеки інформації можна розділити на три основні групи [15]:

1. Обумовлені діями суб'єкта (антропогенні джерела загроз).

2. Обумовлені технічними засобами (техногенні джерела загроз).

3. Обумовлені стихійними джерелами.

Антропогенними джерелами загроз безпеки інформації виступають суб'єкти, дії яких можуть бути кваліфіковані як умисні або випадкові злочини.

Перша група є порівняно найширшою і становить найбільший інтерес з погляду організації захисту, оскільки дії суб'єкта завжди можна оцінити, спрогнозувати та вжити адекватні заходи. Методи протидії в цьому випадку є керованими і безпосередньо залежать від організаторів захисту інформації. Як антропогенне джерело загроз можна розглядати суб'єкта, що має доступ (санкціонований або несанкціонований) до роботи із штатними засобами об'єкта захисту.

Суб’єкти (джерела), дії яких можуть призвести до порушення безпеки інформації, можуть бути як зовнішніми, так і внутрішніми. Зовнішні суб'єкти (джерела) можуть бути випадковими або умисними і мати різний рівень кваліфікації. Внутрішні суб'єкти (джерела), як правило, є висококваліфікованими фахівцями у сфері розробки й експлуатації програмного забезпечення і технічних засобів, знайомими із специфікою

вирішуваних завдань, структурою і основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, мають можливість використання штатного устаткування і технічних засобів мережі.

Необхідно враховувати також, що особливі підгрупи внутрішніх антропогенних джерел складають особи з порушеною психікою і спеціально впроваджені та завербовані агенти, які можуть бути представниками основного, допоміжного і технічного персоналу, а також служби захисту інформації. Остання підгрупа розглядається у складі перерахованих вище джерел загроз, але методи захисту від загроз для цієї підгрупи можуть мати свої відмінності.

Друга група охоплює джерела загроз, зумовлені технократичною діяльністю людини і розвитком цивілізації. Проте йдеться про випадки, коли наслідки, викликані такою діяльністю, вийшли з-під контролю людини і існують самі по собі.

Даний клас джерел загроз безпеки інформації особливо актуальний, оскільки в умовах, що склалися, експерти очікують різке зростання числа техногенних катастроф, викликаних фізичним і моральним старінням устаткування, а також відсутністю матеріальних засобів на його оновлення. Технічні засоби, що є джерелами потенційних загроз безпеці інформації, так само можуть бути зовнішніми і внутрішніми.

Третя група джерел загроз охоплює обставини, що розглядаються як чинники, які мають непереборну силу, тобто такі обставини, які мають об'єктивний і абсолютний характер, поширюючись на всі об’єкти і всіх суб’єктів діяльності у сфері інформаційного обміну. До непереборної сили в законодавстві та договірній практиці відносять стихійні лиха чи інші обставини, які неможливо передбачити або їм запобігти, або ж можливо передбачити, але неможливо запобігти при сучасному рівні розвитку людських знань і можливостей. Такі джерела загроз абсолютно не піддаються прогнозуванню, і тому заходи захисту від них повинні застосовуватися завжди.

Стихійні джерела потенційних загроз інформаційної безпеки, як правило, є зовнішніми стосовно об’єкта захисту, і під ними розуміються, перш за все, природні катаклізми. Також до цієї групи загроз входять різні непередбачувані обставини, нез’ясовані явища та інші форс-мажори. Класифікація джерел загроз наведена на рисунку 1.5.

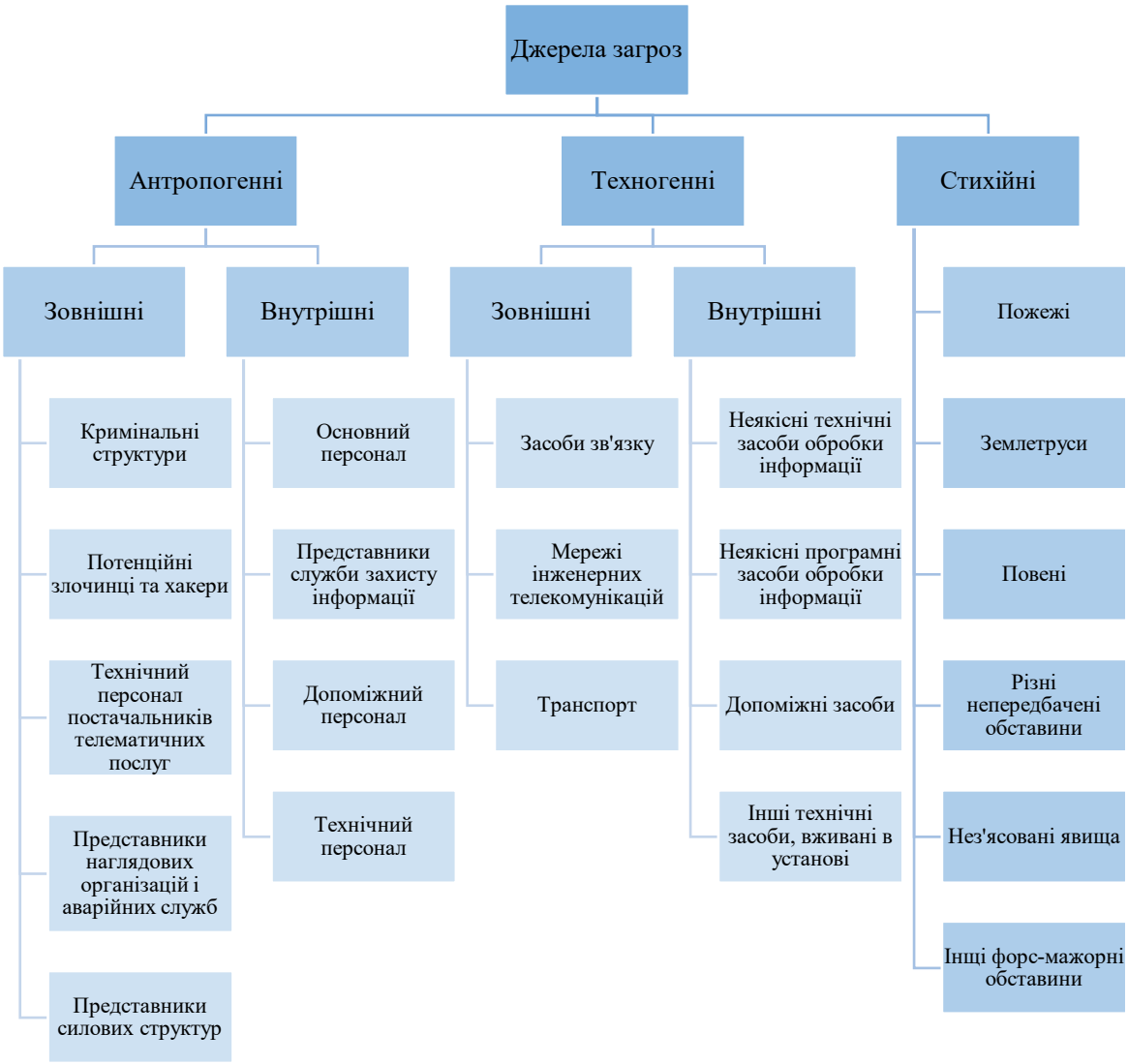

Рис. 1.5. Класифікація джерел загроз

Проникнення в інформаційну сферу та її використання кримінальними, в тому числі й терористичними елементами призвело до появи принципово нового різновиду терористичних дій у віртуальному просторі – кібертероризму. Власне, як термін це поняття в ІТ-лексиконі з’явилось

приблизно в середині 1980-х рр. Саме тоді один із наукових співробітників США Беррі Колін уперше впровадив його в офіційний обіг. У 1997 р. спеціальний агент ФБР М. Полліт визначив цей вид тероризму як «навмисні політично вмотивовані атаки на інформаційні та комп'ютерні системи, комп'ютерні програми й дані, що полягають у застосуванні насильства щодо цивільних цілей із боку субнаціональних груп або таємних агентів».

Одним із нових видів загроз інформаційній безпеці є кібертероризм. На відміну від традиційних крадіжок і шахрайства, він постійно вдосконалюється і йде в ногу з технологіями, що, своєю чергою, ускладнює виявлення і припинення цих протиправних дій. Основною проблемою боротьби зі злочинністю в Інтернеті є сама транснаціональність мережі та відсутність механізмів контролю, необхідних для дотримання закону. Таким чином, необхідним виступає дослідження державної політики в напрямку формування інформаційної безпеки з урахуванням окреслених загроз.

Висновки до розділу 1

Поступове й доволі умовне поєднання умовного і реального просторів за допомогою ІТ-систем і мережних технологій різного функціонального призначення, а також відповідного програмного забезпечення призвело до формування кіберпростору − віртуального комунікаційного середовища, утвореного системою зв'язків між користувачами та об'єктами інформаційної інфраструктури.

Розглядаючи сучасні підходи до трактування поняття «інформаційна безпека» варто визначити, що являє собою поняття «інформація».

Аналіз різноманітних джерел свідчить про наявність безлічі визначень сутності інформації. Виходячи із наукових підходів і законодавчих актів України можна визначити інформацію як документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому середовищі.

Інформаційна безпека є невід'ємною складовою національної безпеки держави. Із зростанням науково-технічного прогресу зростає і важливість питання інформаційної безпеки громадянина, суспільства, держави.

Інформаційна безпека розглядається як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Слід зазначити, що у науковій літературі бракує єдиного погляду на зміст поняття «інформаційна безпека».

Інформаційну безпеку у найзагальнішому розумінні − стан захищеності інформаційного простору держави, за якого неможливо завдати збитку властивостям об'єкта безпеки, що стосується інформації та інформаційної інфраструктури, і який гарантує безперешкодне формування, використання й розвиток національної інфосфери в інтересах оборони.

Основними характеристиками інформаційної безпеки на сьогодні залишаються доступність, цілісність та конфіденційність.

Загалом же, інформаційну безпеку можна розглядати з позиції захисту не тільки інтересів держави, а насамперед особистості і суспільства.

У процесі дослідження інформаційної безпеки важливо моніторити загрози та ризики, що мають негативний вплив, до них відносять: розголошення, витік та несанкціонований доступ до інформації.

Загрози інформаційній безпеці можна трактувати як сукупність умов, які можуть нанести шкоду інтересам особистості та суспільства через небажані інформаційні атаки на відповідні об’єкти інформаційної інфраструктури держави.

Виділяють різноманітну кількість видів загроз інформаційні безпеці, серед яких: загрози впливу неякісної інформації на особистість, суспільство,

державу; загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію та інформаційні ресурси; збої в роботі обладнання; загрози інформаційним правам і свободам особистості.

Фактори загроз інформаційні безпеці держави за видовою ознакою поділяються на політичні, економічні та організаційно-технічні.

Натомість, ієрархічна класифікація загроз інформаційній безпеці включає в себе глобальні, регіональні та локальні фактори.

Носіями загроз безпеки інформації є джерела загроз − суб'єкти та об'єктивні прояви. При цьому, джерела загроз можуть бути як внутрішніми, так і зовнішніми.

Принципово новим різновидом терористичних дій у віртуальному просторі є кібертероризм. Хоча чіткого визначення даного поняття поки не існує, під ним ми розуміємо суспільно небезпечну діяльність, що свідомо здійснюється в кіберпросторі окремими особами або організованими групами з терористичною метою та реалізується ними через заздалегідь сплановані й політично вмотивовані кібератаки на інформаційно-телекомунікаційних системах з використанням високих технологій.

Удосконалення нормативно-правової бази забезпечення інформаційного суспільства в Україні дозволить врегулювати нормативні аспекти діяльності щодо впровадження та використання інформаційних технологій, продукування та розповсюдження електронної інформації, створення та використання національних інформаційних ресурсів та радіочастотного ресурсу, розвитку телекомунікацій, створення системи стандартизації у сфері інформації, забезпечення інформаційної безпеки тощо. Однією з основних перешкод на шляху побудови інформаційного суспільства в Україні є неузгодженість норм національного законодавства між собою, а також з нормами міжнародного права у цій сфері.

Потребує впорядкованості понятійний апарат та термінологія нормативно-правової бази забезпечення розвитку інформаційного суспільства в Україні.

Необхідно нормативно встановити такий порядок підготовки законів і підзаконних актів щодо сфери інформатизації, який забезпечить попередній аналіз проектів законів та підзаконних актів експертами різних секторів – громадського, приватного і державного. Відсутність такої процедури призводить до того, що більшість законів, які формують теоретичну основу галузі, не узгоджуються один з одним і тому виникають проблеми в їх практичному застосуванні.

РОЗДІЛ 2
ОЦІНЮВАННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Методи оцінювання ризиків та загроз безпеці інформаційних ресурсів

Аналіз стану безпеки інформації та відповідних загроз стає дедалі важливішим питанням, що хвилює увесь світ.

Інформаційна безпека – порівняно молода галузь інформаційних технологій, що швидко розвивається. Словосполучення «інформаційна безпека» в різних контекстах може набувати різного змісту. Під інформаційною безпекою розуміють захищеність інформації та підтримувальної інфраструктури від випадкових або навмисних впливів природного чи штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації та відповідної інфраструктури.

Що ж до захисту інформації, то це комплекс заходів, спрямованих на забезпечення інформаційної безпеки.

Вочевидь, для розв'язання проблеми оцінювання безпеки інформаційних ресурсів необхідно дослідити загальні принципи побудови інформаційних систем і мереж, зокрема й таких, що мають спеціальні засоби захисту. Це питання докладно розглянуто в роботі Н.Ф. Козакова [28], завдяки чому маємо змогу встановити параметри оцінювання щодо захищеності ресурсів. Він провів аналіз тенденцій забезпечення захищеності інформаційної безпеки для автоматизованих систем [29]. Спираючись на дані досліджень маємо всі підстави прогнозувати розробку відповідних методик оцінювання інформаційної безпеки. Процедури вибору та застосування програмних засобів для розробки й упровадження систем відповідних оцінок описано в праці М.В. Ткачука. В роботі Н. В. Ващенка відзначено деякі аспекти щодо

створення системи оцінювання, які реалізовано в політиці запобігання загроз інформаційній безпеці в практичній діяльності.

Баскервіль [30] із середини 1980-х рр. здійснює фундаментальні дослідження в галузі аналізу загроз інформаційній безпеці. Він визначив контрольний список аналізу ризиків для інструментів, що використовуються з метою розробки заходів із забезпечення інформаційних систем. Хан [31] запропонував підхід до аналізу ризиків стосовно інформаційної безпеки, яка передбачає безперервність функціонування експлуатаційного середовища. Кілька методик спираються на такі види аналізу, як матричний підхід [32], парне порівняння тощо. Деякі дослідники розробили комплексні інструменти для оцінювання стану інформаційних ресурсів: ISRAM (Information Security Risk Analysis Method), OCTAVE (The Operationally Critical Threat, Asset, and Vulnerability Evaluation), FRAP (Facilitated Risk Assessment Process).

У XXI сторіччі інформаційні технології швидко проникли в усі сфери діяльності суспільства, і це спонукає до модернізації та формування інформаційної системи від базового (фізичного) рівня до верхнього (користувацького). Отже, людство ввійшло в нову еру – еру інформації.

Але зрештою розвиток інформаційних систем приніс не лише велику користь, а й гострі проблеми щодо загроз інформаційній безпеці. Віруси, хакерські атаки, витоки секретної інформації, відмови систем, переривання обслуговування і різні комп’ютерні злочини примножуються. Згідно з дослідженнями Федерального бюро розслідувань США, економічні втрати, зумовлені неналежною мережною безпекою, щороку перевищують 170 млрд. доларів. За даними китайського інформаційного центру Інтернет-мереж (CN CERT), у першій половині 2014 року CN CERT отримав 4780 звітів про інциденти з мережною безпекою. Отже, не дивно, що в 2015 році плата за послуги із забезпечення інформаційної безпеки в Китаї досягла 153 млрд юанів [33].

Проблеми безпеки інформаційних систем привертають пильну увагу фахівців різних сфер приватного і державного секторів. Вони застосовують

різні засоби нагляду, спонукаючи агентства на всіх рівнях підвищувати поінформованість і активізувати заходи з оцінювання стану інформаційної безпеки, щоб уникнути величезних ризиків.

Говорячи про системи безпеки, потрібно наголосити, що вони мають не просто обмежувати доступ користувачів до інформаційних ресурсів, а визначати й делегувати свої повноваження у спільному розв'язанні проблем, виявляти аномальне використання ресурсів, передбачати аварійні ситуації й усувати їхні наслідки, гнучко адаптувати мережеву структуру до збоїв, часткової втрати або тривалого блокування ресурсів.

Не варто, однак, забувати про економічну доцільність застосування тих чи інших заходів забезпечення безпеки інформації, які завжди мають бути адекватні існуючим загрозам.

Надійність захисту інформації, насамперед, буде визначатися повнотою розв’язання цілого комплексу завдань. Інакше кажучи, на практиці інформаційна безпека являє собою сукупність засобів і методів, що регулярно використовуються, а також заходів, що проводяться, щодо систематичного забезпечення необхідної достовірності сформованої та збереженої інформації. й обробляється на об’єкті інформаційно-аналітичною системою та передається по каналах. Захист повинен мати системний характер, тобто для отримання найкращих результатів усі розрізнені види захисту інформації мають бути об’єднані в одне ціле й функціонувати в складі єдиної системи як злагоджений механізм, призначений для виконання завдань із забезпечення безпеки інформації. Він має містити:

- нормативно-правовий базис захисту інформації;
- засоби, способи і методи захисту;
- органи і виконавців.

Визначення інформаційних ризиків – складне завдання. Зазвичай відповідні питання розв’язуються за допомогою експертних методів, що вносять суб’єктивізм в оцінку ризику. Тому, спираючись на таку оцінку, можна ухвалити хибне рішення інвестування в інформаційну безпеку.

Помилково оцінені ризики можуть призвести до переоцінки або, що набагато гірше, недооцінки небезпеки. Ось чому вибір обґрунтованої моделі визначення інформаційних ризиків становить актуальну проблему. Методи та засоби оцінювання інформаційних ризиків у систематизованому вигляді подано на рисунку 2.1.

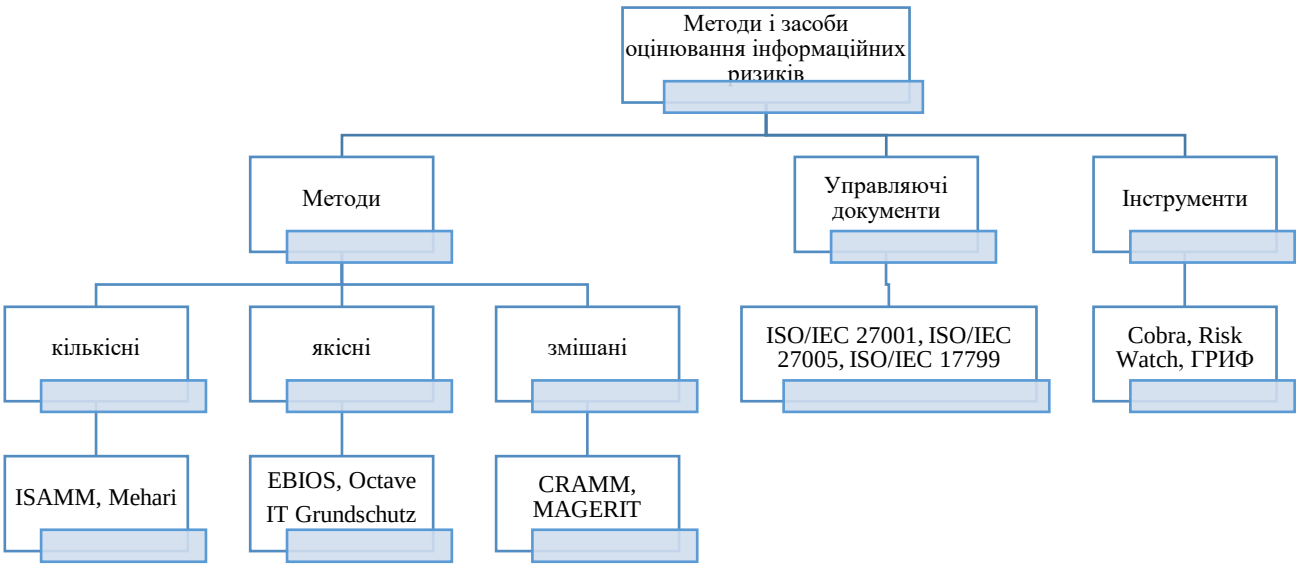

Рис. 2.1. Методи та засоби оцінювання інформаційних ризиків

Під методом розуміється систематизована сукупність кроків, дій, що їх необхідно виконати, аби розв’язати певне завдання чи досягти поставленої мети. У даному разі дати оцінку ризиків. Тобто метод – це покрокова інструкція плюс інструмент (програмний продукт) для оцінювання ризиків.

Усі методи оцінювання ризиків можна поділити на кількісні, якісні або змішані (комбінація кількісних і якісних методів).

Кількісні методи використовують вимірні, об’єктивні дані для визначення числових значень вартості активів, імовірності втрат і пов’язаних із ними ризиків. До цієї групи належать такі методи:

1) ISAMM (Бельгія) − дозволяє показувати й моделювати зниження ризику для кожного поліпшеного контролю і порівнювати з його вартістю

реалізації. Ефективність методу дозволяє виконувати обґрунтовану оцінку ризику в рамках, з мінімальними витратами часу і зусиль;

2) Mehari (Франція) − це модель управління ризиками, з модульними компонентами і процесами. Модуль оцінки охоплює, крім інформаційної системи, організацію та її місця розташування в цілому, а також умови роботи, правові та нормативні аспекти.

Якісні методи використовують відносний показник ризику (низький, середній, високий) чи вартості активу на основі рейтингу або за шкалою від 1 до 10. Якісна модель оцінює дії та ймовірності виявлених ризиків у швидкий і економічно ефективний спосіб. Набори ризиків, сформовані й проаналізовані згідно з якісною оцінкою, можуть виступати основою для цілеспрямованої кількісної оцінки. До групи якісних методів оцінювання інформаційних ризиків включають наступні.

1) EBIOS (Франція) являє собою повний набір посібників. Виробляються кращі практики, а також додатки документів, орієнтовані на кінцевих користувачів в різних контекстах. Цей метод широко використовується як в державному, так і приватному секторі. Формалізує підхід до оцінки ризику в області інформаційної безпеки систем. Метод враховує всі технічні і нетехнічні об'єкти;

2) OCTAVE (США) є самостійним підходом, що вказує на те, що персонал несе відповідальність за встановлення стратегії безпеки організації. Метод вимагає аналізу в розгляді відносини між критично важливими активами, загрозами для цих активів і вразливостями. Він визначає пов'язані з інформацією активи і зосереджує на них діяльність (акцент на важливих активах, не більше п'яти). Існують різні OCTAVE методи, засновані на OCTAVE критеріях: OCTAVE, OCTAVE-S і OCTAVE Allegro;

3) IT Grundschutz (Німеччина) пропонує спосіб для створення системи управління інформаційною безпекою. Включає в себе як загальні рекомендації по забезпеченню безпеки IT так і допоміжні технічні

рекомендації для досягнення необхідного рівня IT безпеки для конкретного домену.

Донедавна кількісні підходи застосовували значно частіше. Проте останнім часом використання суто кількісних методів управління ризиками, пов’язане із надзвичайно трудомісткою роботою, яка зрештою не дає відчутного виграшу, все більше поступається якісним методам оцінювання ризиків у сфері захисту інформації.

Що ж до комбінації кількісних і якісних методів, то вона, вочевидь, поєднує в собі як переваги, так і недоліки обох груп. До цієї категорії відносяться:

1) CRAMM (Великобританія) − метод, що досить складно використовувати без CRAMM інструменту. У інструмента така ж назва, як і у методу. В основі CRAMM лежить комплексний підхід до оцінки ризиків, поєднуючи кількісні та якісні методи аналізу. Метод універсальний і підходить для великих і малих організацій, як державного, так і комерційного секторів. Грамотне використання методу дає змогу отримати дуже хороші результати, найважливішим з яких є можливість економічного обґрунтування витрат організації на інформаційну безпеку та забезпечення безперервності бізнесу. Економічно обґрунтована стратегія управління ризиками зрештою економить гроші, уникаючи непотрібних витрат;

2) Magerit (Іспанія) − відкрита методологія аналізу та управління ризиками, пропонована в якості основи і керівництва: для того, щоб відповідальні особи за інформаційні системи знали про існування ризиків, вносили пропозиції систематичного методу аналізу цих ризиків, описували і планували відповідні заходи по утриманню ризиків під контролем, мали змогу для підготовки організації по процесу оцінки, аудиту, сертифікації та акредитації.

Порівняльну характеристику переваг та недоліків кількісних і якісних методів оцінювання ризиків у сфері захисту інформації наведено в таблиці 2.1.

Таблиця 2.1

Переваги і недоліки кількісних і якісних методів оцінювання ризиків у сфері захисту інформації

	Кількісні методи	Якісні методи
Переваги	Дозволяють визначати наслідки виникнення інцидентів у кількісний спосіб Уможливлюють аналіз витрат і користі при виборі підходу до захисту Допомагають отримати достатньо точну картину ризикованої ситуації	Дозволяють визначити сфери та осередки великої небезпеки в стислі терміни Аналіз ризиків і переваг порівняно легкий і дешевий
Недоліки	Кількісні оцінки неодмінно залежні від розміру та точності вибраної шкали вимірювання і можуть бути не точні, зокрема й через відсутність вірогідних даних про перебіг відповідних подій Остаточні висновки здебільшого мають спиратися на якісний опис Вимагають значно більших витрат, ніж якісні методи, найвищої кваліфікації виконавців і новітніх технічних засобів	Непридатні для визначення ймовірностей результатів, здобутих чисельними засобами Аналіз переваг більш ускладнюється за рахунок вибору захисту Результати мають загальний характер, усі значення тільки наближені тощо

Завданням якісного оцінювання є визначення можливих видів ризиків та ступеня серйозності загроз, виокремлення чинників, які впливають на рівень загроз, обґрунтування різних можливих контрзаходів. Відповідні методики не надають жодних кількісних значень (зокрема у грошовому вираженні). Вони достатньо популярні й порівняно прості. В основу їх розробки покладено, як правило, вимоги міжнародного стандарту ISO 17799:2002.

Кількісне оцінювання уможливлює перехід від імовірнісної оцінки ризику до відповідного числового значення. Методики подають реальні й обґрунтовані числові значення всіх складових процесу аналізу ризиків. Цими складовими можуть бути вартість захисних заходів, цінність активу, збиток для бізнесу, частота виникнення загрози, ефективність захисних заходів, вірогідність використання уразливості і т. ін. Кількісний аналіз дозволяє обчислити конкретне значення (у відсотках) імовірності реалізації загрози.

2.2. Визначення індикаторів оцінювання рівня інформаційної безпеки держави

Враховуючи, що трансформація суспільства відбувається паралельно з розвитком інформаційних технологій та вивченням цього питання в різних сферах людської діяльності, можна висунути гіпотезу щодо наявності взаємообумовлених взаємовпливів між системою інформаційної безпеки та національною економікою. З цією метою слід окреслити показники, які використовуються для вимірювання рівня інформаційної безпеки та розвитку національної економіки.

Оскільки інформаційна безпека є системним поняттям і включає різні аспекти, то на практиці з метою підвищення ефективності управління інформаційною безпекою країн застосовується ряд індикаторів, які характеризують тільки окремі її складові. Серед них можна виділити Глобальний індекс кібербезпеки (The Global Cybersecurity Index – GCI), Національний індекс кібербезпеки (The National Cyber Security Index – NCSI), Індексом розвитку інформаційних та комунікаційних технологій (ICT Development Index – ICTDI), Індекс мережевої готовності (Networked Readiness Index – NRI), Рівень цифрового розвитку (Digital Development Level – DDL). Дані індикатори характеризують рівень інформаційної безпеки з боків технологічного, інформаційного, організаційного забезпечення, тому їх застосування для вимірювання рівня інформаційної безпеки є виправданим.

Глобальний індекс кібербезпеки (далі GCI) вимірює рівень кібербезпеки для країн-членів Міжнародного союзу електрозв'язку та оцінюється за п'ятьма напрямками – технічні заходи, правові заходи, організаційні заходи, нарощування потенціалу, співпраця [102]. Цей показник є продуктом діяльності міжнародних організацій, що сприяють підвищенню ефективності міжнародного співробітництва та обміну знаннями на глобальному рівні. Його основна мета – виявити слабкі сторони кібербезпеки країни і поліпшити її можливості за допомогою розроблення стратегії кібербезпеки та відповідних стандартів.

Використовуючи значення Глобального індексу кібербезпеки за 2021 рік для 159 країн світу, ми побудуємо мапу, яка дасть змогу зробити візуальний аналіз географію країн і дасть змогу оцінити, які країни характеризуються високим рівнем безпеки, а які низьким (рис. 2.2).

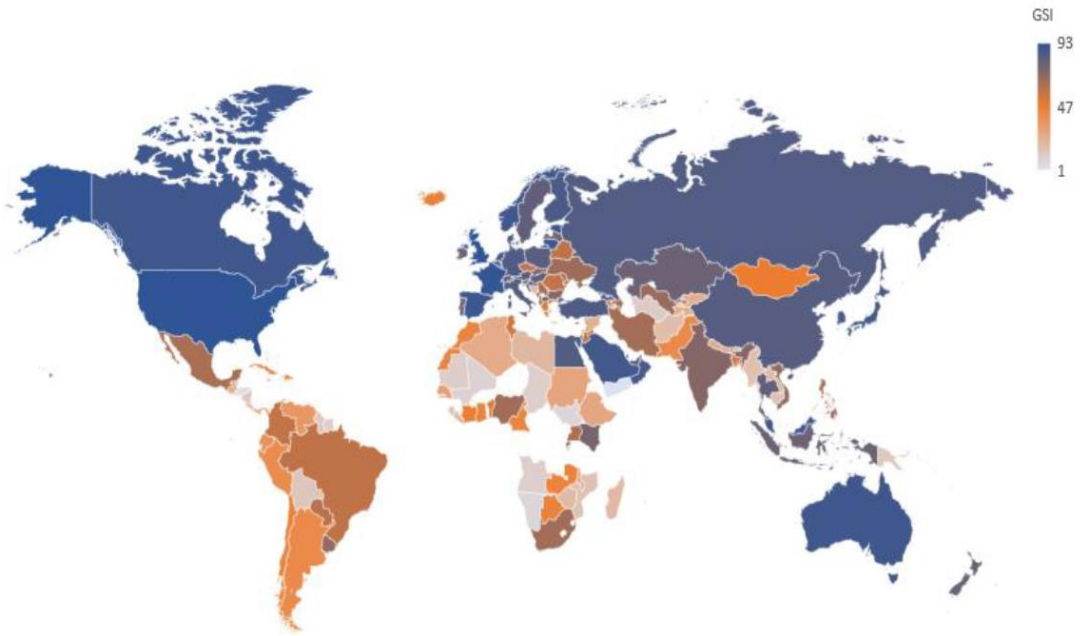

Рис. 2.2. Карта рейтингування країн за Глобальним індексом кібербезпеки за 2021 рік

На рисунку 2.2 представлено тільки ті країни, для яких існують емпіричні дані. Візуальний аналіз показує, що високий рівень кібербезпеки характерний для таких країн, як США (93), Велика Британія (93), Франція (92), Естонія (91), Литва (91), Сінгапур (90), Іспанія (90), Канада (89), Австралія (89), Люксембург (89), Малайзія (89), Нідерланди (89), Норвегія (89), Японія (88), Маврикій (88), Саудівська Аравія (88), Південна Корея (87), Оман (87), ряд країн ЄС та Китай.

Для більшості країн Африки, деяких країн Південно-Східної Азії, пострадянських країн, Гватемали, Гондурасу, Панами, Нікарагуа, Гайани, Болівії, Суринама GSI – є дуже низьким. Для більшості країн Південної Америки, ряду країн Східної Європи, України, Індії, Монголії, Мексики та

інших даний індекс відповідає середньому значенню (47) та вище. Тобто можна зробити попередній висновок про наявність певної залежності між рівнем розвитку економіки країни та рівнем її кібербезпеки, оскільки високі бали GSI відповідають країнам, що характеризуються високим рівнем економічного розвитку. З іншого боку, найменш розвинені країни з низькими показниками економічного розвитку також демонструють низький рівень кібербезпеки.

Національний індекс кібербезпеки (далі NCSI), розроблений Академією електронного врядування, визначає рівень готовності країни протидіяти кіберзагрозам та керувати кіберінцидентами. Результати його визначення застосовують у якості інформації для формування джерел нарощування національного потенціалу у галузі кібербезпеки. На відмінність від GSI, NCSI враховує особливості системи кіберзахисту із врахуванням національних аспектів. Для розрахунку використовують 46 показників, згрупованих за 12 напрямами, а саме: розроблення політики та стратегії у сфері кібербезпеки; аналіз та інформація про кіберзагрози; організація навчання та підвищення кваліфікації у сфері кібербезпеки; оцінювання внеску в глобальну кібербезпеку; рівень захисту цифрових послуг: відповідальність, стандарти, повноваження; організація захисту основних служб; електронна ідентифікація та трастові послуги; захист персональних даних; реагування на кіберінциденти; управління кіберкризою; боротьба з кіберзагрозами; захист персональних даних; реагування на кіберінциденти; кіберрегулювання кризи; боротьба з кіберзлочинністю; військові кібероперації.

Використовуючи емпіричні значення NCSI за 2021 рік для 159 країн світу, побудуємо карту для візуального аналізу та оцінки країн, для яких країн характерний високий рівень безпеки, а для яких країн низький (рис. 2.3).

Аналізуючи дані, представлені на рисунку 2.3, можна сказати, що країни, які відносяться до розвинутих, а саме США, Канада, Австралія, країни Європи, та інші, мають високі значення національного індексу кібербезпеки.

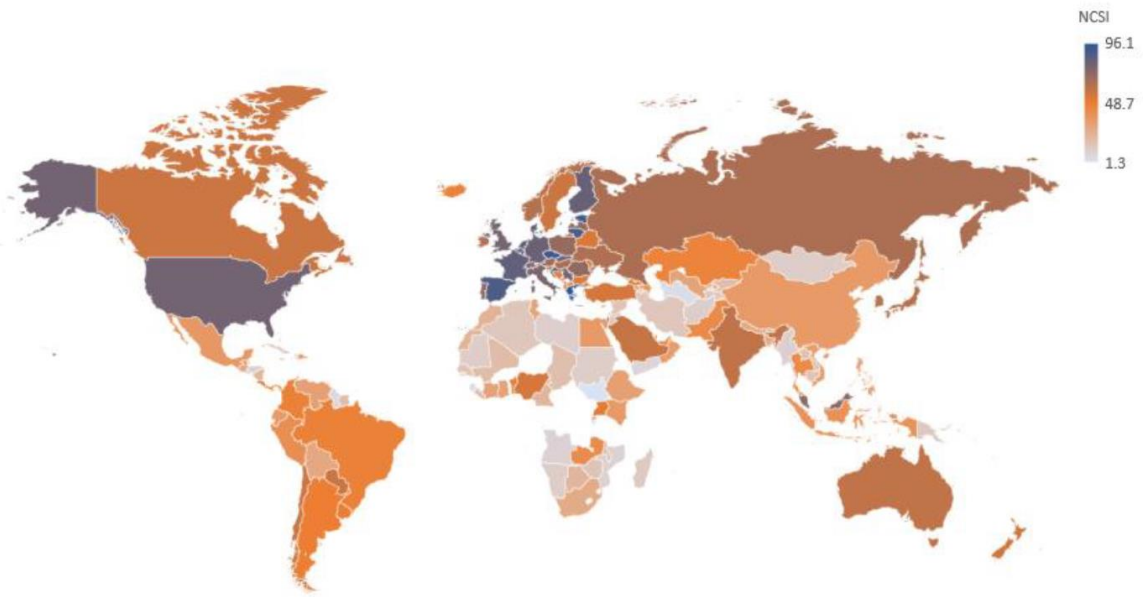

Рис. 2.3. Карта рейтингування країн за Національним індексом кібербезпеки за 2021 рік

Якщо порівнювати країни, що розвиваються, наприклад, Україна, яка має індекс, рівний 64, та розвинуту країну Австралію з індексом 60, то можна дійти висновку, що рівень протидії кіберзагрозам в Україні вищий. Також цей показник у України є вищим у порівнянні з такими розвинутими країнами, як Канада (57), Швеція (57), Норвегія (62), Японія (62). Це характерно й для Малайзії, Росії, Індії та ряду інших країн, що розвиваються, тобто за рівнем національного індексу кібербезпеки вони випереджають ряд розвинутих країн. Можна виділити й Нігерію, показник якої дорівнює 55, тобто за рівнем кібербезпеки дана країна наздоганяє Канаду та Швецію. Що стосується країн, які є найменш розвинутими, то вони мають доволі низькі значення NCSI.

Якщо ви порівняєте рейтинги країн у Глобальному та Національному індексі кібербезпеки, то виявите, що згідно з GCI більшість країн світу мають рейтинг вищий за середній, а згідно з NCSI – більшість середніх значень. Це означає, що хоча загальний стан національної системи кібербезпеки загалом відповідає рівню економічного розвитку країни, існують проблеми, пов'язані з можливістю подолання різного роду кіберзагроз. Цей аспект можна враховувати під час розроблення стратегії інформаційної безпеки країни.

Індекс розвитку інформаційних та комунікаційних технологій (ICT DI) характеризує рівень розвитку інформаційних технологій в країні. Його основними цілями є вимірювання: рівня та еволюції у часі ІКТ в країнах; ступеня прогресу у розвитку інформаційних та комунікаційних технологій (ІКТ); відмінностей між різними країнами з точки зору їх розвитку ІКТ; потенціалу подальшого розвитку ІКТ [34]. Він розраховується, як інтегральний показник на основі 11 показників, які згруповані в свою чергу за трьома субіндексами: доступ, використання та навички. Використовуючи емпіричні значення ICT DI за 2021 рік для 159 країн світу, побудуємо карту для їх візуального аналізу та оцінки (рис. 2.4).

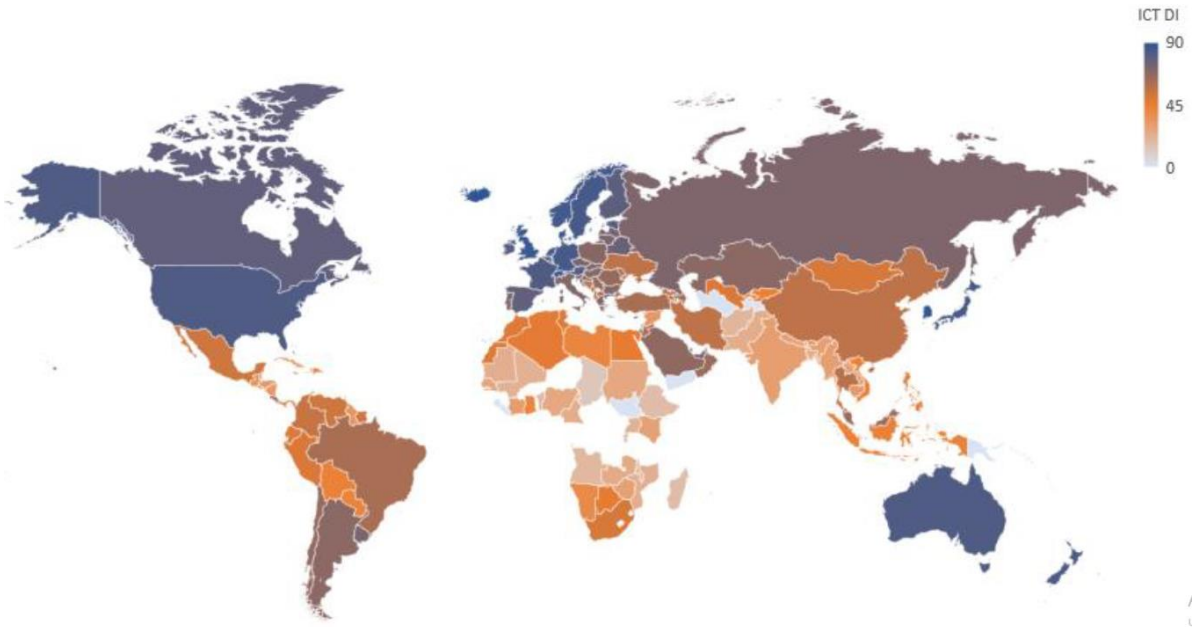

Рис. 2.4. Карта рейтингування країн за Індексом розвитку інформаційних та комунікаційних технологій за 2021 рік

Україна посідає 75-те місце зі значенням показника 56, на рівні Китаю та Ірану, що відповідає середньому рівню розвитку інформаційних і комунікаційних технологій. При зміні лідерів та аутсайдерів порівняно з рейтингами NCSI та GCI зберігається тенденція відповідності рівня економічного розвитку країни відповідному індексу технологічного розвитку.

Індекс мережевої готовності (далі NRI) вимірює ступінь технологічної готовності країни до застосування новітніх інформаційних і комунікаційних технологій у різних галузях. Його використання дає змогу комплексно оцінити багатофакторний вплив ІКТ на розвиток суспільства та окремих країн. Його розрахунок відбувається за чотирма напрямами - технології, люди, управління та вплив, які розбиті на 12 піднапрямків, яким відповідають 62 показники. Використовуючи його фактичні значення за 2021 рік, побудуємо карту для візуального аналізу та оцінки (рис. 2.5).

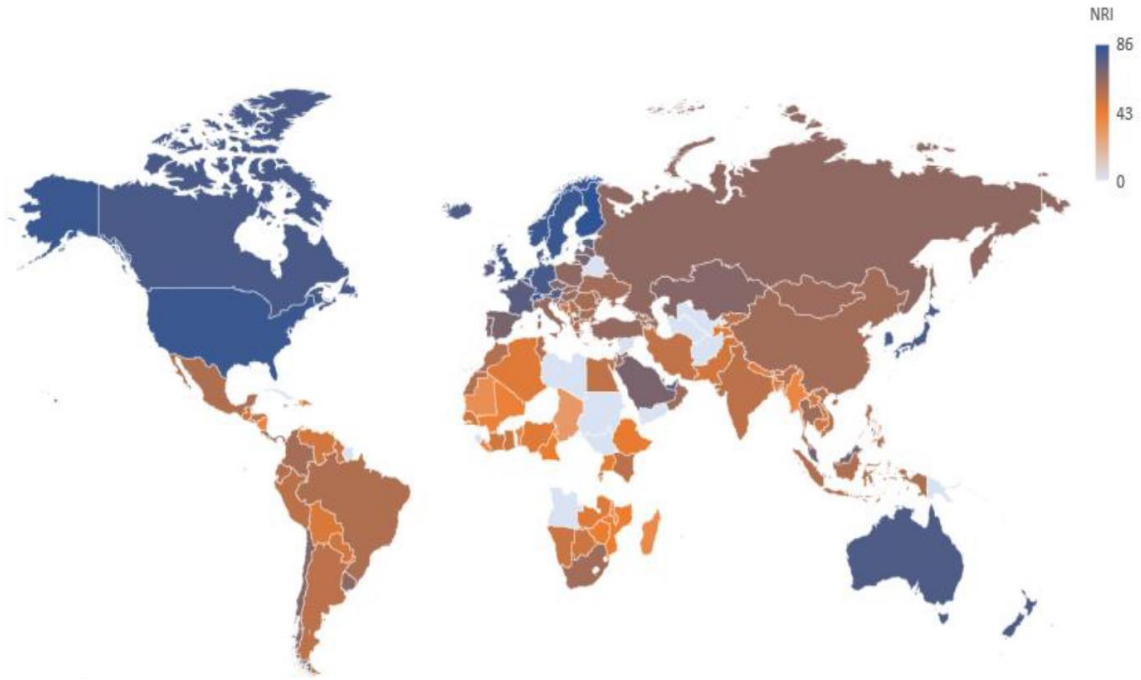

Рис. 2.5. Карта рейтингування країн за індексом мережевої готовності за 2021 р.

Аналізуючи дані NRI, можна побачити, що високій рівень технологічної готовності характерний для наступних країн: Фінляндія (86), Сінгапур (86), Нідерланди (83), Норвегія (83), Швеція (83), Швейцарія (83), США (83), Люксембург (81), Велика Британія (81), Канада (80), Данія (80), Німеччина (80), Японія (80), Південна Корея (80) та інші. Країни із низьким ступенем – це: Чад, Бурунді, Мавританія, Гаїті, Мадагаскар, М’янма, Малаві, Нікарагуа, Ліберія, Танзанія, Малі, Бенін та інші. Україна знаходиться на 61-му місці із

значенням показника 60, на рівні із такими країнами, як Китай, Йорданія, Тайланд, Південна Африка, що відповідає вище середнього рівня технологічної готовності. Не дивлячись на зміни рейтингів країн, можна зробити висновок, що є зв'язок між рівнем розвитку економіки країни та значенням її NRI.

Рівень цифрового розвитку (DDL) характеризує рівень цифровізації країни та визначається, як середній відсоток, який країна отримала від максимального значення Індексу розвитку ІКТ та Індексу мережевої готовності. Порівняння країн за DDL та NCSI дозволяє визначити, наскільки ступінь цифровізації країни відповідає рівню її кібербезпеки, що сприяє формуванню рекомендацій щодо коректування програми кібербезпеки. Використовуючи фактичні значення DDL за 2021 рік, побудуємо карту для візуального аналізу та оцінки (рис. 2.6).

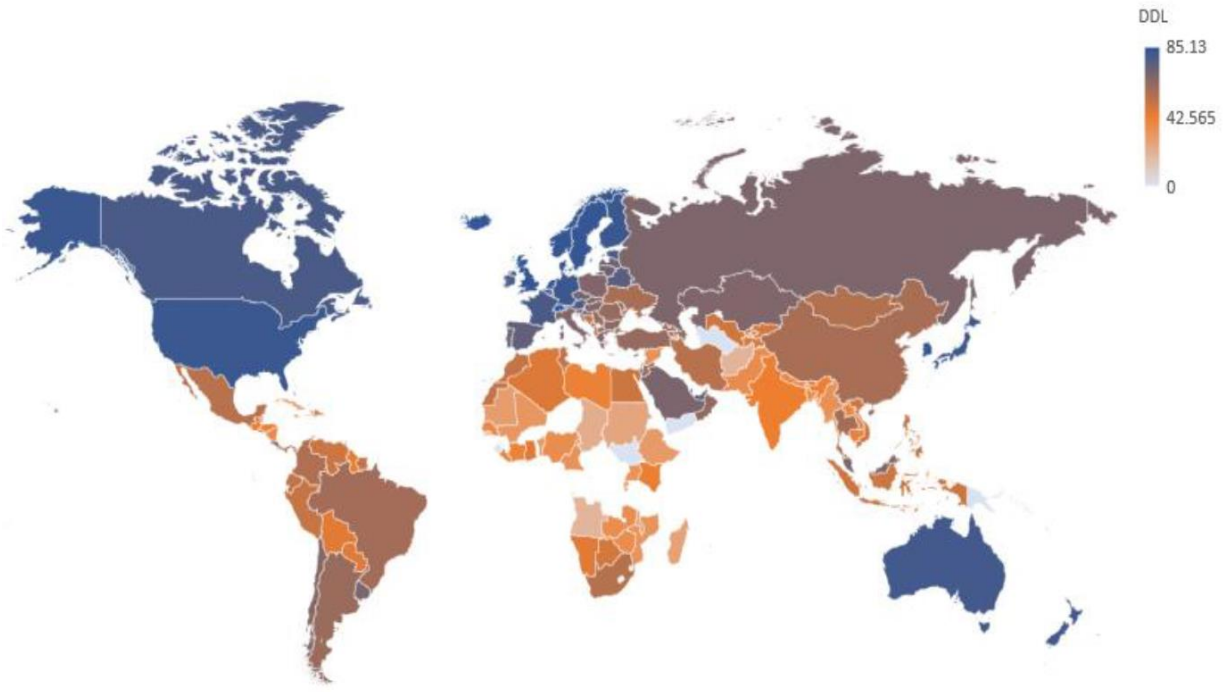

Рис. 2.6. Карта рейтингування країн за рівнем цифрового розвитку за 2021 р.

Значимість проаналізованих п'яти індикаторів для України показує, що в цьому питанні вона зробила потужні кроки на державному рівні. Це може

свідчити про наявність у країни потенційних можливостей для розвитку різних складових її інформаційної безпеки, що виступатиме стимулювальним драйвером національної економіки та національної безпеки загалом.

Методичні підходи до оцінки стану економічної безпеки держави в унормованому вигляді зафіксовано у Методичних рекомендаціях щодо розрахунку рівня економічної безпеки України, затверджених Наказом Міністерства економічного розвитку і торгівлі України від 29.10.2013 №1277, згідно з якими до переліку індикаторів за складовими економічної безпеки держави відносять 8 індикаторів, які ілюструють стан розвитку інформаційно-комунікаційної інфраструктури та можуть ілюструвати стан економічної безпеки держави у сфері комунікаційної діяльності (табл. 2.2.).

Таблиця 2.2

Перелік індикаторів, що ілюструють стан економічної безпеки держави у сфері комунікаційної діяльності

Найменування індикатора, одиниця виміру	Порядок розрахунку індикатора
1	2
1. Частка високотехнологічної продукції в загальному обсязі реалізованої промислової продукції, %	обсяг реалізованої промислової продукції, робіт, послуг у відпускних цінах підприємства, у % до всієї реалізованої продукції: виробництво основних фармацевтичних препаратів + виробництво комп'ютерів, електронної та оптичної продукції + виробництво електророзподільної та контрольної апаратури + виробництво інших транспортних засобів
2. Питома вага обсягу виконаних наукових і науково-технічних робіт у ВВП, %	-
3. Відношення витрат на наукові та науково-технічні роботи за рахунок держбюджету, % ВВП	-
4. Чисельність спеціалістів, які виконують науково-технічні роботи, до чисельності зайнятого населення (на 1 тис. осіб)	чисельність спеціалістів, які виконують науково-технічні роботи, тис. осіб / чисельність зайнятого населення у віці 15-70 р., млн. осіб
5. Питома вага підприємств, що впроваджували інновації, у загальній кількості промислових підприємств, %	-
6. Питома вага реалізованої інноваційної продукції в обсязі промисловості, %	-

Продовження табл. 2.2

1	2
7. Відношення експорту роялті, ліцензійних послуг, комп'ютерних та інформаційних послуг, наукових та конструкторських розробок, послуг в архітектурних, інженерних та інших технічних галузях, 5 до ВВП	комп'ютерні та інформаційні послуги + роялті та ліцензійні послуги + наукові та конструкторські розробки + послуги в архітектурних, інженерних та інших технічних галузях, (млн. дол. США / середній курс грн. до дол. США) / ВВП, млн. грн. *100
8. Частка осіб, які повідомили, що за останні 12 місяців користувалися послугами Інтернету (обстеження домогосподарств), %	-

Проте для врахування результатів глобальної інформаційної економіки та світового інформаційного ринку необхідно враховувати також показники, включені у світові рейтинги та які вимірюють інформаційну безпеку, є показниками цифрової спроможності та кібербезпеки країн.

Висновки до розділу 2

Для того, щоб оцінити рівень економічної безпеки України у сфері інформаційно-комунікаційної діяльності з урахуванням впливів результатів інформаційної економіки та світового інформаційного ринку доцільно використовувати різноманітні статистичні дані, що розраховуються консалтинговими, аудиторськими фірмами та іншими організаціями, що спеціалізуються на дослідженнях даного ринку та світової економіки.

Потенціал України у сфері кібербезпеки відмічається не лише світовими рейтингами, але й міжнародними організаціями. Зокрема, на початку квітня 2022 року Україна прийнята до складу Об’єднаного центру передових технологій з кібероборони НАТО як учасник-контрибутора.

Враховуючи досягнення України в кіберпросторі, правомірно визначити її рівноправним учасником на міжнародній арені у сфері кібербезпеки. Перспективними завданнями мають стати подальше удосконалення систем інформаційного захисту об’єктів критичної інфраструктури на основі

передових світових практик, а також узгодженість дій з міжнародними організаціями щодо протидії загрозам, пов’язаним з розвитком цифрової економіки та інформаційного суспільства. Побудова ефективної системи кібербезпеки в аспекті комплексної протидії кіберзагрозам сприятиме формуванню превентивного механізму протидії загрозам та їх стримуванні, випереджальному реагуванню на динамічні зміни, що відбуваються у кіберпросторі.

Наведені моделі процесів управління ризиками інформаційної безпеки дають можливість зручно, швидко та точно отримати цілісну картину ситуації відносно ризиків та загроз інформаційній безпеці, приймати оптимальні управлінські рішення стосовно обробки ризиків. Представлені моделі у сукупності відтворюють процес управління ризиками інформаційної безпеки, наведений у міжнародному стандарті ISO/IEC 27005:2011.

Запропоновані моделі дозволять отримувати науково-обґрунтовані організаційно-технічні рішення, впровадження яких сприятиме: підвищенню рівня інформаційної безпеки будь-якого суб'єкта господарювання та захисту його активів від множини зовнішніх та внутрішніх загроз, своєчасному виявленню вразливостей, зменшенню потенційних наслідків від реалізації загроз та зниженню ймовірності їх виникнення у майбутньому, мінімізації збитків, усуненню інцидентів та неприйнятних ризиків. У подальшому повинні звести до мінімуму розміри збитків від подій, що несуть загрози безпеці, шляхом їх нейтралізації.

РОЗДІЛ 3
ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВИКЛИКІВ ТА ЗАГРОЗ

3.1. Військова агресія як найбільша загроза інформаційній безпеці України

У XXI столітті інформація набула цінності не тільки з позиції державної таємниці, а й щодо комерційної таємниці, конфіденційної інформації, персональних даних. Дедалі збільшується кількість способів маніпуляції за допомогою інформації. Одночасно бурхливий розвиток інформатизації, разом із усіма перевагами, створив нові проблеми та загрози у сфері національної безпеки.

Особливо значного поширення набув інформаційний тероризм, оскільки в умовах глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби національних інтересів будь-яких держав стає інформаційний простір. Осмислення феномену інформаційного тероризму є передумовою формування більш чітких уявлень про запобігання загроз, здатних зруйнувати державні інститути, основи національної безпеки держави загалом.

В останні роки можна спостерігати значне підвищення уваги до питання протидії інформаційному тероризму, водночас багато питань залишаються невивченими. Значною мірою це викликано розв’язаною проти України «гібридною війною», однією із ключових складових якої була інформаційна сфера [33]. Таким чином, військове вторгнення супроводжувалося і нині супроводжується війною на інформаційному полі: інформаційний тероризм, масштабні кібератаки – це ті деструктивні феномени, які заполонили сучасний світ. Вони завдають шкоди не менше ніж прямі воєнні дії. Потреба підтримки національної економіки під час зовнішньої агресії передбачає необхідність забезпечення функціонування бізнесу на засадах інформаційної захищеності.

Сутність феномену інформаційного тероризму досліджується в працях вітчизняних та зарубіжних науковців. Перш за все, зупинимося на дослідженні такого поняття як «тероризм». Перші історичні згадки про появу цього терміну з'явилися у 1798 році, коли філософ Іммануїл Кант використав його для висвітлення песимістичного погляду на долю людства [34].

У теперішній час серед науковців не існує єдиного трактування поняття «тероризм». У. Лаккер звернув свою увагу на випадковості, ірраціональності та недоступності розуміння тероризму. Він зауважив, що: «Не повинно бути ілюзій стосовно того, що можна дізнатися про походження та характер тероризму. Встановленню піддається лише той факт, що при одних, обставинах терор частіше здійснюється, ніж при інших, і що при деяких обставинах він взагалі не може мати коріння. Перевантажений значенням за своєю природою поняття не піддається всім зусиллям виробити всеохоплююче і об'єктивне визначення тероризму. Такого визначення не існує і не буде знайдено в найближчому майбутньому» [35]. Однак, тероризм, може отримати своє визначення, так як основним питанням в даному випадку стає з'ясування того, наскільки послідовно і точно поняття використовується до певних явища, та що визначається основним критерієм для визначення сутності поняття.

На сьогодні, існує багато пояснень, або ж визначень тероризму. Розглядаючи це поняття в загальному значені, тероризм – це метод впливу шляхом здійснення теракту для досягнення поставлених цілей, через який постраждалі від теракту не є об'єктом. Зараз цей феномен став настільки поширеним, що стає всесвітнім явищем і його масштаби перетворюються на багатоаспектне явище, яке останнім часом дуже швидко еволюціонує, і як наслідок набуває міжнародного характеру. Міжнародний тероризм – це здійснення у світовому чи регіональному масштабі дії терористичними організаціями, угрупованнями, а також за підтримки державних органів окремих держав, з метою досягнення певних цілей, які є суспільно небезпечними насильницькими діяннями, що пов'язані з викраденням,

захопленням, вбивством ні в чому не винного населення, чи загрозою їх життю і здоров'ю, руйнуванням чи загрозою знищення важливих народногосподарських об'єктів, систем життєзабезпечення, комунікацій, застосуванням чи загрозою застосування ядерної, хімічної, біологічної та іншої зброї масового ураження [36].

Суть тероризму – насильство з цілю залякування. Суб'єкт терористичного насильства – окремі люди, чи неурядові організації. Об'єкт насилля – влада під маскою окремих урядових виконавців, або окремі представники від суспільства. Крім того, це може бути державна або приватна власність, інфраструктура, системи, які забезпечують нормальне життя населення. Ціль насилля – досягнення бажаного для терористів розвитку подій – революція, дестабілізація суспільства, початок війни з іншою державою, отримання незалежності певної території, падіння престижу влади, політичних змін зі сторони влади та інше.

Терористичну діяльність можуть проводити терористи в одній особі, терористичні угрупування і організації (в тому числі і міжнародні, які підтримуються зарубіжними державами). Тероризм здійснюється як підпільна, насильницька, цілеспрямована, керуюча, ідеологічна боротьба. Жертви тероризму можуть бути випадкові або обрані терористом. Терористичний акт виконує функцію залякування певних категорій людей або ж пропаганда ідей терористів.

Інформаційна епоха розширила сферу діяльності тероризму, що призвело до появи «інформаційного тероризму», основою якого є маніпуляція свідомістю мас, розповсюдження інформаційно-емоційного ефекту на який розраховано більшість терористичних актів, залучення прихильників серед членів суспільства, вплив на владні структури, які приймають політичні рішення [37].

Порівнюючи визначення понять «тероризм» та «інформаційний тероризм», складається враження, що інформаційний тероризм не є жахливим. Оскільки відсутні загиблі, поранені. Однак, якщо дослідити його сутність, то

сучасний інформаційний тероризм можна охарактеризувати як множину інформаційних війн та спецоперацій, пов'язаних із національними або транснаціональними кримінальними структурами та спецслужбами іноземних держав. Крім того, доступність інформаційних технологій значно підвищує ризики інформаційного тероризму, а розвиток інформаційної інфраструктури суспільства сприяє створенню додаткових ризиків інформаційного тероризму [38].

Інформаційний тероризм поділяють на:

– інформаційно-психологічний тероризм (контроль над ЗМІ для поширення дезінформації, чуток, демонстрації могутності терористичних організацій);

– інформаційно-технічний тероризм (завдання збитків окремим елементам і всьому інформаційному середовищу загалом: руйнування елементної бази, створення перешкод на лініях зв'язку, штучне перенавантаження вузлів комунікації та інше) [39].

Виокремимо основні складові тероризму: суб'єкт (або декілька суб'єктів); об'єкт (або об'єкти); мета здійснення; причина і мотив; часові та просторові характеристики; інструменти, які використовуються; наслідки.

Звичайно ж можна виділити підгрупи із перерахованих складових.

За критерієм інструментів (засобів), які використовуються, можна виокремити різноманітні типи тероризму. Складність використання цього критерію полягає в тому, що суб'єкти тероризму, як правило, поєднують кілька засобів – це може бути і захоплення стратегічно важливого об'єкту, в якому знаходяться люди, що стають заручниками, і транспортного засобу із одночасною зупинкою нормального функціонування транспортної системи та інше [40].

На даний момент найбільш ефективними і найдешевшими інструментами тероризму, які активно використовується є глобальне ЗМІ та Інтернет. У поєднанні вони формують інформаційне поле, де реальність подана у дещо викривленому вигляді, яка повертає настрої людей в дещо інше

русло, що дає можливість терористичній стороні схилити погляди населення на свою користь. Також терористи використовують засоби масової інформації для інформування суспільства про свою діяльність, залучення активних людей до своїх дії або психологічний вплив на людей. Важливим завданням для терористів є використання міжнародних засобів інформації для того, щоб поширювати власні ідеї або ж ідеологію. І такі випадки в історії прослідковуються не одноразово. Коли відомий британський телеканал «Channel 4» оприлюднив інтерв'ю в якому показав відомого міжнародного терориста Шаміля Басаєва, Російська Федерація відреагувала обуренням.

Медіа-тероризм або «медіа-кілерство» – це зловживання інформаційними системами, мережами та їхніми компонентами для здійснення терористичних дій та акцій [38].

Ще одним видом тероризму, який варто виокремити є кібертероризм. Його розглядають, як інформаційну атаку на електронну інформацію, обчислювальні системи, банківські системи, технічні засоби передачі даних та інші системи інформаційної інфраструктури. Здійснюється окремими особами або терористичними угрупуваннями.

Кібертероризм спрямований на те, щоб заволодіти контролем інформаційно-телекомунікаційними системами, тобто не проводити свої ідейні виступи, а системне проникнення, що дасть змогу контролювати інформаційні потоки, завдання шкоди мережам інформаційного обміну та інші деструктивні дії. Перевагою для терористичної сторони є те, що дії такого характеру не обмежені кордонами чи відстанню, тобто не існує національних меж. Також складно виявити об'єкт терористичних дій в інформаційному просторі, оскільки хакери проводять ці операції через підставні комп'ютери, чи певну мережу комп'ютерів, що значно ускладнює пошук чи ідентифікацію місцезнаходження злочинця. Особливо сьогодні, коли технологічне вдосконалення розвивається швидкими темпами, стало важко створити надійну систему безпеки, яка захищатиме від кібертерористів.

Так, якщо на початку 2020 року кількість кібератак у світі складала близько 5 тисяч за тиждень, то на початку 2021 року їхня кількість зросла до 200 тисяч [1]. 19% усіх кібератак, зафіксованих у 2021 році, було скоєно проти України (на першому місці США – 46%). Для порівняння, частка Бельгії, Німеччини та Японії не перевищує 3% (рис. 3.1) [2].

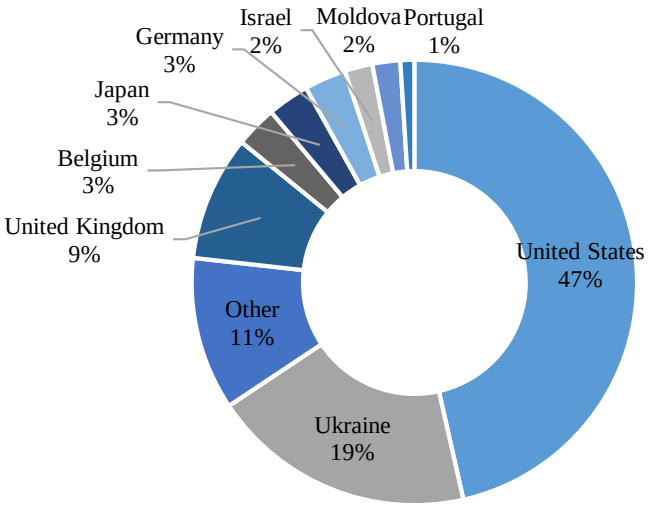

Рис. 1. Рейтинг країн за кількістю кібератак за 2021 рік

Згідно з офіційними даними, Україна посідає друге місце у світових рейтингах за кількістю кібератак, які спрямовані на об’єкти критичної інфраструктури країни, тобто такі галузі як енергетична, фінансова, телекомунікаційна тощо, та державні електронні інформаційні ресурси, порушення функціонування яких є загрозою національним інтересам [3]. З початку 2022 року інтенсивність кібератак зросла: лише у січні було виявлено вже 6,8 млн підозрілих подій інформаційної безпеки, 25,5 тис. потенційних кіберінцидентів та зупинено 121 кібератаку. Для порівняння у квітні 2021 року фахівцями Служби безпеки України було виявлено 1,5 млн підозрілих подій та припинено 53 критичні кіберінциденти [4]. За січень-лютий 2022 року на об’єкти критичної інфраструктури та державні інформаційні ресурси України було здійснено 436 кібератак у порівнянні з 64 за такий же період 2021 року. Наймасштабніші з них представлено на рисунку 2. У березні-травні 2022 року

кібератаки на енергетичну сферу, логістичну інфраструктуру, сайти українських онлайн-медіа та офіційні державні ресурси продовжувалися.

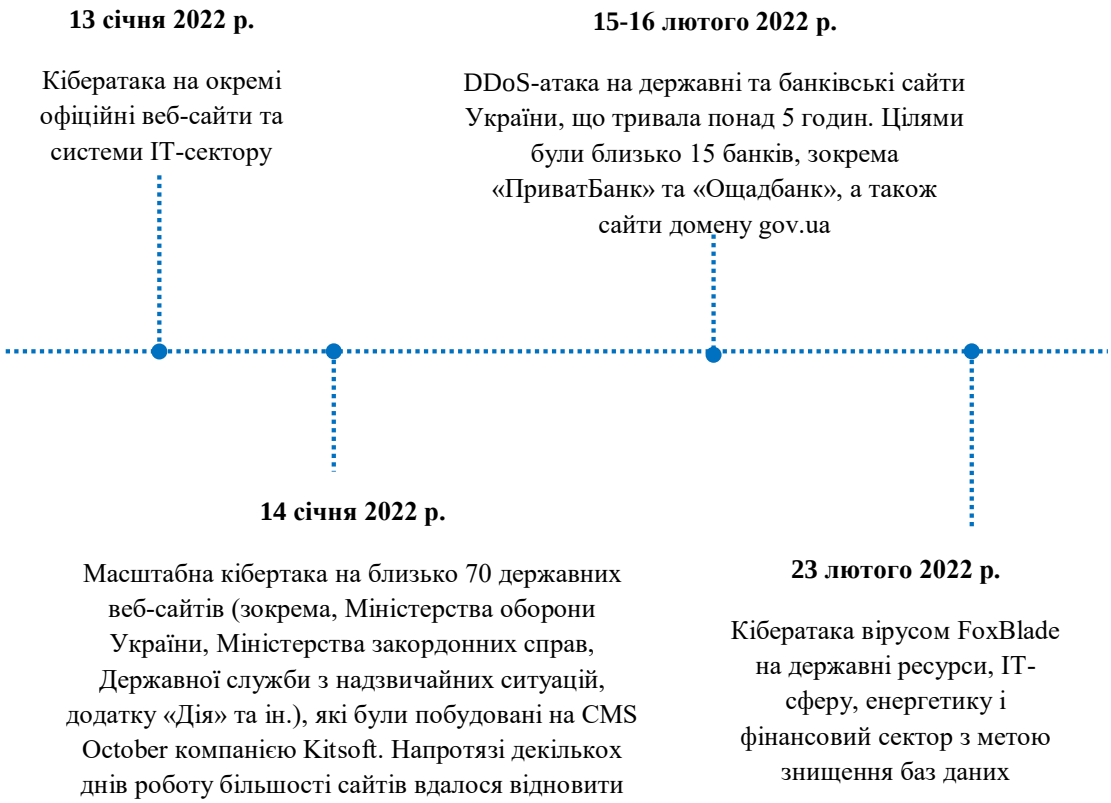

Рис. 3.2. Кібератаки на об’єкти критичної інфраструктури та державні інформаційні ресурси України у січні-лютому 2022 року

Основними видами кібератак, які становлять найбільшу загрозу інформаційній безпеці національній економіці визначено програми-вимагачі, інсайдерські атаки, фішинг, цільові кібератаки та DDoS-атаки. Їх деструктивний вплив спричиняє, в першу чергу, значні фінансові втрати. Так, за даними американської компанії McAfee, яка спеціалізується на комп’ютерній безпеці, та Центру стратегічних і міжнародних досліджень (CSIS) у 2020 р. втрати світової економіки у результаті кібератак склали понад 1 трлн дол США, що становило 1% світового ВВП. У порівнянні із 2018 р., даний показник зріс на понад 50%. У 2021 році збитки від кібератак зросли до

4,2-6 трлн. дол. США (рис. 3.3). Прогнозується, що у 2025 році обсяг фінансових втрат від кіберзлочинності сягне 10,5 трлн. дол. США.

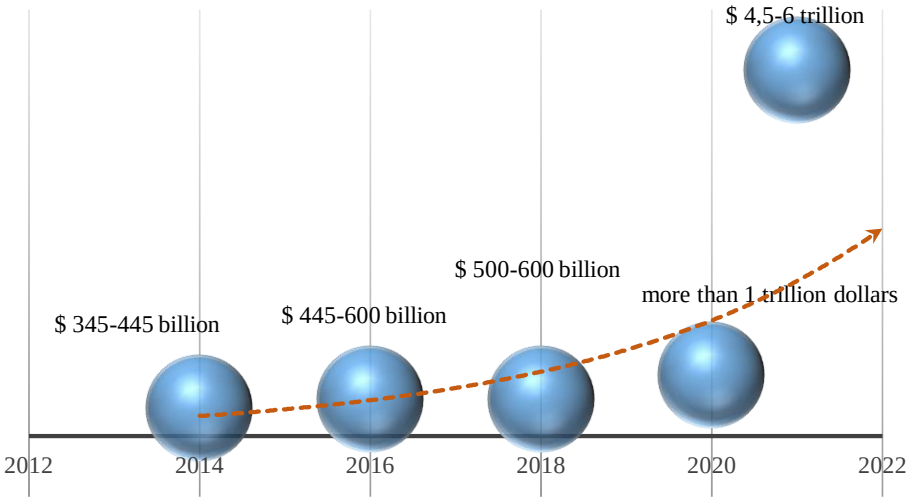

Рис. 3.3. Світові фінансові втрати від кібератак у 2014–2021 роках

Слід відмітити, що у 2021 році зафіксовано найвищу середню вартість витоку даних за останні 17 років – 4,24 млн дол. Аналогічний показник за 2020 рік становив 3,86 млн дол. [9]. Найбільш поширеною причиною витоку даних були фішинг-атаки. Крім прямих фінансових збитків кібератаки спричиняють втрати робочого часу, а також іміджеві втрати компаній [10]. Є й інші приховані втрати від кіберзлочинності – зокрема, зниження рівня задоволеності працівників роботою.

Враховуючи зростання негативних фінансових наслідків від реалізації кіберзагроз, необхідність підвищення рівня інформаційної безпеки в умовах розвитку цифрової інфраструктури є безумовною.

Тому кожній державі необхідно провести ряд заходів для протидії інформаційному тероризму. Варто зауважити, що значну роль в цьому відіграє правова база, яка слугує основою для запобігання терористичних актів. Ефективною складовою стає наявність у відповідних структурах будь-якої держави, наприклад в Україні – це СБУ та МВС, спільної бази даних про терористів та осіб, які можуть бути причетними до цього. Це буде ефективним

засобом для протидії та профілактики терористичних дій. Для попередження кібертерористичних дій слід виокремити основні напрями такої боротьби:

– уніфікація та гармонізація національного законодавства та міжнародних актів;

– проведення наукових розробок в сфері створення сучасних технологій виявлення та запобігання кримінальним і терористичним впливам на інформаційні ресурси;

– створення спеціалізованих підрозділів у сфері боротьби з комп'ютерними злочинами та комп'ютерним тероризмом;

– удосконалення міжнародної організаційно-правової взаємодії з питань протидії комп'ютерній злочинності та комп'ютерному тероризму;

– удосконалення багаторівневої системи підготовки кадрів у сфері інформаційної безпеки [39].

Стає зрозуміло, що запобігання терористичних дій, особливо боротьба з кібертероризмом, повинні здійснюватись комплексним підходом, поєднуючи силові, політико-дипломатичні, економічні та гуманітарні методи протидії.

Отже, розглядаючи інформаційний тероризм як сучасне явище, можна сказати, що він становить значну загрозу суспільству, населенню та міжнародній безпеці. Технологічний прогрес надає більше можливостей терористам здійснювати вплив на людей, на їх свідомість, до- зволяє їм притягувати до себе увагу, поширювати свою ідеологію навіть на великі відстані, тобто не обмежуючи себе територіально. Сьогодні вже усі технічні засоби обробки та зберігання інформації стали легко вразливі силам терористів.

Варто розуміти те, що проблема протидії інформаційного тероризму – це комплексна проблема. Закони держав повинні беззаперечно відповідати технологічній революції і бути готовими захищати їхні інтереси в будь-якому інформаційному полі. Тому уряди держав повинні здійснювати заходи необхідні для гармонізації та вдосконалення законодавства заради їхньої інформаційної безпеки.

Наразі можна виокремити наступні завдання, які в комплексному застосуванні допоможуть створити суттєвий інформаційний захист для держави.

1. Постійний моніторинг інформаційного середовища на випадок потенційної кібертерористичної загрози.
2. Захист елементів вітчизняної інфраструктури.
3. Створення та оновлення програмного забезпечення, яке зможе захистити інформаційне середовище держави.
4. Усунення прогалин в законодавстві держави.
5. Зауваження населення про кіберзлочини, оскільки 80% атак залишаються невисвітленими для правоохоронних органів.
6. Боротьба з не ліцензованим програмним забезпеченням.
7. Створення системи, яка забезпечить загальнодержавний захист інформації [41].

Беззаперечно найкращим методом боротьби з інформаційним тероризмом є підтримка новітніх інформаційних технологій та стимули для науково-технічного прогресу всередині держави, що допоможе запобігти кібертероризму. А спонсорування даних заходів має на себе взяти держава, яка зможе коректно спрямувати усі напрацювання науково-технічного процесу.

3.2. Державна політика формування інформаційної безпеки в умовах викликів та загроз

Стан нормативно-правового забезпечення інформаційної безпеки держави визначається ступенем регулювання національним законодавством, нормами міжнародного права, міжнародними договорами України суспільних відносин у сфері її національним інтересам в інформаційній сфері.

Сучасний стан нормативно-правового забезпечення інформаційної безпеки в Україні характеризується фрагментарністю вибору суб'єктів правового регулювання, недостатньою узгодженістю правових норм, що

використовуються для цього, та покоординованістю діяльності суб'єктів законодавчої ініціативи з розвитку та вдосконалення правових норм, тому у ряді випадків не в змозі адекватно вирішувати проблеми, що виникають.

Більшість чинних законів і підзаконних актів, спрямованих на регулювання інформаційних відносин, було ухвалено до набрання чинності Конституцією, і навіть з істотними змінами та доповненнями не відповідають потребам сучасності. Здебільшого або дають терміни, або декларують окремі положення без вказівки, як їх реалізувати, або є «посилання на положення», або посилання на такі норми окремих законів, які до сфери інформаційних відносин неможливо застосувати без врахування специфіки об'єкта.

Нормативно-правове регулювання інформаційної безпеки у сфері прав та свобод здійснюється Конституцією України, Стратегією інформаційної безпеки, Стратегією кібербезпеки України і такими базовими законами України: «Про інформацію», «Про науково-технічну інформацію», «Про Національну програму інформатизації», «Про Концепцію Національної програми інформатизації», Про поштовий зв'язок» та ін.

Вказані нормативно-правові акти регулюють питання забезпечення інформаційної безпеки, питання захисту інформації, охорони державної таємниці, забезпечення захисту конфіденційної інформації, інформаційних ресурсів, спрямовані на реалізацію положень Доктрини безпеки особистості, держави і суспільства та ін.

Аналіз чинної нормативної бази показує, що поняття «інформаційна безпека України» досить широко застосовується в Конституції України та низці інших нормативно-правових актів, підготовлених і затверджених Верховною Радою, Президентом України, Кабінетом Міністрів, центральними органами виконавчої влади.

Так, ст. 17 Конституції наголошує, що забезпечення інформаційної безпеки – «одна з найважливіших функцій держави, справа всього українського народу» [9], а Закон України «Про Концепцію Національної програми інформатизації» проголошує, що «інформаційна безпека є

невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки» [21].

У ст. 13 Закону України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» надається визначення поняття «інформаційна безпека» – це «… стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через:

– неповноту, невчасність та невірогідність інформації, що використовується;

– негативний інформаційний вплив;

– негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [22].

Разом з цим у Законі України «Про інформацію» визначення «інформаційна безпека» взагалі немає. А в Законі України «Про національну безпеку України», який є основним орієнтиром забезпечення безпеки нашої держави, сутність «інформаційної безпеки» подано як невід'ємний складник національної безпеки України без точного визначення цього поняття [23].

Як бачимо, у цитованих документах дано лише загальні визначення терміна «інформаційна безпека», до того ж вони не узгоджені одне з одним. Але ці документи не містять якихось системних підходів до забезпечення інформаційної безпеки в Україні, не визначають суб'єктів розвідувальної діяльності та не розподіляють між ними повноваження.

Також, 15 березня 2016 р. введено в дію Указ Президента України №96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України» [24].

Метою Стратегії є створення умов для безпечного функціонування кібепростору, його використання в інтересах особи, суспільства і держави.

Документ базується на положеннях Конвенції про кіберзлочинність, законодавства України щодо основ національної безпеки, засад внутрішньої та

зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом та спрямована на реалізацію до 2020 р. Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 р. №287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 р. «Про Стратегію національної безпеки України».

Стратегія передбачає комплекс заходів, пріоритетів і напрямів із забезпечення кібербезпеки України, зокрема створення та оперативну адаптацію державної політики, спрямованої на розвиток кіберпростору та забезпечення сумісності з відповідними стандартами ЄС і НАТО, створення конкурентного середовища у сфері електронних комунікацій. , надання послуг із захисту інформації та кіберзахисту. Передбачає залучення потенційної експертизи наукових установ, фахових та громадських об'єднань до підготовки проєктів концептуальних документів у даному напрямі; підвищення цифрової грамотності громадян і культури безпечної поведінки в кіберпросторі; розвиток міжнародного співробітництва та підтримка міжнародних ініціатив у сфері кібербезпеки, зокрема, поглиблення співробітництва України з ЄС і НАТО. Згідно з документом, основу національної системи кібербезпеки складуть Міністерство оборони, Державна служба спеціального зв'язку та захисту інформації України, СБУ, Національна поліція, НБУ та розвідувальні органи.

Останнім часом розроблено низку нових законопроектів стосовно інформаційної безпеки держави, а саме «Про засади інформаційної безпеки України», «Про кібернетичну безпеку України», «Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України». У цих законопроектах частково враховано зазначені недоліки вітчизняного законодавства.

Ухвалену Урядом у вересні 2021 року Стратегію інформаційної безпеки правомірно вважати концептуальною основою формування інформаційної безпеки в Україні. Стратегією визначені методологічні аспекти забезпечення

інформаційної безпеки України, упередження появи та мінімізації загроз національній безпеці в інформаційній сфері, захисту прав громадян на інформацію та захист персональних даних.

Таким чином, прийняття Стратегії інформаційної безпеки є свідченням усвідомлення необхідності забезпечення інформаційної безпеки України як основи захисту національних інтересів в умовах діджиталізації. Цей документ окреслив вектори державної регуляторної політики у зазначеній сфері та стане базисом для формування ґрунтовного інституційно-правового забезпечення інформаційної безпеки.

Слід зазначити, що події в інформаційному просторі України, викликані агресією з боку російської федерації, змусили керівництво держави до більш рішучих кроків у цей сфері. Проте Уряд має додатково опрацювати питання щодо створення національної захищеної операційної системи, антивірусного програмного забезпечення спеціальними програмно-апаратними комплексами для захисту державних інформаційних ресурсів та інформаційно-комунікаційних мереж; вжити заходів для забезпечення поширення у світі об'єктивної інформації про суспільно-політичну ситуацію в Україні, зокрема шляхом створення медіахолдингу для підготовки якісного конкурентоздатного інформаційного продукту.

Проте, на сьогоднішній день в державі не створено цілісної системи національної інформаційної безпеки. Вважаємо проблему створення такої системи ключовою у питанні забезпечення надійної інформаційної безпеки України. На наше глибоке переконання зазначена система має стати системоутворюючим чинником для більш ефективної реалізації державної інформаційної політики, надійної протидії деструктивному іноземному інформаційному впливу та інформаційним загрозам у цілому (рис. 3.4).

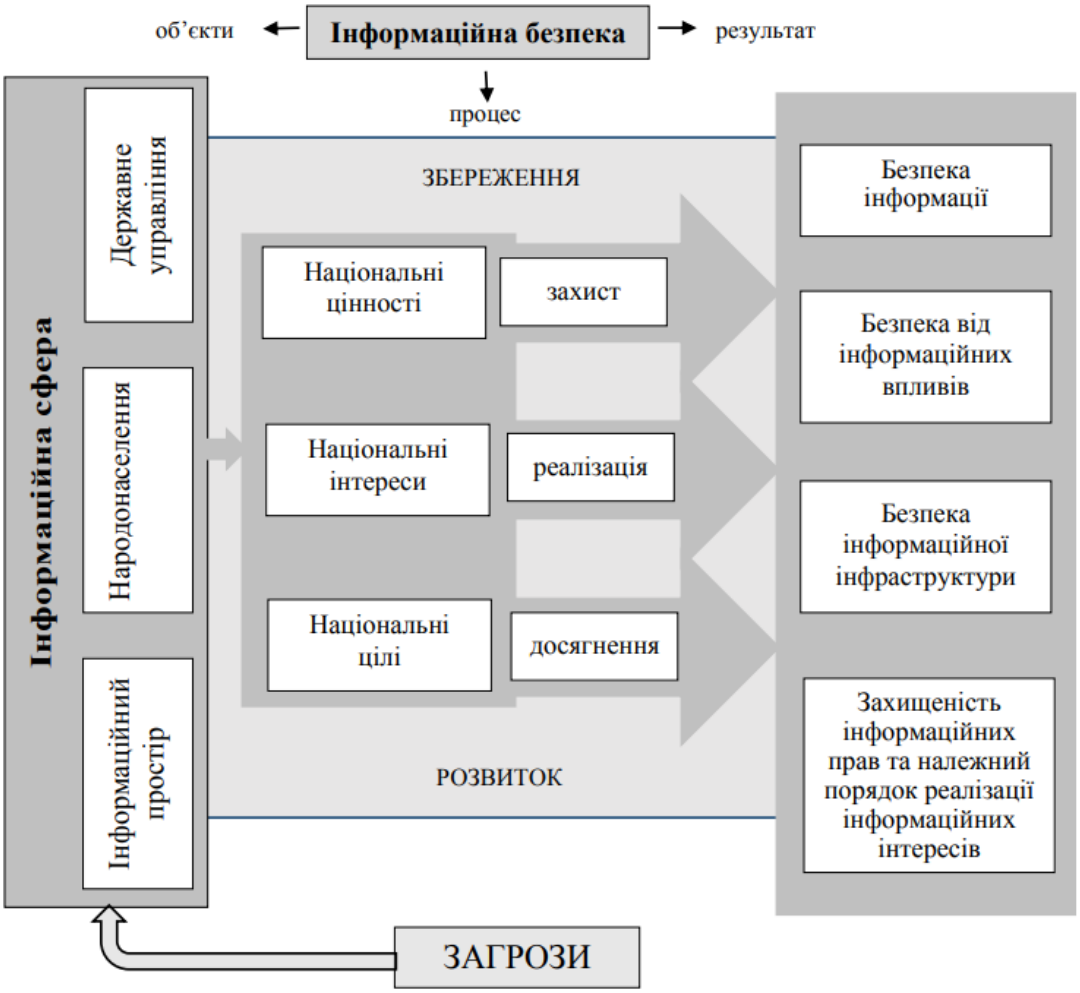

Рис. 3.4. Система інформаційної безпеки

Питання створення та функціонування системи інформаційної безпеки держави необхідно включати до проектів всіх ключових профільних документів і, в першу чергу, концептуальних.

Недостатність регулювання правової бази інформаційних правовідносин суттєво ускладнює появу якісних змін у цій сфері суспільних відносин. На сьогоднішній день через відсутність взаємозалежних і чітко опрацьованих заходів та теоретичних розробок щодо забезпечення безпеки державної інформації ми стикаємося з низкою перешкод на шляху повного виконання державою своїх зобов'язань із забезпечення інформаційної безпеки, що, своєю чергою, є невід'ємною частиною національної безпеки. Лише реалізація обґрунтованих доказів державної інформаційної політики може створити ефективну систему протидії правопорушенням у цій сфері.

3.3. Взаємовідносини держави та інститутів громадського суспільства з питань забезпечення інформаційної безпеки України

В сучасних умовах інформаційна безпека набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки. Водночас, інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку. Відповідно, рівень розвитку та безпеки інформаційного простору, який є системоутворюючим фактором у всіх сферах національної безпеки, суттєво впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України.

Унаслідок відсутності дієвої системи забезпечення інформаційної безпеки України спостерігається низка негативних явищ, які створюють реальні та потенційні загрози інформаційній безпеці людини і громадянина, суспільства і держави. Такі умови вимагають від органів державної влади пошуку нових методів протидії загрозам інформаційній безпеці, що з врахуванням сьогоднішніх реалій передбачає залучення інститутів громадянського суспільства, як повноправних суб'єктів забезпечення інформаційної безпеки. Тобто, перед державою постає завдання реалізації партисипаторної функції системи забезпечення інформаційної безпеки, що сприятиме соціалізації громадян України, з метою їх активної участі в процесах відстоювання національних інтересів у інформаційній сфері.

Перш ніж перейти до розгляду зазначеної проблематики, розглянемо сутність понять «громадянське суспільство» та «інститут громадянського суспільства». Дослідивши різні точки зору, які існують у науковому дискурсі [74–84] ми дійшли висновку, що в нашому дослідженні зміст поняття «громадянське суспільство» буде доречно розглядати як сукупність соціальних відносин та інститутів, що функціонують відносно незалежно від публічної влади та здатні чинити усвідомлений вплив на органи публічної влади у прийнятті ними тих чи інших політичних рішень, у розробці та

реалізації державної політики. При чому такий вплив може бути як позитивного, так і деструктивного характеру. Однак, як правило, та чи інша спрямованість подібного впливу виступає як відповідна реакція на впроваджуваний керівництвом країни політичний курс [85].

Як підструктура суспільної системи, громадянське суспільство має складну внутрішню структуру, до якої, як один із компонентів, входять його інститути. Так, відповідно до п.2 «Порядку сприяння проведенню громадської експертизи діяльності органів виконавчої влади» затвердженою Постановою Кабінету міністрів України №976 від 05.11.2008 р., до інститутів громадянського суспільства відносяться громадські організації, професійні та творчі спілки, організації роботодавців, благодійні і релігійні організації, органи самоорганізації населення, недержавні засоби масової інформації та інші непідприємницькі товариства і установи, легалізовані відповідно до законодавства [86].

Викладене вище є беззаперечним доказом того, що перелік та різноманіття інститутів громадянського суспільства є надзвичайно об'ємними. В такому випадку ми розглядатимемо лише один з різновидів таких інститутів, а саме: громадські (неурядові) організації, діяльність яких безпосередньо або ж потенційно може впливати на забезпечення інформаційної безпеки України.

У даному дослідженні неурядові організації визначаються як добровільні, приватні, некомерційні, організаційно оформлені об'єднання громадян, які репрезентують інтереси певних верств населення, реалізують суспільно корисні цілі у різних галузях, діють за статутом на основі принципів самоврядування і законності, а їхня діяльність ґрунтується на неурядових угодах. Тобто, держава не несе відповідальність за діяльність своїх громадян у таких організаціях. Досить часто неурядові міжнародні організації називають групами тиску, адже, мобілізуючи громадськість вони здійснюють тиск на суспільство [87].

В якості першопричин створення неурядових організацій щодо забезпечення безпеки абсолютно справедливо вказується на те, що «державні

органи, покликані забезпечувати безпеку в різних сферах, самі частково дезорганізовані і в сьогоднішній ситуації не здатні повністю впоратися з усім різноманіттям завдань, що постають перед ними в сфері забезпечення безпеки. Гостро відчуваючи свою незахищеність суспільство без підтримки з боку держави, самостійно намагається створити для себе належний рівень безпеки» [88].

В умовах нових викликів національній безпеці деякі державні діячі, маючи консервативні погляди, прагнуть обмежити, зростання активності недержавного сектора та повернути собі традиційне місце у вирішенні питань забезпечення безпеки в тому числі й інформаційної. Проте, як вважає Т. Карозерс, «добре налагоджена робота неурядових організацій зміцнює, а не послаблює потенціал держави» [89]. Тобто держава і неурядові організації разом можуть бути набагато ефективнішими у формуванні державної політики, якщо перша проводить узгоджену політику і підтримує інститути громадянського суспільства. А другі цілеспрямовано окреслюють існуючі проблеми, пропонують варіанти їх вирішення у взаємодії з населенням [90].

На нашу думку, підхід в рамках якого абсолютизується роль державних структур у формуванні системи забезпечення інформаційної безпеки має свої суттєві недоліки. По-перше, закритість політики забезпечення інформаційної безпеки призводить до виключення участі суспільства у її розробці та реалізації. Це призводить до деякого відчуження між державою та її громадянами. яке може виражатися, як мінімум, в неусвідомленні останніми цілей державної політики забезпечення інформаційної безпеки, а значить в соціальній пасивності, і, як максимум, в неприйнятті та протидії такій політиці. По-друге, відсутність громадянського контролю та громадських обговорень з питань реалізації політики забезпечення інформаційної безпеки призведе до поступового падіння ефективності її реалізації. По-третє, можливий непомітний перехід від цілей забезпечення інформаційної безпеки людини (громадянина) і суспільства до цілей забезпечення безпеки лише самої держави.

Основну проблематику взаємодії держави та неурядових організацій у сфері забезпечення інформаційної безпеки можна умовно звести до кількох напрямків. Деякі з дослідників [91, 92] розвивають свої концепції з позиції підходів А. де Токвілля [93] та Р. Патнема [94]. У своїх роботах вони виходять з того, що основою неурядової організації, як і будь-якого інституту громадянського суспільства є людина, яка, реалізує свої інтереси, потреби, людський потенціал за допомогою таких об'єднань. Тому неурядові організації і мають можливість впливати на становлення і поширення демократичних норм і стилів поведінки в державі щодо участі громадськості в розробці та реалізації інформаційної безпеки [95].

Інші дослідники дотримуються позиції, що вплив неурядових організацій на інформаційну безпеку може бути як позитивним, так і негативним. Т. Карозерс [96], Д. Фернандо, А. Хестон [97] вважають, що неурядові організації не є виключно позитивним інститутом, вони можуть здійснювати негативний вплив через деструктивні політичні угруповання, які прагнуть реалізувати свої інтереси і потреби будь-якими доступними методами.

Л. Ніковська з цього приводу зазначає, що неурядові організації є структурами, які функціонально виникли в соціумі як інститут зворотного зв'язку для взаємодії з державою, як інститут оптимізації соціальних процесів і контролю за ними. Але взаємодія держави і неурядових організацій «постійно генерує і відтворює протиріччя, пов'язане з плюралізмом соціальної сфери та суверенністю державної влади» [98]. Таке протиріччя може виражатися в різних формах: від співпраці і переговорів до відкритих конфліктів і «актів громадянської непокори» [99].

Проте, саме неурядові організації є ефективним інструментом у системі «стримувань і противаг». Як пише А. Сунгуров, аналізуючи моделі взаємовідносин «держава-громадянське суспільство», найбільш ефективною схемою в умовах демократичної політичної системи є «партнерство». «Важливим критерієм для існування подібної моделі є розуміння

відповідальними представниками органів державної влади важливості самого феномена громадського контролю» [100].

У цьому аспекті досить цікавим є досвід США, які в сфері будівництва демократії і формування громадянського суспільства мають тривалу історію. У Стратегії національної безпеки Б. Обами досить докладно описано участь громадян у діяльності щодо забезпечення інформаційної безпеки. Їм передано частину повноважень на локальному та регіональному рівнях. Громади і неурядові організації вважаються не тільки органами, що забезпечують інформаційну безпеку, але й органами, що формують нову політику інформаційної безпеки. Громадяни, неурядовий і некомерційний сектор в США є повноправними суб'єктами політики, вони приймають участь в розробці політичних стратегій через «фабрики думки», дослідницькі інститути і т. д.

Стратегія Б. Обами пропонує запровадити «прозору структуру» системи інформаційної безпеки для забезпечення дієвого контролю над федеральним бюджетом США та діяльністю посадових осіб. Такі нововведення зорієнтовані на технології взаємодії держави і неурядових організацій як найбільш ефективного суб'єкта забезпечення інформаційної безпеки [101].

Повертаючись до питання громадської участі в сфері забезпечення інформаційної безпеки обов'язково необхідно зазначити про рівень (ступінь) впливу неурядових організацій на прийняття політичних рішень. Для цього, на приклад, можна використати класифікацію Ш. Арнштайн, що виокремлює 8 рівнів громадської участі (табл. 3.9) [102].

Перші два рівні характеризуються підміною реальної громадської участі, її імітацією владою (підміною мети, відсутністю альтернативних варіантів рішень, відсутністю «зворотного зв'язку», маніпулятивними підходами тощо).

Імітація взаємодії з громадськістю на рівні маніпуляції і «терапії» часто породжує конфлікти і не задовольняє потреби громади.

Таблиця 3.9

Класифікація рівнів впливу неурядових організацій на прийняття управлінських рішень

Рівні громадської участі	Рівень участі (впливовості)
1. Маніпулювання	Відсутність участі (впливовості)
2. «Терапія»	Відсутність участі (впливовості)
3. інформування	Обмежена участь (впливовість)
4. Консультація	Обмежена участь (впливовість)
5. Врахування думки	Обмежена участь (впливовість)
6. Партнерство	Реальна (дієва) участь (впливовість)
7. Делегування повноважень	Реальна (дієва) участь (впливовість)
8. Громадське керування	Реальна (дієва) участь (впливовість)

Зрозуміло, що рівень впливовості громадськості у цьому випадку є практично нульовим.

Третій і четвертий рівні − рівні обмеженої участі громадськості, які характеризуються можливістю громадян отримувати інформацію та висловлювати свої думки без гарантії, що їх думки вплинуть на суб'єкта ухвалення управлінських рішень. Рівень впливовості громадськості в цьому разі є обмеженим.

Деяке (обмежене, часткове) врахування думки громадськості передбачає п'ятий рівень.

Шостий, сьомий і восьмий рівні характеризують реальну участь громадян у процесі планування в ухваленні рішень. Тут може бути громадська участь в широкому діапазоні взаємодії: від партнерської участі в переговорному процесі з метою досягнення компромісу з владою − до ухвалення важливих управлінських рішень через референдум. Це є найвищий рівень впливовості громадськості, рівень суттєвого впливу на прийняття політичних рішень.

Безсумнівно, що участь громадськості у виконанні таких важливих завдань, як забезпечення інформаційної безпеки має не тільки практичну значимість, а й ідеологічне підґрунтя, оскільки дозволяє виробити «імунітет» в суспільстві до негативних інформаційно-психологічних впливів та

сформувати негативне сприйняття подібних дій у свідомості пересічних громадян. Саме тому серед розмаїття форм участі неурядових організацій у формуванні та впровадженні заходів із забезпечення інформаційної безпеки в сучасних умовах одне з провідних місць займає формування громадської думки. Стосовно важливості такої форми участі для неурядових організацій, як суб'єктів забезпечення інформаційної безпеки, професор В. Полторак доводить, що громадська думка реалізує в процесі життєдіяльності суспільства цілу низку найважливіших функції, ключовими серед яких є управлінська, експресивна, консультативна, спонукальна і директивна, в рамках яких виявляється «механізм дії» громадської думки на процеси соціального управління суспільством [86].

У зв'язку з вище викладеним можна констатувати, що участь неурядових організацій у забезпеченні інформаційної безпеки має особливе значення, оскільки дозволяє налагодити діалог та конструктивну співпрацю держави з громадянським суспільством для забезпечення стабільності, зниження рівня соціальної напруженості, своєчасного виявлення та успішного реагування на загрози національним інтересам в інформаційній сфері.

Разом з цим, як вже зазначалося раніше, вплив неурядових організацій на інформаційну безпеку може бути як позитивним, так і негативним. Джерелами негативного впливу є діяльність іноземних та міжнародних неурядових організацій, а також вітчизняні неурядові організацій, що функціонують на гроші міжнародних донорських агенцій. Саме їх зусиллями в українське суспільство вносяться непритаманні для вітчизняної цивілізаційної моделі ідеологія і цінності, організаційні моделі тощо. Їх замовниками виступають деякі впливові міжнародні структури, які мають в Україні достатньо розгалужені й ефективні аналітичні, інформаційні та пропагандистські центри, що можуть сприяти просуванню певних ідеологій, негативно впливати на суспільну думку щодо проблем внутрішньої та зовнішньої політики тощо. Інакше кажучи, вони лобіюють свої інтереси за

допомогою неурядових громадських організацій (які у цьому випадку виступають по суті як інструмент цілеспрямованого впливу) [103].

З'ясування сутності та змісту взаємовідносин держави та інститутів громадянського суспільства, а також визначення ролі і місця неурядових організацій в системі забезпечення інформаційної безпеки України дозволяє констатувати: комунікація стає невід'ємною частиною сучасних демократичних режимів. Ефективна комунікація вирішує проблему участі громадськості у прийнятті рішень та контролі за діями влади у різних сферах суспільного життя, включаючи сферу інформаційної безпеки; забезпечує відкритість влади для громадськості та, навпаки, - громадськості для влади у спосіб двостороннього обміну інформацією; формує довіру громадян до влади та дає владі можливість отримати суспільну підтримку; стабілізує суспільні відносини.

Функціональна структура системи забезпечення інформаційної безпеки за рахунок створення каналу «комунікативна підсистема (неформальний контроль) − суб'єкти управління» зумовлює задіяння механізму неформальної самоорганізації, що функціонує паралельно з формальними структурами в рамках моделі «партисипаторного» управління. Партисипаторна підсистема включає в себе «профільні» суб'єкти та суб'єкти «загальної компетенції» недержавного сектору, що безпосередньо та опосередковано опікуються питаннями забезпечення інформаційної безпеки, підсистему недержавних аналітичних інститутів. Саме партисипаторна підсистема забезпечує ненасильницьку конкуренцію в політиці, економіці та будь-якій іншій сфері суспільства з відкритим доступом.

Отже, належна комунікація між суб'єктами забезпечення інформаційної безпеки є одночасно і реалізацією партисипаторної функції системи забезпечення інформаційної безпеки, і доказом належного урядування.

Неурядові організації неоднозначно впливають на інформаційну безпеку як окремої особистості, суспільства, так і держави в цілому. Позитивні та негативні аспекти діяльності неурядових організацій в Україні потребують

окремого комплексного дослідження у контексті впливу на інформаційну безпеку. В сучасних умовах для української держави досить важливим є активне використання наявного потенціалу вітчизняних неурядових організацій, оскільки якщо його не буде використовувати українська влада, то це зроблять сили, які вороже налаштовані до нашої держави.

В сучасних умовах інформаційної агресії Росії виняткове значення має розвиток системи неурядових організацій в сфері забезпечення інформаційної безпеки України, яка базується на активності громадян, різних груп і верств населення. На особливу увагу заслуговує проблема взаємодії державної та недержавної систем забезпечення інформаційної безпеки. Ці системи можуть підсилювати одна одну або протидіяти, вступати в конфлікт між собою. Лише раціонально організована взаємодія державного і суспільного механізмів може запобігти виникненню кризових явищ у суспільстві, конфлікту між державою та громадянським суспільством.

Висновки до розділу 3

Для того, щоб оцінити рівень безпеки України у сфері інформаційно-комунікаційної діяльності з урахуванням впливів результатів інформаційної економіки та світового інформаційного ринку доцільно використовувати різноманітні статистичні дані, що розраховуються консалтинговими, аудиторськими фірмами та іншими організаціями, що спеціалізуються на дослідженнях даного ринку та світової економіки.

У даному розділі було проведено аналіз системи моніторингу розвиту інформаційної економіки та інформаційного суспільства, що розроблені міжнародними організаціями.

Розглядаючи перспективи розвитку інформаційної складової економічної безпеки держави в умовах глобалізації, варто відмітити наступне. Комплексне забезпечення інформаційної безпеки являє собою систему організаційно-правових, соціальних, духовних, інформаційних, програмно-

математичних і технічних методів, заходів і засобів, що забезпечують нормальне функціонування держави, її структур, населення й підприємств.

Державне управління й захист національних інформаційних ресурсів є важливою складовою державної інформаційної політики та інформаційної безпеки держави.

Інформаційна безпека тісно пов'язана з функціонуванням інформаційного ринку, найбільш розгалуженою частиною якого є сфера інформації, а її головним сектором є економічна інформація, що, в свою чергу, безпосередньо пов'язана із проблемою забезпечення економічної безпеки країни в цілому, різних суб'єктів господарювання й особистості.

В умовах реформування економіки України в сучасному глобалізованому економічному та суспільному житті чітко мають бути окреслені та науково обґрунтовані пріоритети національної інформаційної політики, спрямованої на забезпечення економічного зростання. Сьогодні знання та інформація перетворилися у важливий фактор економічного розвитку країни, який залежить від підтримки та розширення глобальної бази знань, що стало можливим за умови існування інформаційного суспільства.

Для забезпечення взаємовідносин між державою та інститутами громадського суспільства з питань забезпечення інформаційної безпеки України в теперішній час ми пропонуємо запровадити «прозору структуру» системи інформаційної безпеки, перейнявши досвід США. Так, у Стратегії національної безпеки громадяни, неурядові організації та некомерційний сектор є повноправними суб'єктами політики та приймають участь в розробці політичних стратегій у сфері інформаційної політики.

Участь неурядових організацій у забезпеченні інформаційної безпеки дозволяє налагодити діалог та конструктивну співпрацю держави з громадянським суспільством для забезпечення нормального функціонування в інформаційній сфері. Адже комунікація між суб'єктами забезпечення інформаційної безпеки є реалізацією партисипаторної функції системи забезпечення інформаційної безпеки.

РОЗДІЛ 4
СТРАТЕГІЧНІ НАПРЯМИ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

4.1. Світовий досвід забезпечення інформаційної безпеки

Національна безпека України, її економічне процвітання та соціальне благополуччя все більше залежать від доступності, цілісності та конфіденційності інформаційних ресурсів, що забезпечуються інформаційними та комунікаційними технологіями.

Доречним є розгляд зарубіжної практики організації і забезпечення інформаційної та кібернетичної безпеки з метою визначення можливостей її використання в Україні. Окреслення ключових стратегічних проблем забезпечення безпеки в інформаційному просторі і шляхів їх вирішення задля розбудови ефективних механізмів державного управління є нагальною потребою сьогодення.

За останні десять років по всій Європі отримали поширення плани заходів та стратегії, покликані вирішити завдання забезпечення інформаційної безпеки. Так, у 2005 році Німеччина прийняла Державний план захисту інформаційної інфраструктури (National Plan for Information Infrastructure Protection – NPSI); у наступному році Швеція розробила Стратегію посилення безпеки Інтернету в Швеції (Strategy to improve Internet security in Sweden). Естонія стала однією з перших країн-членів Євросоюзу, що опублікувала в 2008 р. Державну стратегію кібернетичної безпеки. З тих пір в цій сфері на державному рівні була проведена велика робота, і за останні десять років десять країн-членів Євросоюзу опублікували свої державні стратегії кібернетичної безпеки.

Слід зазначити, що Естонія надає особливого значення необхідності захисту кіберпростору в цілому і ставить в центр уваги безпеку інформаційних

систем. Рекомендовані заходи носять цивільний характер і ґрунтуються на правовому регулюванні, навчанні та співробітництво.

В фінській стратегії, в основі лежить розуміння кібернетичної безпеки як проблеми економічного характеру, тісно пов'язаної з розвитком фінського інформаційного суспільства.

В Словаччині забезпечення інформаційної безпеки розглядається як необхідна умова нормального функціонування і розвитку суспільства. Тому мета стратегії – служити міцним фундаментом для захисту інформації. Стратегія спрямована як на запобігання загрозам, так і на забезпечення готовності і стійкості засобів їх запобігання.

Ключові цілі стратегії кібербезпеки Чехії включають в себе захист інформаційно-комунікаційних систем від вразливостей, яким ці системи піддані, і зменшення потенційного збитку від атак на системи. Основний фокус стратегії доводиться на проблеми вільного доступу до інформаційних сервісів, цілісності і конфіденційності даних в кіберпросторі Чеської Республіки. Стратегія достатньо інтегрована та узгоджується з іншими нормативно-правовими документами Чеської Республіки.

Франція орієнтується на те, щоб інформаційні системи були здатні протистояти подіям в кіберпросторі, які можуть негативно вплинути на доступність, цілісність і конфіденційність інформації. Держава робить акцент на технічні засоби захисту інформації, боротьбу з кіберзлочинністю і встановлення кіберзахисту.

Стратегія Німеччини закладає основу для безпеки критично важливих інформаційних систем. Німеччина зосереджена на запобіганні і кримінальному переслідуванні кібератак, а також на запобігання виходу з ладу IT-обладнання, викликаного випадковими чинниками. Особливо останнє стосується критично важливих інформаційних систем. У стратегії аналізується, чи потрібно проводити додаткові дії (і якщо так, то де саме) щодо захисту IT-систем шляхом надання основних функцій безпеки,

сертифікованих державою, а також підтримкою малого і середнього бізнесу за допомогою створення нової робочої групи.

Литва орієнтується на визначення цілей і заходів, спрямованих на розвиток обороту електронної інформації, а також забезпечення її конфіденційності, доступності та цілісності в кіберпросторі. Крім того, стратегія Литви спрямована на захист персональних даних, телекомунікаційних мереж, інформаційних систем і критично важливих інфраструктур від порушення безпеки і кібератак. У стратегії також визначені заходи, реалізація яких буде гарантувати повну безпеку роботи в кіберпросторі.

Усвідомлюючи вразливість інформаційно-комунікаційних технологій, стратегія Люксембургу стверджує, що найважливіше – громадська та економічна безпека. У стратегії також наголошується на важливості інформаційно-комунікаційних технологій для економічного зростання, як окремих громадян, так і суспільства в цілому. Стратегія працює за п'ятьма напрямами: захист ключової інформаційної інфраструктури і своєчасна реакція на інциденти безпеки; модернізація нормативно-правової бази; державне і міжнародне співробітництво; навчання та інформування; просування стандартів.

Голландія, з одного боку, прагне до безпечних і надійних інформаційно-комунікаційних систем, побоюючись серйозних порушень в цих системах, а з іншого боку, визнає необхідність свободи і відкритості Інтернет-простору. У стратегії дається визначення кібербезпеки, яку розуміють як захищеність від збоїв і неправильної експлуатації інформаційно-телекомунікаційних систем.

Політика Великобританії спрямована на розвиток кібербезпеки і має інноваційну спрямованість. Її метою є виведення на перше місце країни з інновацій, інвестицій та якості сервісів у сфері інформаційно-телекомунікаційних технологій, і тим самим, в повній мірі скористатися всіма перевагами і достоїнствами кіберпростору [105, 106].

У середовищі, де постійно з'являються і еволюціонують інформаційні загрози, державна політика країн Євросоюзу ґрунтується на гнучких, оперативних стратегіях кібернетичної безпеки. Транскордонний характер загроз змушує країни вступати в тісну міжнародну взаємодію, така співпраця необхідна не тільки для ефективної підготовки до кібератак, а й для своєчасної реакції на них, вироблення узгоджених механізмів запобігання. Саме формування національної державної стратегії кібербезпеки є основою для вироблення ефективної державної політики.

Європейська Комісія просуває різні ініціативи, спрямовані як на підвищення цифрових компетенцій робочої сили, так і на споживачів; модернізацію освіти в усіх країнах ЄС; освоєння цифрових технологій для навчання і для визнання і перевірки навичок; прогнозування й аналізу потреб у навичках. «Навички» означає здатність застосовувати знання та використовувати ноу-хау для виконання завдань і вирішення проблем. У контексті «Європейської рамки кваліфікацій» навички описуються як когнітивні або практичні. Цифрова економіка має велике значення для інновацій, зростання, робочих місць і конкурентоспроможності України на шляху євроінтеграції. Поширення цифрових технологій має великий вплив на ринок праці і тип навичок, необхідних в економіці й суспільстві.

За результатами дослідження потенціалу діджиталізації економіки України можна виокремити низку проблем. Це:

– слабка обізнаність українського суспільства щодо переваг діджиталізації та її наслідків;

– недостатнє залучення представників бізнесу, банків і громадського сектору до ІКТ;

– дисбаланси у використанні діджитал-технологій основними групами вітчизняних стейкхолдерів.

Для розв’язання перелічених проблем необхідно:

– підвищити ступінь обізнаності окремих верств суспільства стосовно переваг діджиталізації шляхом популяризації ІКТ у рамках стратегічних

пріоритетів на національному рівні. Досягненню окресленої мети сприятиме проведення конференцій, симпозіумів, воркшопів із залученням вітчизняних експертів та іноземних фахівців;

– на державному рівні розглянути можливість розширення спектра доступних цільових грантів для впровадження й розвитку діджитал-технологій, наприклад за рахунок створення окремих фондів для фінансування ІКТ, співпраці держави з комерційними банками та небанківськими фінансовими установами в напрямі розроблення програм підтримки ІКТ;

– збалансувати ступінь діджиталізації між провідними стейкхолдерами на вітчизняних ринках шляхом стимулювання співпраці представників бізнесу, громадського сектору, банків і освіти. Це дасть змогу визначити потреби кожного стейкхолдера та можливості їх спільного задоволення в умовах діджиталізації.

З огляду на зазначене, державне регулювання процесів становлення та розвитку цифрової економіки в Україні має зосередитись на реалізації наступних основних функцій: створення інституціональної інфраструктури діджиталізації економіки і суспільства; сприяння розвитку інформаційних технологій, розбудові вітчизняної мікроелементної бази; перехід від електронного до цифрового врядування; стимулювання цифровізації виробничих процесів і застосування відповідних бізнес-моделей; інформаційна, цифрова безпека; подолання цифрової нерівності і забезпечення рівного доступу до цифрових послуг; боротьба з корупцією через цифровізацію економіки, широке застосування блокчейн-технологій; всезагальна і неперервна цифрова освіта, підготовка фахівців в галузі цифрових технологій, діджиталізації економіки і врядування.

На сьогодні відсутній єдиний документ, який би визначав стратегічні підходи, механізми, інструменти, заходи з протидії викликам і загрозам у зазначеній сфері.

Формування пакету документів нормативно-правового характеру з даного питання дозволить, визначити правові та організаційні засади

державної політики у цій сфері, основні принципи та напрями забезпечення кібербезпеки держави.

Основними напрямами забезпечення кібернетичної безпеки України сьогодні мають бути наступні:

– розвиток інформаційної інфраструктури держави, забезпечення безпечного функціонування об'єктів критичної інформаційної інфраструктури;

– розвиток міжнародного співробітництва у сфері кібербезпеки;

– зосередження ресурсів і посилення координації діяльності правоохоронних, розвідувальних і контр розвідувальних органів України для боротьби з проявами кіберзлочинності та кібертероризму;

– розвиток пріоритетних напрямів науки і техніки як основи створення високих інформаційних технологій;

– підтримка виробників продукції та послуг у сфері кібербезпеки на засадах стимулювання вітчизняних виробників;

– адаптація законодавства України до норм ЄС, створення нормативно-правових та економічних передумов для розвитку інформаційної інфраструктури держави, підвищення її стійкості до кібератак, спроможності держави більш ефективно захищати національні інтереси в інформаційному просторі;

– забезпечення неухильного дотримання власниками об'єктів критичної інформаційної інфраструктури вимог законодавства у сфері захисту державних інформаційних ресурсів, криптографічного та технічного захисту інформації, захисту персональних даних;

– підвищення рівня обізнаності суспільства щодо ризиків, викликів і загроз у кіберпросторі.

У Конвенції про кіберзлочинність виділяють категорії злочинів, що представлені на рисунку 4.1 (розроблено на основі [107]).

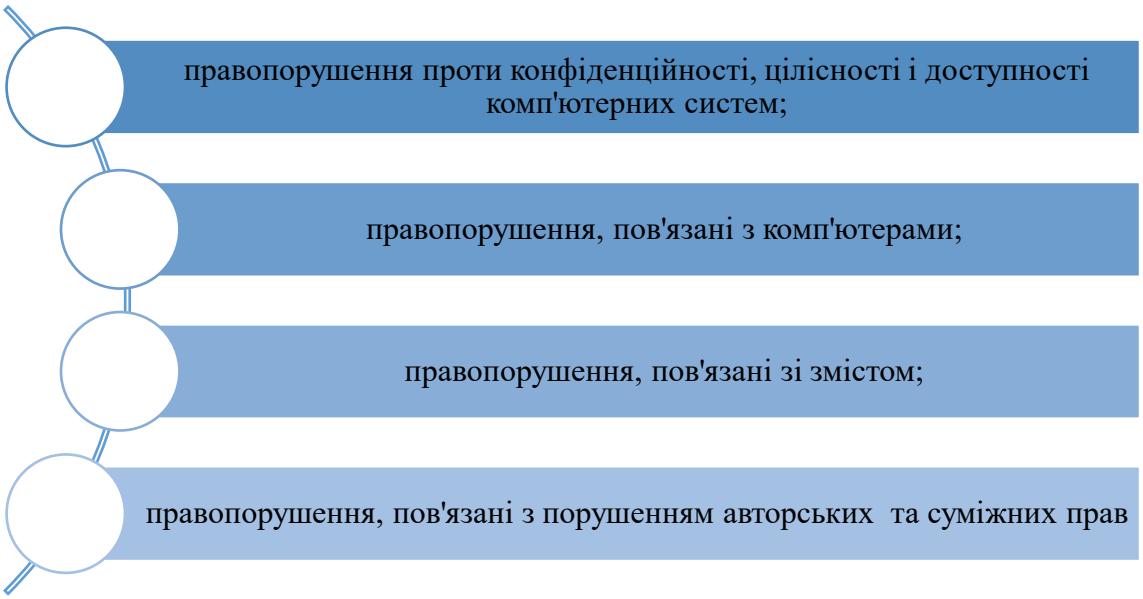

Рис. 4.1. Категорії кіберзлочинів згідно Конвенції про кіберзлочинність

Серйозною перешкодою в питанні забезпечення безпеки «в мережі» є відсутність єдиного центру прийняття рішень та реалізації політики держави. За фактом, відповідальність в питанні кібернетичної безпеки розділяється між декількома структурами, які сьогодні діють не достатньо узгоджено.

В державній стратегії кібернетичної безпеки мають бути розглянуті та висвітлені положення, що стосуються наступного:

– побудова принципової державної моделі, спрямованої на забезпечення кібербезпеки;

– визначення відповідного державного механізму, що дозволяє приватним і державним зацікавленим сторонам обговорювати і затверджувати заходи, пов'язані з проблемою кібербезпеки;

– планування та визначення необхідної політики і регулюючих механізмів, чітке позначення ролей, прав і відповідальності для приватного і державного сектора;

– розробка системного та інтегрованого підходу до державного управління ризиками;

– визначення і позначення цілей інформаційних програм, покликаних прищепити користувачам нові моделі поведінки і моделі роботи;

– доказ необхідності нової програми освіти, що робить упор на навчання ІТ- фахівців і професіоналів у сфері кібербезпеки.

Принципами, на яких має ґрунтуватись та здійснюватися державна політика забезпечення інформаційної та кібернетичної безпеки України представлено на рисунку 4.2.

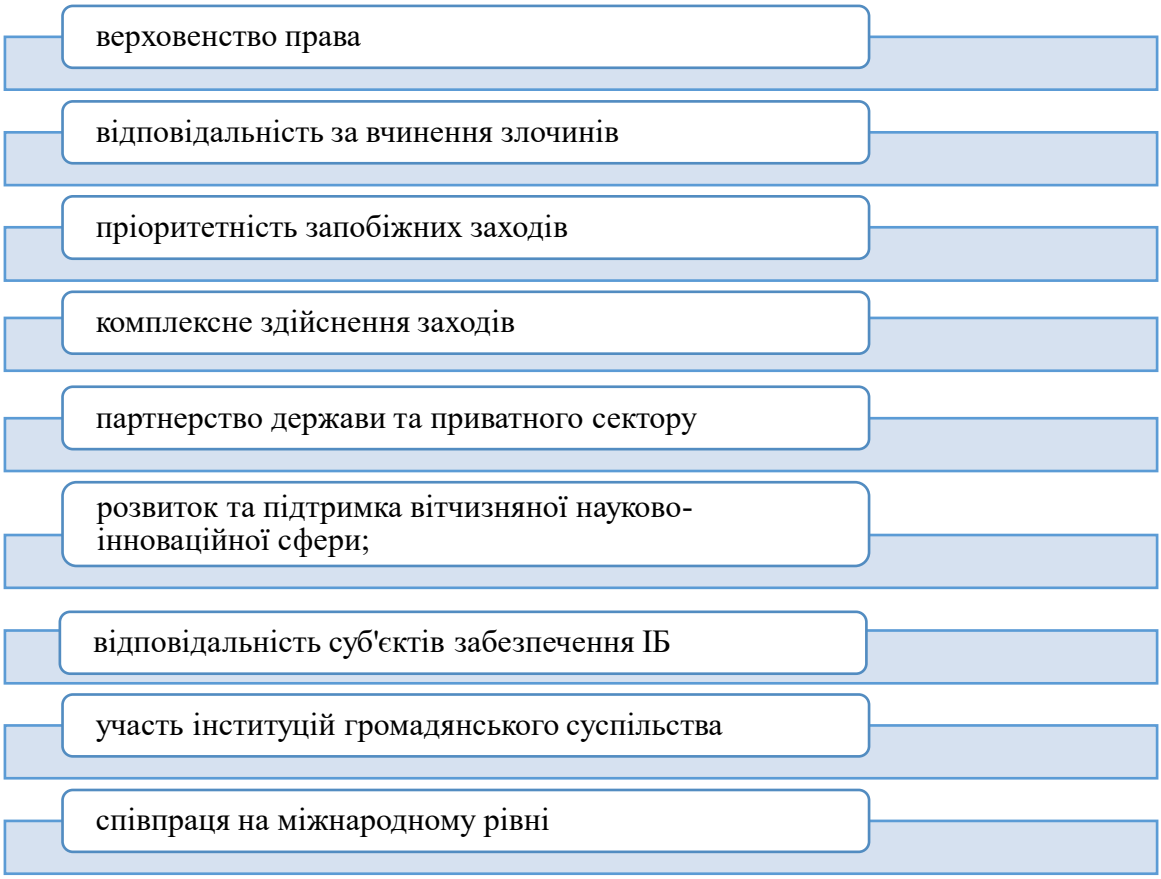

Рис. 4.2. Принципи забезпечення безпеки в інформаційному просторі

Слід констатувати, що в Україні механізми державного забезпечення інформаційної та кібербезпеки, все ще знаходяться на етапах становлення. Деякі з них потребують вдосконалення, однак для розробки більшості та їхніх окремих елементів передусім бракує концептуального обґрунтування. Крім того, в Україні досі відсутні критично важливі елементи національної системи кібернетичної безпеки.

Забезпечення безпеки України в інформаційному просторі має відбуватись із врахуванням існуючої нормативно-правової бази, а саме:

положень Конституції, ЗУ «Про основні засади внутрішньої та зовнішньої політики», ЗУ «Про національну безпеку України», Стратегії національної безпеки України, Доктрини інформаційної безпеки України та ін.

Вкрай необхідним є формування дієвих механізмів державного управління забезпеченням єдиної системи інформаційного захисту, яка б пов'язувала роботу різних структур і підрозділів і стала центром політики держави в сфері інформаційної безпеки країни включно з кібербезпекою.

4.2. Напрями формування інформаційної безпеки України з урахуванням сучасних викликів та загроз

Поступово все більша частина людства долучається до реалізації програм становлення інформаційного суспільства, концепцій переходу до інформаційної доби, планів участі в трансформації суспільних інститутів тощо, прийнятих міжнародними організаціями ООН/ЮНЕСКО, Світовим банком, Світовою організацією торгівлі, Організацією економічного співробітництва і розвитку, Радою Європи, Європейським Союзом, Європейським банком реконструкції і розвитку та іншими міжнародними й регіональними урядовими і неурядовими інституціями, які, зокрема, можуть розглядатися як суб’єкти забезпечення інформаційної безпеки. Основною метою цих документів є визначення стратегічних напрямів розвитку інформаційного суспільства, основних положень, умов і пріоритетів міжнародної, регіональної та національної інформаційної політики, а також політичних, правових, соціально-економічних, культурних та технологічних передумов переходу до інформаційного суспільства [94].

Забезпечення інформаційної безпеки в широкому розумінні має нерозривний сутнісний зв’язок із розвитком інформаційного суспільства як на теоретичному, так і на практичному рівні. Виділення змістових елементів забезпечення інформаційної безпеки зумовлює особливу важливість

приєднання до міждержавних програм розвитку інформаційного суспільства. До таких елементів відносяться:

– мета – суспільство, в якому забезпечується вільний доступ, створення та обмін інформацією, а також інтеграція у світовий інформаційний простір;

– об’єкт – людина і її права на інформацію;

– суб’єкти – міжнародні організації;

– засоби та методи – правове регулювання;

– принципи – гарантованості доступності інформації, інформаційної рівності, використання в інтересах країни міждержавних систем та механізмів міжнародної колективної безпеки.

Еру становлення глобального інформаційного суспільства започаткувала Окінавська хартія глобального інформаційного суспільства, ухвалена 22 липня 2000 р. лідерами країн «великої вісімки».

У вступній частині Хартії зазначається, що інформаційно-телекомунікаційні технології є одним із найбільш важливих факторів, що впливають на формування суспільства XXI ст., створюючи величезні додаткові можливості вжитті людей, їх освіті й роботі, а також взаємодії уряду і громадянського суспільства.

Окремо визначається, що сутність стимульованих інформаційно-телекомунікаційними технологіями економічних та соціальних трансформацій полягає в їх здатності сприяти людям і суспільству у використанні знань та ідей із метою розвитку свого потенціалу та реалізації своїх прагнень. При цьому визнаються необхідними гарантії забезпечення сталого економічного зростання, підвищення суспільного добробуту і створення соціальної злагоди, а також реалізації потенціалу інформаційно-телекомунікаційних технологій у сфері зміцнення демократії, більш прозорого та відповідального управління, в захисті прав людини й сприянні збереженню культурного розмаїття, збереженні миру та стабільності у всьому світі [99].

Стрижневою основою Хартії є визнання необхідності подолання електронно-цифрового розриву всередині держав та між ними, оскільки саме цей фактор гальмує формування глобального інформаційного суспільства й забезпечення реальної інформаційної рівноправності.

У самій Хартії безпосередньо не йдеться про необхідність забезпечення інформаційної безпеки, але практично в кожному пункті наголошується на важливих проблемах, які визначають напрями забезпечення інформаційної безпеки глобального інформаційного суспільства, а саме:

– захист прав людини й сприяння збереженню культурного розмаїття;

– сприяння формуванню мережевої культури та довіри;

– забезпечення рівного, вільного та безпечного доступу всіх до інформаційних ресурсів (подолання електронно-цифрового розриву);

– створення передбачуваної, прозорої й недискримінаційної інформаційної політики та нормативної бази;

– протидія зловживанням, що підривають цілісність інформаційної мережі;

– боротьба з кіберзлочинністю та протидія транснаціональній організованій злочинності;

– захист інтелектуальної власності;

– удосконалення механізмів захисту конфіденційності, а також захисту оброблення персональних даних за умов збереження вільного інформаційного потоку;

– розвиток людських ресурсів [93].

Таким чином, Окінавська хартія є закликом міжнародної спільноти як на державному, так і на приватному рівні до ліквідації розриву в рівні використання інформації і знань, до консолідації зусиль на шляху побудови глобального інформаційного суспільства та забезпечення його безпечного

існування, що сприятиме вирішенню економічних і соціальних світових проблем та утверджуватиме у світі демократичні цінності.

Одним із перших здобутків міжнародної співпраці, що відіграв важливу роль у формуванні уявлень щодо можливої стратегії розбудови інформаційного суспільства в глобальному масштабі, стала прийнята на 29-й сесії Генеральної Конференції ЮНЕСКО в 1996 р. концепція «Інформаційне суспільство для всіх» [94], яка знайшла своє продовження в низці програм під егідою ООН/ЮНЕСКО, відомих під назвами «На шляху до комунікаційного та інформаційного суспільства»,«Комунікація, інформація, інформатика», «Інформація для всіх» та інших.

Виходячи з положень ст. 19 Загальної декларації прав людини, яка закріплює свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів [102], цими програмами ЮНЕСКО відводить собі провідну роль у формуванні глобального інформаційного суспільства, в якому інформація сприймається передусім як знання та забезпечується вільний доступ усіх до неї.

Визнаючи провідну роль інформації в процесах розвитку людства та виступаючи каталізатором діяльності держав,ЮНЕСКО пріоритетною метою на межі 2000 р. визначила створення платформи для дискусії щодо міжнародної політики у сфері захисту інформації і всезагального доступу до неї, стосовно всезагальної участі в глобальному інформаційному суспільстві, а також щодо моральних, правових та суспільних наслідків розвитку інформаційно-телекомунікаційних технологій.

Серед напрямів своєї роботи ЮНЕСКО називала:

– заохочення й розширення доступу до інформації за допомогою її організації, перетворення на цифрову електронну форму й захисту;

– розвиток міжнародної рефлексії та дискусій щодо етичних, правових і суспільних загроз та викликів в інформаційному суспільстві;

– сприяння тренінгу, безперервній освіті й навчанню у сфері інформації та інформатики;

– просування використання міжнародних стандартів і передового досвіду у сфері інформації та інформатики в межах компетенції ЮНЕСКО;

– просування мережевої взаємодії у сфері інформації й знань на локальному, національному, регіональному та міжнародному рівнях [55].

Серед основних негативних чинників, що гальмують розбудову глобального інформаційного суспільства, в документах ЮНЕСКО виокремлюються:

– інформаційно-технологічний дисбаланс та інформаційна ізоляція окремих регіонів і країн (збільшення розриву між інформаційно багатими та інформаційно бідними країнами);

– негативні впливи інформаційно-телекомунікаційних технологій;

– загрози інформаційним правам і свободам людини, включаючи право на доступ до інформації й конфіденційність інформації, а також розповсюдження інформації расистського, агресивного та дискримінаційного характеру;

– інформаційна неосвіченість і різниця у володінні інформаційними навичками [104].

Загальний аналіз програм ЮНЕСКО дозволяє виділити дві основні складові її діяльності в напрямі розвитку інформаційного суспільства й забезпечення інформаційної безпеки:

1) сприяння вільному поширенню інформації (ідей, знань)і загальному доступу до неї;

2) збагачення комунікаційного та інформаційного потенціалу з метою забезпечення всім націям і спільнотам можливості брати участь у світових процесах розбудови глобального інформаційного суспільства.

Єдиний ідеологічний напрям з Окінавською хартією та програмами ЮНЕСКО мають міжнародні домовленості, досягнуті на Всесвітніх зустрічах на вищому рівні з питань інформаційного суспільства, які відбулися в Женеві (2003 р.) та Тунісі (2005 р.), проведених ООН і Міжнародним союзом електрозв’язку.

За підсумками Женевської зустрічі 2003 р. було прийнято Декларацію принципів, яка сформувала бачення концепції становлення інформаційного суспільства як «глобального завдання в новому тисячолітті» [105].

Загальна концепція інформаційного суспільства і керівні положення Декларації принципів знайшли своє втілення в Плані дій, також прийнятому на Женевському саміті 2003 р. [46].

План дій має більш конкретизований зміст і визначає основні напрями діяльності, які ведуть до досягнення цілей розвитку, шляхом сприяння широкому впровадженню інформаційно-комунікаційних технологій, а також спрямовані на подолання розриву в цифрових технологіях.

Третім пунктом Плану окреслюється роль органів державного управління, міжнародних і регіональних установ, інститутів громадянського суспільства та приватного сектору в становленні інформаційного суспільства. Провідну роль у формуванні національних стратегій інформаційного розвитку План відводить державі. Разом із тим, участь приватного сектору має велике значення для активізації процесів інформатизації, міжнародні організації відіграють ключову роль в інтеграційних процесах, а громадянське суспільство покликане сприяти збереженню та примноженню загальнолюдських цінностей, передусім справедливості.

Серед спільних напрямів діяльності згідно з Планом дій виокремлюються наступні:

1) розвиток інформаційно-комунікаційної інфраструктури на основі новітніх технологій;

2) популяризація електронних інформаційних ресурсів та забезпечення всезагального доступу до них;

3) сприяння освіті у сфері інформаційно-комунікаційних технологій та інформатизація освіти загалом;

4) створення сприятливих політичних, економічних, правових умов для розвитку інформаційно-комунікаційних технологій, зокрема Інтернету як важливого засобу розвитку інформаційного суспільства;

5) забезпечення безпеки й надійності використання інформаційно-комунікаційних технологій;

6) глибока інформатизація суспільно важливої діяльності – державного управління, комерції, науки, навчання, охорони здоров'я, охорони навколишнього середовища, сільського господарства, а також сфери культури й засобів масової інформації;

7) утвердження загальнолюдських цінностей;

8) міжнародне та регіональне співробітництво з метою подолання цифрового розриву.

На відміну від інших розглянутих міжнародних документів, План дій певною мірою конкретизує і сферу забезпечення інформаційної безпеки. Так, його п. 12 довіра й безпека відносяться до «головних опор інформаційного суспільства». Цей же пункт містить прямі настанови органам державного управління, за підтримки приватного сектору, щодо попередження і виявлення проявів кіберзлочинності та неналежного використання інформаційно-комунікаційних технологій шляхом застосування необхідних заходів правового й організаційного характеру, міжнародної співпраці та сприяння обізнаності людей щодо нових загроз конфіденційності їх життя й способів захисту від них.

Наступний саміт із питань інформаційного суспільства, проведений у Тунісі у 2005 р., підтвердив усі попередні прагнення та цілі щодо розвитку інформаційного суспільства. Його результатами стало прийняття Туніського зобов'язання і Туніської програми для інформаційного суспільства.

Туніське зобов'язання стало черговим закликом світової спільноти до консолідації зусиль на шляху розбудови відкритого для всіх, справедливого інформаційного суспільства. При цьому виокремлено основоположну роль інформаційно-комунікаційних технологій для економічного зростання, необхідність усунення перешкод на шляху подолання «цифрового розриву», а також необхідність ефективної протидії проблемам і загрозам, що виникають унаслідок використання інформаційно-комунікаційних технологій усупереч

цілям підтримання міжнародної безпеки й стабільності. Серед таких загроз зазначається зловживання інформаційними ресурсами і технологіями зі злочинними й терористичними цілями та недотримання прав людини [93].

Особливістю Туніської програми для інформаційного суспільства є те, що поряд із напрямами вирішення фінансових питань щодо подолання «цифрового розриву» широко піднімаються проблеми Інтернету, який визнається цим документом основним елементом інфраструктури інформаційного суспільства, що перетворився з науково-дослідного й навчального інструменту на загальнодоступний глобальний інструмент. У зв'язку з цим гостро ставляться питання глобальної безпеки Інтернету, а саме: постійний розвиток культури кібербезпеки, посилення захисту інформації особистого характеру і персональних даних, удосконалення механізмів притягнення до кримінальної відповідальності за кіберзлочини (включаючи злочини,скоєні в межах юрисдикції однієї країни, які призвели до наслідків в іншій країні), а також вирішення проблем із поширенням спаму [74].

Розглянуті міжнародні акти свідчать, що країни-члени ООН намагаються докладати значних зусиль для досягнення світової злагоди і забезпечення належного рівня життя шляхом розбудови глобального інформаційного суспільства. Водночас за результатами Оцінки прогресу, досягнутого в здійсненні рішень, і подальшої діяльності за підсумками Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства, представленої Економічною та Соціальною Радою ООН у 2010 р.,поряд із позитивними здобутками відмічаються недостатні темпи скорочення цифрового розриву, особливо щодо можливостей користування швидкісним Інтернетом, що призводить до посилення нерівності доступу до інформаційно-телекомунікаційної інфраструктури між розвинутими країнами і країнами, що розвиваються, а також різними верствами населення [34].

Давню правову історію має суто європейський досвід становлення інформаційного суспільства. Серед перших нормативно-правових актів, спрямованих на вирішення питання становлення інформаційного суспільства

в ЄС є Резолюція Європейського Союзу «Біла Книга. Зростання, конкурентоспроможність, зайнятість: виклики та стратегії XXI століття» 1993 р., Директива ЄС «Зелена Книга. Життя і працевлаштування в інформаційному суспільстві» та Рекомендація «Інформаційна магістраль для глобального суспільства» 1996 р.

Діалектичний взаємозв'язок європейської і глобальної стратегій становлення інформаційного суспільства представлено в концептуальній доповіді Європейської комісії з проблем інформаційного суспільства «Європа і глобальне інформаційне суспільство: рекомендації для Європейської Ради ЄС» 1994 р. У ній зазначається, що глобальні інформаційні процеси впливають на становлення нової ієрархії держав, відкривають нові можливості промислового розвитку, зумовлюють створення відповідної правової бази, підвищують рівень обміну культурою та традиціями [15]. «Європа усвідомлює важливість глобального співробітництва і необхідність правил для інформаційного суспільства, які стосуються права на інтелектуальну власність, недоторканність приватного життя, охорони персональних даних, інформаційної безпеки, використання інформаційного ресурсу, заборони незаконної інформації. В документах підкреслюється, якщо Європа не зможе ефективно адаптуватися до нових умов, вона втратить конкурентоспроможність на світових і регіональних ринках і матиме соціальні проблеми в європейських країнах» [72].

Реалізація стратегії інформаційного суспільства в ЄС ґрунтується на потужному матеріально-фінансовому забезпеченні. Для розвитку ідей інформаційної політики ЄС в окремих сферах життєдіяльності суспільства створюються програми та проекти, а саме: «Розвиток технологічних досліджень», «Інформаційні технології і ринкова політика», «Європейська стратегічна програма промислового розвитку і впровадження технологій», «Он-лайн для урядів», «Глобальна інвентаризація», «Електронна комерція», «Дистанційна освіта, медицина, культура та інформаційні послуги» [91].

Як орієнтир діяльності практичну цінність для України мають європейські програми, сформовані в межах Лісабонської стратегії (Lisbon Strategy) 2000 р. [79]. Їх відображенням є послідовні плани дій становлення інформаційного суспільства і забезпечення безпеки головного стратегічного інструменту – мережі Інтернет. До них належать низка планів дій «Електронна Європа» («e-Europe») та «Безпечніший Інтернет» («Safer Internet»).

Загалом Плани дій «e-Europe» охоплюють багато напрямів, які згруповані навколо трьох основних пріоритетів:

1) дешевий, швидкий, безпечний Інтернет;

2) інвестиції в людей та їхні інформаційно-комунікаційні навички;

3) стимулювання використання Інтернету в різних галузях діяльності.

Особливим здобутком європейської співпраці, що заслуговує окремої уваги, є Конвенція Ради Європи про кіберзлочинність 2001 р., яка здійснила прорив у забезпеченні інформаційної безпеки, заклавши основи світових стандартів протидії злочинам у сфері інформаційно-комунікаційних технологій [38].

Виходячи із численних міжнародних домовленостей і рішень світового та європейського масштабу, спрямованих на забезпечення безпеки інформаційно-комунікаційних технологій та забезпечення прав людини під час їх використання, Конвенція покладає на держави, що її підписали, зобов’язання встановлення кримінальної відповідальності за поведінку, що вважається проявом кіберзлочинності.

Крім того, Конвенцією на загальному рівні врегульовуються питання надання повноважень, достатніх для ефективної боротьби з означеними кримінальними правопорушеннями «шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва» [38].

Підписання Конвенції про кіберзлочинність є важливим кроком міжнародної спільноти на шляху практичного забезпечення

інформаційної безпеки в глобальному масштабі. Наявні й інші міжнародні досягнення в галузі безпосереднього забезпечення інформаційної безпеки на рівні окремих організацій різних форм власності. Найвідоміші з них – узагальнені принципи організації системи управління інформаційною безпекою, які отримали назву «Стандарти управління інформаційною безпекою» та завдяки своїй ефективності набули широкого визнання, ставши основою національних стандартів багатьох сучасних держав.

Першопричиною виникнення стандартів управління інформаційною безпекою були потреби великих комерційних структур у забезпеченні власної інформаційної безпеки, особливо стосовно захисту комерційної таємниці та належного забезпечення доступу до інформаційних ресурсів. Однак комплексність підходів, закладена цими стандартами, є практичним втіленням багатьох концептуальних положень міжнародних актів щодо забезпечення інформаційної безпеки і, зокрема, ефективним превентивним заходом протидії кіберзлочинності.

Родоначальником низки сучасних міжнародних стандартів у галузі систем управління інформаційною безпекою (СУІБ) став стандарт BS 7799, розроблення якого Британським інститутом стандартів BSI (British Standards Institution) почалася ще1995 р. [12].

Положення цього стандарту на добровільній основі застосовує велика кількість компаній у десятках країн світу (у 27 країнах видано понад 1100 сертифікатів відповідності). Сертифікація системи управління інформаційною безпекою на відповідність стандарту BS 7799 дозволяє власникам інформаційних ресурсів та їх партнерам переконатися в тому, що підсистема інформаційної безпеки побудована правильно й функціонує ефективно.

Слід зазначити, що стандарт BS 7799 не є технічним. Він визначає загальну організацію, класифікацію даних, системи доступу,напрями планування, відповідальність співробітників, використання оцінки ризиків тощо в контексті забезпечення інформаційної безпеки.

Основні напрями управління інформаційною безпекою стандарту представлено на рисунку 4.3.

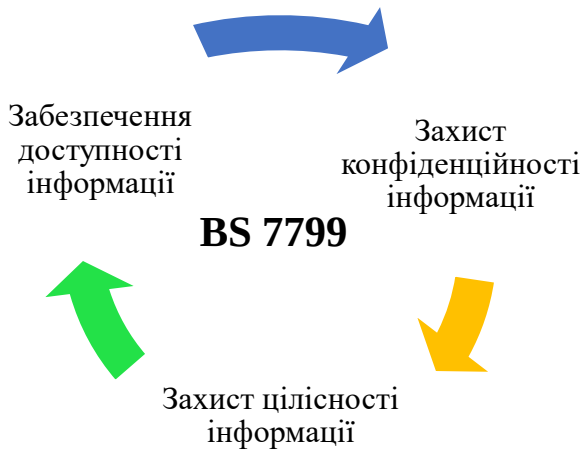

Рис. 4.3. Напрями управління ІБ стандарту BS 7799

Певної універсальності цьому стандарту надає й те, що він не концентрується лише на конфіденційності. У комерційних організаціях, із погляду можливих матеріальних втрат, цілісність і доступність даних найчастіше є більше критичними.

Серед можливих загроз, на протидію яким орієнтовано стандарт, виділяються: хакерські атаки; зараження комп'ютерними вірусами; комп'ютерне піратство; промислове шпигунство; фізичне втручання в комп'ютерні системи; несумлінність персоналу; надійність апаратно-програмних засобів тощо [71].

Таким чином, основну мету Стандарту можна сформулювати як створення загальної методології для розроблення, впровадження й оцінювання ефективності систем управління інформаційною безпекою, що може застосовуватись в умовах як комерційних компаній, так і державних та некомерційних структур із чисельністю в десятки тисяч співробітників.

На основі стандарту BS 7799 Міжнародною організацією стандартизації ISO (International Organization for Standardization)та Міжнародною електротехнічною комісією IEC (International Electro technical Commission)

розроблено сімейство стандартів ISO/IEC 27000, які удосконалюються і доповнюються кожного року. Також проводиться його уніфікація з популярними стандартами управління COBIT (Control Objectives for Informationandrelated Technology – Міжнародний стандарт управління інформаційними технологіями) й ITIL (Information Technology Infrastructure Library – бібліотека інфраструктури інформаційних технологій) та іншими.

Крім управління інформаційною безпекою, є ще один напрям стандартизації –захист інформації з обмеженим доступом, особливо важливий на державному рівні. До відомих стандартів у цій сфері належить розгалужена система стандартів STANAG (Standardization Agreement), більшість яких повторюють стандарти військового відомства США –MIL Standart [81] і є основою політики захисту інформації з обмеженим доступом країн НАТО; а також канадський Стандарт CSA1996 р., який Міжнародною організацією стандартизації було покладено в основу розвитку міжнародних стандартів щодо персональної інформації, зокрема ISO 29100 «Information technology. Security techniques. Privacy framework» (Інформаційні технології. Методи забезпечення безпеки. Межі конфіденційності) [47].

Слід зазначити, що Україна не в авангарді широкого впровадження міжнародних стандартів у сфері забезпечення інформаційної безпеки, хоча необхідність цього процесу сьогодні вже усвідомлена. Так, Доктриною інформаційної безпеки України серед напрямів державної політики у сфері забезпечення інформаційної безпеки зазначається гармонізація вітчизняного законодавства з питань інформаційної безпеки в економічній сфері з міжнародними нормами і стандартами [47]. Крім того, ще у 2002 р. Проект Концепції національної інформаційної політики як одну з основних вимог до національної інформаційної інфраструктури визначав відповідність міжнародним стандартам і рекомендаціям Міжнародного телекомунікаційного союзу (ITU), Європейської конференції адміністрацій поштового та електрозв’язку (CEPT) і Міжнародної організації стандартизації/Міжнародної електротехнічної комісії (ISO/IEC), що повинно

сприяти взаємодії технічних засобів, інформаційних пристроїв і послуг із тими, що діють у світовому інформаційному просторі в складі Глобальної інформаційної інфраструктури [68].

Утім, упровадження стандартів управління інформаційною безпекою в Україні просувається вкрай повільно. Наразі офіційного визнання набули лише два, як галузеві стандарти банківської сфери, введені в дію НБУ:СОУ Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги» (ISO/IES 27001:2005, MOD) та СОУ Н НБУ 65.1 СУІБ2.0:2010 «Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою» (ISO/IES 27002:2005,MOD). Прикладом для України в цьому напрямі може бути досвід Російської Федерації, яка впроваджує міжнародні стандарти управління інформаційною безпекою на рівні державних (національних) стандартів із 2005 р. [85; 86].

Теоретично альтернативним для України на шляху становлення інформаційного суспільства й забезпечення інформаційної безпеки міг би стати досвід євразійської міжнародної співпраці, зокрема напрацьований Шанхайською організацією співробітництва (ШОС) і Євразійським економічним співтовариством (ЄврАзЕС). Проте проблеми становлення інформаційного суспільства не привертають увагу на рівні офіційних документів навіть як перспективні, а питання забезпечення інформаційної безпеки сприймаються більшою мірою в контексті спрямованості діяльності цих організацій.

Так, представниками ШОС у 2007 р., разом із підписанням Бішкекської декларації, був затверджений План дій із забезпечення міжнародної інформаційної безпеки, який стосується спільної протидії кіберзлочинності та кібертероризму, що розглядається в рамках співробітництва в боротьбі з тероризмом, сепаратизмом і екстремізмом [17].

Із результатів діяльності ЄврАзЕС корисними досвідом для України можуть стати типові проекти законів, серед яких і проект закону «Про інформаційну безпеку», розроблені в межах створення Податкового союзу і

Єдиного економічного простору [25]. Зауважимо, що ці типові проекти формують певні законодавчі стандарти для країн-членів ЄврАзЕС у сфері інформаційно-комунікаційних технологій.

Відтак, пріоритетами удосконалення забезпечення інформаційної безпеки є:

1) удосконалення правового забезпечення інформаційної безпеки шляхом розробки її концептуальних основ:

– визначення або уточнення завдань, функцій і повноважень суб'єктів забезпечення інформаційної безпеки України;

– забезпечення інформаційного суверенітету України з метою недопущення інформаційної залежності та інформаційної експансії з боку інших держав чи міжнародних структур;

– сприяння розвитку міжнародного співробітництва в інформаційній сфері в умовах перегляду його принципів і механізмів, посиленню міжнародно-правової відповідальності за використання в інформаційній сфері сил і засобів, які негативно впливають або створюють загрози людині, суспільству, державі;

2) зміцнення організаційних основ забезпечення інформаційної безпеки:

– вирішення питання координації діяльності суб'єктів забезпечення інформаційної безпеки, зокрема у сфері протидії інформаційній агресії, забезпечення кібернетичної безпеки України;

– налагодження системи державно-приватного партнерства у сфері забезпечення інформаційної безпеки;

– запровадження системи демократичного контролю за діяльністю державних суб'єктів забезпечення інформаційної безпеки;

– розвиток комунікаційної політики у стосунках "держава-суспільство".

Головним тригером, який ініціює необхідність формування інформаційної безпеки, є загрози. Результатом їх впливу, як правило, є негативні наслідки. Для зниження їх рівня слід застосовувати спеціальні

заходи інформаційної безпеки, які дозволять виявляти та попереджати загрози. Їх організація потребує фінансових ресурсів, які інвестуються у придбання, розробку та впровадження інструментів безпеки. При чому обсяг фінансування залежатиме від рівня та важливості наслідків іфнормаційних загроз для кожного суб'єкта національної економіки. З метою чіткого розуміння процесу забезпечення інформаційної безпеки, проаналізуємо, як це здійснюється у державному, підприємницькому секторах та для окремих осіб.

На рисунку 4.4 представлена концептуальна модель забезпечення інформаційної безпеки держави з урахуванням загроз та їх наслідків, де можна побачити, що різного роду загрози впливають на інформацію, знання та інформаційні системи, результатом чого є негативні наслідки для країни. Для попередження загроз повинні існувати відповідні заходи інформаційної безпеки, організація яких пов'язана із джерелами фінансування.

Рис. 4.4. Концептуальна модель забезпечення інформаційної безпеки держави з урахуванням загроз та їх наслідків

Що стосується забезпечення інформаційної безпеки економічних агентів (суб'єктів підприємницької діяльності, банків, страхових компаній, тощо), то її концептуальна модель представлена на рисунку 4.5.

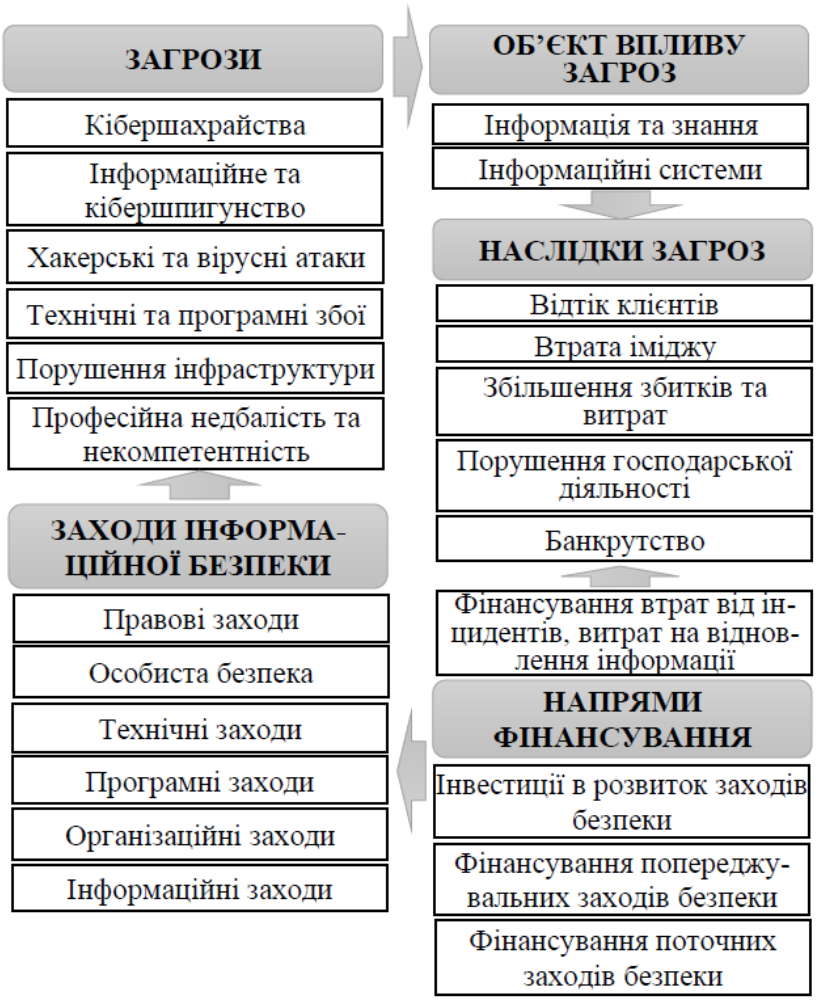

Рис. 4.5. Концептуальна модель забезпечення інформаційної безпеки економічних агентів

Порівнюючи моделі забезпечення інформаційної безпеки держави та економічних агентів, можна виокремити безліч спільних характеристик, що характеризують події, об'єкти безпеки та напрями фінансування. Відмінності полягають у масштабах і характері наслідків, а також типах загроз. Таким чином, для економічних агентів вплив інформаційних загроз відчувається в результатах їхньої господарської діяльності, що може призвести до їхнього повного зупинення, а згодом стати причиною банкрутства. Для держави

характер наслідків також може бути масштабним, але не призводити до повного руйнування економіки.

Що стосується рівня окремих індивідумів, то концептуальна модель забезпечення їх персональної інформаційної безпеки представлена на рисунку 4.6.

Рис. 4.6. Концептуальна модель забезпечення персональної інформаційної безпеки індивідів

Можна зазначити, що крім перерахованих вище загроз, характерних також для рівня держави та економічних агентів, для окремих індивідів найбільш значущою є соціальна інженерія, що полягає у використанні різних способів маніпулювання людьми для отримання особистих фінансових даних, а також паролів для доступу до особистих сторінок. , поштових скриньок і рахунків. Це звичайна кіберзагроза для клієнтів банку. Низька інформованість про заходи захисту інформації є причиною недбалого ставлення людини до

засобів індивідуального захисту при виконанні операцій з використанням мобільних та обчислювальних пристроїв, що призводить до втрати інформації. Наслідки впливу інформаційних загроз для людини - втрата даних, грошей і пристроїв. За умови застосування превентивних заходів і постійних заходів захисту можна підвищити рівень особистої безпеки кожної людини.

Для забезпечення функціонування системи інформаційної безпеки на державному рівні і рівні господарюючих суб'єктів необхідно сформувати дієвий механізм, тобто комплекс суб'єктів-виконавців, який здійснюватиме безпосередній захист інформації та інформаційних систем з урахуванням вимог законодавства. Це можливо лише шляхом створення низки відповідних органів виконавчої влади, функції яких будуть безпосередньо пов'язані із захистом, координацією, контролем за забезпеченням державної інформаційної безпеки та захисту, фізичним, логічним та адміністративним контролем за безпекою підприємств та фінансових інститутів.

Висновки до розділу 4

Отже, орієнтирами для державної політики України в напрямі формування інформаційної безпеки мають бути: по-перше, продовження міжнародної, зокрема європейської, співпраці з інформаційно розвиненими державами, спрямованої на повноцінне приєднання до програм інформаційного розвитку та гармонійне впровадження отриманого досвіду в справу розбудови майбутнього українського суспільства; по-друге, продовження гармонізації положень міжнародних актів із законодавством України (особливо це стосується вимог Конвенції про кіберзлочинність); по-третє, посилення практичної реалізації задекларованих намірів щодо розвитку національної інформаційно-комунікаційної інфраструктури, створення якісних і доступних інформаційних ресурсів, інформатизації освіти й науки, підтримання національної інформаційної продукції, забезпечення повсюдного доступу всіх громадян до мережі Інтернет, розширення можливостей

отримання електронних послуг, широке впровадження визнаних світових стандартів у сфері безпеки інформаційно-телекомунікаційних технологій тощо.

Основними детермінантами формування архітектоніки інформаційної безпеки України є зовнішні та внутрішні загрози, що впливають на порушення цілісності, конфіденційності та доступності інформації, знань і безпосередньо інформаційних систем суб'єктів, у результаті цього виникають деструктивні наслідки для економічного, соціального та політичного розвитку країни. Для їх попередження і виявлення інцидентів на рівні держави, суб'єктів господарювання, фінансових інститутів та індивідуумів повинна бути сформована відповідна організаційно-правова структура, ефективність функціонування якої повинна оцінюватися за обсягами зменшення втрат національної економіки від дій інсайдерів та кібершахраїв.

ВИСНОВКИ

Поступове й доволі умовне поєднання умовного і реального просторів за допомогою ІТ-систем і мережних технологій різного функціонального призначення, а також відповідного програмного забезпечення призвело до формування кіберпостору − віртуального комунікаційного середовища, утвореного системою зв'язків між користувачами та об'єктами інформаційної інфраструктури.

Інформаційна безпека є невід'ємною складовою національної безпеки держави. Із зростанням науково-технічного прогресу зростає і важливість питання інформаційної безпеки громадянина, суспільства, держави.

Інформаційна безпека розглядається як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Слід зазначити, що у науковій літературі бракує єдиного погляду на зміст поняття «інформаційна безпека».

Інформаційну безпеку у найзагальнішому розумінні − стан захищеності інформаційного простору держави, за якого неможливо завдати збитку властивостям об'єкта безпеки, що стосується інформації та інформаційної інфраструктури, і який гарантує безперешкодне формування, використання й розвиток національної інфосфери в інтересах оборони.

Основними характеристиками інформаційної безпеки на сьогодні залишаються доступність, цілісність та конфіденційність.

У процесі дослідження інформаційної безпеки важливо моніторити загрози та ризики, що мають негативний вплив, до них відносять: розголошення, витік та несанкціонований доступ до інформації.

Принципово новим різновидом терористичних дій у віртуальному просторі є кібертероризм. Хоча чіткого визначення даного поняття поки не існує, під ним ми розуміємо суспільно небезпечну діяльність, що свідомо здійснюється в кіберпросторі окремими особами або організованими групами з терористичною метою та реалізується ними через заздалегідь сплановані й політично вмотивовані кібератаки на інформаційно-телекомунікаційних системах з використанням високих технологій.

Кібертероризм як головна складова кіберзлочинності посідає не останнє місце серед низки загроз національній безпеці та інтересам України.

Протягом останніх років Україна, як і більшість країн світу, робить певні кроки в розбудові інформаційного суспільства, забезпечення інформаційної та кібербезпеки, а також у боротьбі з кіберзлочинністю.

Удосконалення нормативно-правової бази забезпечення інформаційного суспільства в Україні дозволить врегулювати нормативні аспекти діяльності щодо впровадження та використання інформаційних технологій, продукування та розповсюдження електронної інформації, створення та використання національних інформаційних ресурсів та радіочастотного ресурсу, розвитку телекомунікацій, створення системи стандартизації у сфері інформації, забезпечення інформаційної безпеки тощо. Однією з основних перешкод на шляху побудови інформаційного суспільства в Україні є неузгодженість норм національного законодавства між собою, а також з нормами міжнародного права у цій сфері.

Потребує впорядкованості понятійний апарат та термінологія нормативно-правової бази забезпечення розвитку інформаційного суспільства в Україні.

Необхідно нормативно встановити такий порядок підготовки законів і підзаконних актів щодо сфери інформатизації, який забезпечить попередній

аналіз проектів законів та підзаконних актів експертами різних секторів – громадського, приватного і державного. Відсутність такої процедури призводить до того, що більшість законів, які формують теоретичну основу галузі, не узгоджуються один з одним і тому виникають проблеми в їх практичному застосуванні.

Наведені моделі процесів управління ризиками інформаційної безпеки дають можливість зручно, швидко та точно отримати цілісну картину ситуації відносно ризиків та загроз інформаційній безпеці, приймати оптимальні управлінські рішення стосовно обробки ризиків. Представлені моделі у сукупності відтворюють процес управління ризиками інформаційної безпеки, наведений у міжнародному стандарті ISO/IEC 27005:2011.

Запропоновані моделі дозволять отримувати науково-обґрунтовані організаційно-технічні рішення, впровадження яких сприятиме: підвищенню рівня інформаційної безпеки будь-якого суб'єкта господарювання та захисту його активів від множини зовнішніх та внутрішніх загроз, своєчасному виявленню вразливостей, зменшенню потенційних наслідків від реалізації загроз та зниженню ймовірності їх виникнення у майбутньому, мінімізації збитків, усуненню інцидентів та неприйнятних ризиків. У подальшому повинні звести до мінімуму розміри збитків від подій, що несуть загрози безпеці, шляхом їх нейтралізації.

Для того, щоб оцінити рівень економічної безпеки України у сфері інформаційно-комунікаційної діяльності з урахуванням впливів результатів інформаційної економіки та світового інформаційного ринку доцільно використовувати різноманітні статистичні дані, що розраховуються консалтинговими, аудиторськими фірмами та іншими організаціями, що спеціалізуються на дослідженнях даного ринку та світової економіки.

Аналіз даних за індексом EGDI, свідчить, що динаміка субіндексу HCI в Україні практично не змінилася, показники субіндексу TII – телекомунікаційної інфраструктури вказують на постійне зростання. Але субіндекс онлайн послуг – OSI має значні коливання, що вказує на те, що

Україна не встигає за лідерами у сфері запровадження та модернізації онлайн послуг.

Інформаційна безпека тісно пов'язана з функціонуванням інформаційного ринку, найбільш розгалуженою частиною якого є сфера інформації, а її головним сектором є економічна інформація, що, в свою чергу, безпосередньо пов'язана із проблемою забезпечення економічної безпеки країни в цілому, різних суб'єктів господарювання й особистості.

В умовах реформування економіки України в сучасному глобалізованому економічному та суспільному житті чітко мають бути окреслені та науково обґрунтовані пріоритети національної інформаційної політики, спрямованої на забезпечення економічного зростання. Сьогодні знання та інформація перетворилися у важливий фактор економічного розвитку країни, який залежить від підтримки та розширення глобальної бази знань, що стало можливим за умови існування інформаційного суспільства.

Світовий досвід розвитку інформаційного ринку показує, що управлінська та підприємницька діяльність потребують постійного отримання економічної інформації, а також інформації соціального характеру. Зважаючи на зростання значущості інформаційної складової економічної безпеки, необхідно перейти до прогностичної випереджувальної моделі інформаційного забезпечення, яка передбачає ефективний захист від технологій інформаційного впливу та задовольняє зростаючу потребу суспільства в одержанні необхідного обсягу достовірної і корисної інформації.

Для забезпечення взаємовідносин між державою та інститутами громадського суспільства з питань забезпечення інформаційної безпеки України в теперішній час ми пропонуємо запровадити «прозору структуру» системи інформаційної безпеки, перейнявши досвід США. Так, у Стратегії національної безпеки громадяни, неурядові організації та некомерційний сектор є повноправними суб'єктами політики та приймають участь в розробці політичних стратегій у сфері інформаційної політики.

Участь неурядових організацій у забезпеченні інформаційної безпеки дозволяє налагодити діалог та конструктивну співпрацю держави з громадянським суспільством для забезпечення нормального функціонування в інформаційній сфері. Адже комунікація між суб'єктами забезпечення інформаційної безпеки є реалізацією партисипаторної функції системи забезпечення інформаційної безпеки.

Отже, орієнтирами для державної політики України в напрямі вирішення проблем забезпечення інформаційної безпеки мають бути: по-перше, продовження міжнародної, зокрема європейської, співпраці з інформаційно розвиненими державами, спрямованої на повноцінне приєднання до програм інформаційного розвитку та гармонійне впровадження отриманого досвіду в справу розбудови майбутнього українського суспільства; по-друге, продовження гармонізації положень міжнародних актів із законодавством України (особливо це стосується вимог Конвенції про кіберзлочинність); по-третє, посилення практичної реалізації задекларованих намірів щодо розвитку національної інформаційно-комунікаційної інфраструктури, створення якісних і доступних інформаційних ресурсів, інформатизації освіти й науки, підтримання національної інформаційної продукції, забезпечення повсюдного доступу всіх громадян до мережі Інтернет, розширення можливостей отримання електронних послуг, широке впровадження визнаних світових стандартів у сфері безпеки інформаційно-телекомунікаційних технологій тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Шульга В.І. Сучасні підходи до трактування поняття інформаційна безпека [Електронний ресурс] / В.І. Шульга // Електронне наукове фахове видання «Ефективна економіка». – 2015. - № 4. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=5514.

2. Зубок М.І. Інформаційна безпека [Текст] : навч. посібник / М.І. Зубок; Київський національний торговельно-економічний ун-т. – К. : КНТЕУ, 2005. – 133.

3. Гавловський В. Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект) // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К., 2000. – С 50-52.

4. Богуш В. Інформаційна безпека держави / Володимир Богуш, Олександр Юдін; Гол. ред. Ю. О. Шпак. – К.: «МК-Прес», 2005. – 432 с.

5. Барановський О.І. Фінансова безпека / О.І. Барановський. – К.: Фенікс, 1999. – 338 с.

6. Гавловський В. Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект) // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К., 2000. – С 50-52.

7. Жарков Я. М., Бєсєдіна Л.М. Напрямки зовнішнього інформаціно-психолоічного впливу на Україну [Електронний ресурс] / Жарков Я. М., Бєсєдіна Л.М. // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. – 2009. – № 19. – Режим доступу: http//www.nbuv.gov.ua / portal / natural/ znpviknu / 2009-19 / vip19-21.pdf.

8. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз / Т. Ткачук // Інформаційне право. – 2017. – № 10. – с. 182-186.

9. Конституція України. Прийнята Верховною Радою України 28 червня 1996 року // Відомості Верховної Ради України. – 1996. – №30 – Ст. 141.

10. Макаренко В. Правове регулювання захисту конфіденційної інформації, що є власністю держави: становлення, розвиток, проблемні питання / В. Макаренко // Право України. – 2006. – № 1. – С. 132-135.

11. Кормич Б.А. Інформаційна безпека: організаційно-правові основи [Текст]: навч. посібник для студ. вищих навч. закл. / Б.А. Кормич. – К.: Кондор, 2004. – 384 с. – (Юридична книга).

12. Ковтун С. В. Інформаційна безпека: підручник / С.В. Ковтун. – Харків. Вид. ХНЕУ, 2009. – 368 с.

13. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник / Ліпкан В. А., Максименко Ю. Є., Желіховський В. М.. - К.: КНТ, 2006. - 280 с. (Серія: Національна і міжнародна безпека) [Електронний ресурс]. – Режим доступу: http://pidruchniki.com/component/option,com_jdownloads/Itemid,999999/catpid,349/task,view.annotation.

14. Світлична В.Ю. Інформаційна безпека: багатогранність сутності, види загроз та шляхи забезпечення / В.Ю. Світлична, Т.І. Світлична // Науково-технічний збірник. – 2013. – № 109. – с. 360-369.

15. Юдін О.К. Концептуальна модель інформаційної безпеки державних інформаційних ресурсів / О.К. Юдін // Наукоємні технології. – 2014. – № 4 (24). – с. 462-467.

16. Корченко О.Г. Ознаковий принцип формування класифікацій кібератак / О.Г. Корченко, Є.В. Паціра, С.О. Гнатюк, В.М. Кінзерявий, С.В. Казмірчук // Вісник Східноукраїнського національного університету імені Володимира Даля. – №1, 2010. – С. 32-38.

17. Гавриш С.Б. Комп’ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії / С.Б. Гавриш // Боротьба з організованою злочинністю і корупцією (теорія і практика) [Електронний ресурс]. –

Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/bozk/2009_20/20text/g20_01.htm

18. Климчик О.О. Кримінально-правова кваліфікація використання комп'ютерних технологій для вчинення терористичних актів / О.О. Климчик, Р.М. Кравченко // Інформаційна безпека людини, суспільства, держави. – №1 (3), 2010. – С. 26-30.

19. Довгань О.Д. Кібертероризм як загроза інформаційному суверенітету держави / О.Д. Довгань, В.Г. Хлань // Інформаційна безпека людини, суспільства, держави. – №3 (7), 2011. – С. 49-53.

20. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення: підруч. / О.К. Юдін. – К.: НАУ, 2011. – 640 с.

21. Закон України «Про національну програму інформатизації» // Відомості Верховної Ради України (ВВР), 1998, N 27-28, ст.181.

22. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» // Відомості Верховної Ради України (ВВР), 2007, № 12, ст.102.

23. Закон України «Про національну безпеку України» // Відомості Верховної Ради (ВВР), 2018, № 31, ст.241.

24. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 року № 96/2016 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/96/2016.

25. Закон України «Про телекомунікації» // Відомості Верховної Ради України (ВВР), 2004, № 12, ст.155.

26. Закон України «Про засади внутрішньої і зовнішньої політики» // Відомості Верховної Ради України (ВВР), 2010, № 40, ст.527.

27. Закон України «Про об'єкти підвищеної небезпеки» // Відомості Верховної Ради України (ВВР), 2001, N 15, ст.73.

28. Казакова Н.Ф. Принципи побудови захищених інтелектуальних мереж / Н.Ф. Казакова // Вісник ДУІКТ. – К.: ДУІКТ. – 2009. – № 4. – С. 381–388.

29. Казакова Н.Ф. Аналіз розвитку сучасних напрямів інформаційної безпеки автоматизованих систем / О.О. Скопа, Н.Ф. Казакова // Системи обробки інформації. – Харків: ХУПС ім. І. Кожедуба. – 2009. – № 7(79). –С.48–54.

30. Ткачук М. В. Розробка методики комплексної оцінки ефективності впровадження систем управління IT-інфраструктурою організацій / М.В. Ткачук, В.Є. Сокол, О.В. Черкашенко // Вісник Національного технічного університету «ХПІ». – Харків: НТУ «ХПІ». – 2012. – № 30. – С.94–104.

31. Goel S. Information security risk analysis a matrix-based approach / S. Goel, V. Chen // UniverSUNY, 2005.

32. Laqueur W. New terrorism / NY., Oxford: Oxford University Press, 1977. – 290 p.

33. Пилипчук В.Г. Запобігання інформаційній безпеці України: сучасні тенденції та проблеми / В.Г. Пилипчук // Матеріали наук.-практ. конф. (6 жовтня 2016 р.). – К.: НТУУ «КПІ імені Ігоря Сікорського», Вид-во Політехніка, 2016. – С. 24–28.

34. Діордіца І.В. Поняття та зміст кібертероризму [Електронний ресурс]. – Режим доступу: http://goal-int.org/ ponyattya-ta-zmist-kiberterorizmu.

35. Бойченко О.В. Медіа-тероризм: особливості сучасних ознак інформаційній безпеці / О.В. Бойченко // Інтегровані інтелектуальні робототехнічні комплекси (ПРТК-2009): друга міжнародна наук.-практ. конф. (25–28 травня 2009 р.). – К.: НАУ, 2009. – С. 230–232.

36. Конвенція про кіберзлочинність: за станом на 7 вересня 2009 р. [Електронний ресурс] // Офіційний веб- портал Верховної Ради України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_575

37. Глазов О. В. Міжнародний інформаційний тероризм в контексті загроз національній безпеці України / О.В. Глазов [Електронний ресурс]. – Режим доступу: http://lib.chdu.edu.ua/ pdf/naukpraci/politics/2012/197–185–15.pdf

38. Яцик Т.П. Особливості інформаційного тероризму як одного із способів інформаційної війни / Т.П. Яцик // Науковий вісник Національного університету державної податкової служби України (економіка, право). – 2014. – № 2. – С. 55–60.

39. Гавриш С.Б. Комп'ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії / С.Б. Гавриш // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2009. – № 20.

40. Медіа-тероризм серед інших видів тероризму: спроба типологічного аналізу / Тетяна Єрохіна [Електронний ресурс]. – Режим доступу: http://www.social-science.com.ua/article/1002

41. Смачило Т.В. Феномен інформаційного тероризму як загрози міжнародній безпеці / Т.В. Смачило, А.Р. Кривцун // Молодий вчений. – 2017. - № 11 (51). – с. 124-127.

42. Методичні рекомендації щодо розрахунку рівня економічної безпеки України, затверджені наказом Міністерства економічного розвитку і торгівлі України 29.10.2013 № 1277 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/rada/show/v1277731-13.

43. Богдан Н. М. Оцінювання рівня фінансово-економічної безпеки регіонів України: методологія і практика // Проблеми економіки. – 2018. – №1. – С. 142–149.

44. Вахлакова В. В. Економічна безпекологія: становлення науки // Проблеми економіки. - 2017. - №1. - С. 290-290.

45. Веретенников В. І., Тарасенко Л. М, Гевлич Г. І. Управління проектами: навч. посібн. - К.: ЦУЛ, 2006. - 280 с.

46. Ілляшенко О. В. Механізми системи економічної безпеки підприємства: монографія. - Харків: Мачулін, 2016. - 504 с.

47. Резніков О. Л. Забезпечення соціально-економічної безпеки регіону – нагальне завдання сьогодення // Економіка промисловості. – 2008. – № 1. – С. 78-82.

48. Диба М.І., Гернего Ю.О. Діджиталізація економіки: світовий досвід та можливості розвитку в Україні // «Фінанси України». – №7. –2018. – С. 50-63.

49. Harnessing the Power of Connectivity. URL: http:// www.huawei.com/minisite/gci/files/gci_2021_whitepaper_n.pdf?v=20170421.

50. Правове забезпечення здійснення державної політики з реконструкції економіки : монографія / за заг. ред. В.А. Устименка; НАН України, Ін-т економіко-правових досліджень. Чернігів : Десна Поліграф, 2016. - 160 с.

51. The Rise of Digital Challengers. Digital / McKinsey. URL: https://digitalchallengers.mckinsey.com/

52. Туль С.І. Трансформація світового ринку праці в умовах діджиталізації: дис. на здоб. наук. ступ. канд. екон. наук. – Вінниця. – 2019. – 279 с.

53. Digital America: a tale of the haves and have-mores / J. Manyika et al. McKinsey & Company. URL: URL: https://www.mckinsey.com/~/media/McKinsey/Industries/High%20Tech/Our%20Insights/Digital%20America%20A%20tale%20of%20the%20haves%20and%20have%20mores/Digital%20America%20Full%20Report%20December%202015.ashx

54. Digital Europe: pushing the frontier, capturing the benefits / J. Bughin et al. McKinsey & Company. URL: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20Europe%20Pushing%20the%20frontier%20capturing%20the%20benefits/Digital-Europe-Fullreport-June-2021.ashx

55. International Digital Economy and Society Index 2021. – SMART 2020/0052. Luxembourg : Publications Office of the European Union., 2021. URL: https://ec.europa.eu/digital-single-market/en/news/international-digital-economy-andsociety-index-2021

56. The ICT Development Index (IDI): conceptual framework and methodology. ITU. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2021/methodology.aspx

57. Measuring the Information Society Report. ITU iLibrary. URL:https://www.itu-ilibrary.org/science-and-technology/measuring-the-information-societyreport_pub_series/76a34020-en

58. Maximizing the impact of digitization / PWC. URL: https://www.strategyand.pwc.com/media/file/Strategyand_Maximizing-the-Impact-of-Digitization.pdf.

59. Human Development Report 2021. // Human Development for Everyone. N. Y. : UNDP, 2016. 286 p.

60. World Bank Open Data. Free and open access to global development data. URL: http://data.worldbank.org/.

61. Коломієць Г.М., Глушач Ю.С. Цифрова економіка: контроверсійність змісту і впливу на господарський розвиток. // Бізнес Інформ. – 2017. – № 7. – С. 137–143.

62. Туль С.І. Сучасні методики інтегральної оцінки діджиталізації світової економіки та ринку праці. // Причорноморські економічні студії. – 2019. – Вип. 42. – С. 12–18.

63. Данніков О.В., Січкаренко К.О. Концептуальні засади цифровізації економіки України // Економіка та управління національним господарством. 2018. – Вип. 17. – С. 73-79.

64. Краус Н.М., Голобородько О.П., Краус К.М. Цифрова економіка: тренди та перпективи авангардного характеру розвитку // Ефективна економіка. 2018. № 1. URL: http://ojs.dsau.dp.ua/index.php/efektyvna-ekonomika/article/viewFile/997/862.

65. Управління економічної безпекою: підручник / Козаченко Г.В., Онищенко С.В., Завора Т.М.; за ред. В.О. Онищенка та Г.В. Козаченко. – Полтава: ПолтНТУ ім. Ю. Кондратюка, 2018. – 530 с.

66. Onyshchenko, S., Yanko, A., Hlushko, A., Sivitska, S. Increasing Information Protection in the Information Security Management System of the Enterprise. In: Onyshchenko V., Mammadova G., Sivitska S., Gasimov A. (eds) Proceedings of the 3rd International Conference on Building Innovations. ICBI 2020. Lecture Notes in Civil Engineering. Springer, Cham. Volume 181, 725-738 (2020). https://doi.org/10.1007/978-3-030-85043-2_67

67. Пилипчук В.Г. Теоретичні та державно- правові аспекти протидії інформаційному тероризму в умовах глобалізації / В.Г. Пилипчук, О.П. Дзьобань // Стратегічна пріоритети. – №4 (21), 2011. – С. 12-17.

68. Onyshchenko S., Yanko A., Hlushko A., Sivitska S. Conceptual principles of providing the information security of the national economy of Ukraine in the conditions of digitalization. *International Journal of Management (IJM).* 2020. Volume 11, Issue 12. P. 1709-1726. DOI: 10.34218/IJM.11.12.2020.157

69. Юдін О.К. Правові аспекти формування системи державних інформаційних ресурсів / О.К. Юдін, С.С. Бучик // Безпека інформації. –2014. – Т. 20 (1) / Технічні науки. – С. 76–82.

70. Бажал Ю. Інформаційна економіка / В кн.: Роль інформації у формуванні ринкової економіки: Монографія / Ю. Бажал, В. Бакуменко, І. Бондарчук та ін.; За заг. ред. І. Розпутенка. – К.: Вид-во «К.І.С.», 2004. – С. 33-57.

71. Барановський О.І. Фінансова безпека в Україні (методологія Оцінки та механізми забезпечення) / О.І. Барановський / Київ, нац. торг.-екон. ун-т. – К.: 2004 – 759 с.

72. Білорус О.Г. Глобальные трансформации и стратегии развития / О.Г. Білорус, Д.Г. Лук'яненко и др. // Монографія. – К. – 2000. – 424 с.

73. Бандурка О.М. Основи економічної безпеки: підруч. / О.М. Бандурка, В.Є. Духов, К.Я. Петрова, І.М. Червяков. – Харків: Вид-во Нац. ун-ту внутр. справ, 2003. – 236 с.

74. Варналій З.С. Тіньова економіка: сутність, особливості та шляхи легалізації / Варналій З.С. та інші / За ред. З.С. Варналія. – К.НІСД. 2006. – 576 с.

75. Власюк О.С. Теорія і практика економічної безпеки в системі науки про економіку / Власюк О.С. // Наук. доповідь. – К.: НІПМБ, 2008. – 48 с.

76. Державна служба статистики України [Електронний ресурс]. – Режим доступу: http://ukrstat.gov.ua/

77. Економічна безпека України: сутність і напрямки забезпечення / В.Т. Шлемко, І.Ф. Бінько: Монографія. – К.: НІСД, 1997. – 144 с. (Сер. «Нац. безпека»; Вип. 2).

78. Єрмошенко М.М. Фінансова безпека держави: національні інтереси, реальні загрози, стратегія забезпечення. – К.: Київ. нац. торг-екон. ун-т, 2001. – 268 с.

79. Іляш О.І. Структурно-інституціональні трансформації та економічна безпека держави / О.І. Іляш: монографія / [за ред. О.С. Власюка, А.І. Мокія]. – Львів: Апріорі, 2012. – 836 с.

80. Кириченко О.А. Економічна безпека суб'єктів зовнішньоекономічної діяльності України в умовах фінансової кризи. Експертно–аналітична доповідь / О.А. Кириченко, О.В. Конончук, В.Д. Кудрицький та інші. – К.: УЕП «КРОК», 2009. – 760 с.

81. Кизим М.О. Моделювання економічної безпеки: держава, регіон, підприємство / В.М. Геєць, М.О. Кизим, Т.С. Клебанова, О.І. Черняк та ін.: Монографія; за ред. В.М. Гейця. – ВД «ІНЖЕК», 2006. – 240 с.

82. Корнейчук Б.В. Информационная экономика / Б.В. Корнейчук. – СПб.: Питер, 2006. – 400 с.

83. Микитенко В.В. Экономическая безопасность государства и информационно–технологические аспекты её обеспечения: [монография] / [Д.А. Андреєв, О.А. Веклич, В.В. Микитенко та ін.]; під заг. ред. Г.К. Вороновського. – К.: Знания Украины, 2005. – 664 с.

84. Методичні рекомендації щодо розрахунку рівня економічної безпеки України, затв. Наказом Міністерства економічного розвитку і торгівлі України 29.10.2013 N 1277 [Електронний ресурс]. – Режим доступу: http://cct.com.ua/2013/29.10.2013_1277.htm.

85. Мунтіян В.І. Економічна безпека України [Текст]: монографія / В.І. Мунтіян. – К.: Вид-во КВІЦ, 1999. – 464 с.

86. Браун П. Посібник з аналізу державної політики / П. Браун; [пер. з англ.]. – К.: Основи, 2000. – 243 с.

87. Буркальцева Д.Д. Суб'єктно-інституційне забезпечення економічної безпеки держави / Д.Д. Буркальцева // Вісник Чернівецького торгівельно-економічного інституту. – Чернівці: ЧТЕІ КНТЕУ, 2012. – Вип. II (46). Економічні науки. – С. 121 – 127.

88. Економічна криза в Україні: виміри, ризики, перспективи / [Я.А. Жаліло, О.С. Бабанін, Я.В. Белінська та ін.]; відп. ред. Я.А. Жаліло. – К.: НІСД, 2009. – 142 с.

89. Економічна теорія (Політекономія. Мікроекономіка. Макроекономіка). Навч. посібник / Л.В. Білецька, О.В. Білецький, В.І. Савич. – [2-ге вид. перероб. та доп.]. – К.: Центр учбової літератури, 2009. – 688 с.

90. Жалило Я. Экономическая стратегия государства: теория, методология, практика. Монография / Я. Жалило. – К.: НИСИ, 2003. – 368 с.

91. Інструментарій впливу громадських рад на процес реалізації державної політики на місцевому рівні: навчальний посібник / Буковинська фундація підтримки регуляторної реформи в Україні. – Чернівці, 2011. – 160 с.

92. Кравцова Т.М. Правові форми залучення громадськості до регуляторної діяльності державних установ у сфері господарської діяльності / Т.М. Кравцова // Підприємництво, господарство і право: наук.-практ. господарсько-прав. журн. – К.: Ін Юре, 2004. – Вип. 4. – С. 3 – 6.

93. Літвінов О. В. Проблеми забезпечення участі громадськості у здійсненні державної регуляторної політики / Літвінов О.В. // Актуальні

проблеми державного управління: зб. наук. пр.; голов. ред. С.М. Серьогін. – Д., 2006. – Вип. 1 (23). – С. 108 – 120.

94. Норт Д. Інституції, інституційна зміна та функціонування економіки / Д. Норт. – К.: Основи, 2000. – 198 с.

95. Онищенко В.О. Концептуально-методичні засади оцінки рівня економічної безпеки держави / Онищенко В.О., Онищенко С.В., Мирошніченко В.В. // Вісник економіки транспорту і промисловості. – Х.: ХНЕУ, 2012. – № 38. – С. 102–108.

96. Скрипничук Т. Запровадження проектів електронного врядування в процесі реалізації державної регуляторної політики / Т. Скрипничук // Ефективність державного управління: зб. наук. пр.; за заг. ред. П.І. Шевчука. – Львів: ЛРІДУ НАДУ, 2009. – Вип. 20. – С. 236 – 244.

97. Новикова О.Ф. Економічна безпека: концептуальне визначення та механізм забезпечення / О.Ф. Новікова, Р.В. Покотиленко; [наук. ред. О.І. Амоша]; ПАН України, Ін-т економіки пром-сті. – Донецьк, 2006. – 407 с.

98. Наумік-Гладка К.Г. Проблеми забезпечення економічної безпеки держави в умовах становлення інформаційної економіки / К.Г. Наумік-Гладка // Глобальні та національні проблеми економіки. – 2015. – №6. – С. 206–209 [Електронний ресурс]. – Режим доступу: http://global-national.in.ua/issue-6-2015.

99. Наумік-Гладка К.Г. Державне регулювання розвитку сфери комунікаційної діяльності в системі економічної безпеки України / К.Г. Наумік-Гладка // Проблеми економіки. – 2015. – № 2. – С. 87–92.

100. Осовська Г.В. Комунікації в менеджменті / Г.В. Осовська. – К.: Кондор, 2003. – 218 с.

101. Форми та методи залучення громадськості: Навч. посіб. / Інститут громадянського суспільства; за заг. Ред. В. Артеменка. – К.: ІКЦ «Леста», 2007. – 240 с.

102. Загрози безпеці України та інших країн регіону Східного партнерства й можливі відповіді на них: результати експертного опитування.

URL: http://eesri.org/wp-content/uploads/2018/01/2018-01_Ukraine-EaP-security_Expert-survey-EESRI_UKR.pdf

103. Романов В. Аналіз політики як інструмент ефективного державного управління // Актуальні проблеми державного управління: Зб. наук. Праць ДФ УАДУ. – 2000. – № 3. – С. 18-26.

104. Онищенко С.В., Глушко А.Д. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. Економіка і регіон. 2022. № 1 (84). С. 13-20.

105. Юлдашев О.О. Адміністративно-правове забезпечення права громадських організацій на доступ до інформації і державна регуляторна політика / О.О. Юлдашев // Наше право. – К.: спец. в-во «Юнеско», 2011. - № 2. – Ч.1. – С. 70 – 74.

106. Конвенція про кіберзлочинність Конвенцію ратифіковано із застереженнями і заявами Законом N 2824-IV (2824-15) від 07.09.2005, ВВР, 2006, N 5-6, ст.71 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_575.