МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІВЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА

Факультет історії, політології та міжнародних відносин
Кафедра міжнародних відносин та суспільних комунікацій

СИСТЕМА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ, СУСПІЛЬСТВА І ДЕРЖАВИ

Кваліфікаційна робота
Рівень вищої освіти – другий (магістерський)

Виконав:
студент 6 курсу, 604 групи
Терновецький Дмитро Андрійович
Керівник:
кандидат політичних наук,
доцент **Осадца І.С.**

До захисту допущено
на засіданні кафедри
протокол ___від _____2023р.
Заф.кафедрою_____проф. Макар В.Ю.

Чернівці – 2023

Анотація

Магістерська робота присвячена дослідженню системи захисту персональних даних в контексті забезпечення інформаційної безпеки людини, суспільства і держави.

Автор розглянув суть, значення та методологічні підходи інформаційної безпеки особистості, суспільства та держави, загрози, що можуть виникати в системі захисту персональних даних та способи їх уникнення. У роботі також висвітлено сучасний стан забезпечення інформаційної безпеки людини, суспільства і держави, в тому числі охарактеризовані основні види інтернет-шахрайства та методи їх недопущення. Дослідник в роботі зосередив увагу на напрямках вдосконалення системи захисту персональних даних на основі зарубіжного досвіду у сфері інформаційної безпеки. Важливим аспектом в забезпеченні інформаційної безпеки є формування культури в даній галузі в умовах глобальної цифрової трансформації.

Ключові слова: персональні дані, захист персональних даних, інформаційні загрози, інформаційна безпека, держава, суспільство, особистість.

Summary

The master's thesis is devoted to the study of the personal data protection system in the context of ensuring the information security of a person, society and the state.

The author considered the essence, significance and methodological approaches of information security of the individual, society and the state, the threats that may arise in the personal data protection system and ways to avoid them. The work also highlights the current state of ensuring information security of a person, society and the state, including the main types of Internet fraud and methods of preventing them. In this work, the researcher focused on areas of improvement of the personal data protection system based on foreign experience in the field of information security. An important aspect in ensuring information security is the formation of culture in this field in the conditions of global digital transformation.

Keywords: personal data, protection of personal data, information threats, information security, state, society, personality.

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів наукових досліджень інших авторів мають посилання на відповідне джерело.

_____

ЗМІСТ

ВСТУП

В сучасному світі цифровізація набуває дедалі більших масштабів і проникнення у різні сфери та галузі суспільного життя, реципієнти інформації повинні володіти необхідними знаннями та навичками для захисту своїх персональних даних від потенційних зловмисників. Адже деякі фізичні особи, надаючи свої персональні дані, навіть не замислюються, що отримувачі інформації (компанії, установи чи організації) можуть порушувати національне законодавство і міжнародне право, які регулюють питання захисту персональних даних. Водночас актуальним є і вдосконалення відповідної нормативної бази, щоб її зміст не відставав від стрімких тенденцій цифровізації світової спільноти. Саме тому потрібно розуміти свої права, які в майбутньому дозволять обґрунтовано та якісно відстоювати свої інтереси в разі несанкціонованого доступу сторонніх осіб до особистих даних, в разі питань, пов’язаних з державною безпекою, боротьбою зі злочинністю та для запобігання правопорушень. Відтак важливим моментом є забезпечення інформаційної безпеки особистості, суспільства та держави.

У зв’язку з широким використанням інформаційно-комунікаційних технологій все більшого значення набуває недобросовісне використання таких технологій, що в результаті призводить до порушення прав людини, що може шкодити у різних масштабах. В Україні це особливо актуально, зважаючи на ворожі інформаційні процеси, які широко використовує Російська Федерація з метою деструктивних впливів на наше суспільство і державу.

Зважаючи на глобальний контекст і реалії воєнного сьогодення України, виникає нагальна потреба проведення якісного і комплексного співвідношення інформаційної безпеки і прав людини. Вагомою проблемою в захисті персональних даних також є неможливість забезпечення захисту інформації при широкому використанні суб’єктів такої інформації на

Інтернет-ресурсах. Адже щойно фізичні особи публікують свої дані у глобальній павутині, вони одразу стають публічними, а відтак – дозвіл на їх використання третіми особами, у багатьох випадках, не потрібен.

З огляду на недосконаліть системи захисту персональних даних в епоху триваючого розвитку цифрових технологій, які неминуче фундаментально впливають на життя кожної людини, навіть якщо вона того не бажає, актуальним питанням є убезпечення від інформаційних загроз як окремого громадянина, так і держави в цілому. Питання інформаційної безпеки та захисту персональних даних були висвітлені в працях як вітчизняних, так і зарубіжних науковців, таких як О. Гронь, О. Бернадзюк, М. Рощук, А. Гордієнко, Я. Малик, О. Береза, В. Брижко, Г. Линник, Г. Одерман, які досліджували інформаційну безпеку, захист персональних даних в публічному управлінні та її правові аспекти.

Метою роботи є вивчення та аналіз стану забезпечення інформаційної безпеки особистості, суспільства та держави, напрямів вдосконалення управління інформаційною безпекою на всіх трьох рівнях та застосування зарубіжного досвіду з даного питання в Україні.

Завданнями магістерської роботи є:

– охарактеризувати сутність персональних даних, інформаційної безпеки, їх трактування з різних точок зору та їх значення, функції;

– вказати інформаційні загрози, їх види, фактори з урахуванням Стратегії інформаційної безпеки;

– визначити методологічні підходи щодо забезпечення інформаційної безпеки;

– визначити правила, рекомендації щодо роботи в Інтернеті, в тому числі в соціальних мережах, в електронному листуванні та в органах державної влади;

– пояснити суть та значення банківської таємниці, а також чітко визначити правила зберігання, захисту та використання банківської таємниці;

– проаналізувати досвід країн Європейського Союзу та інших високо розвинутих країн в сфері інформаційної безпеки;

– сформувати перспективні напрямки вдосконалення системи захисту персональних даних.

Об’єктом дослідження є інформаційна безпека особистості, суспільства та держави.

Предметом дослідження є система захисту персональних даних в контексті забезпечення інформаційної безпеки людини, суспільства і держави.

Методологія магістерської роботи включає використання наукових методів, зокрема – методи аналізу, синтезу й узагальнення, що дозволило комплексно вивчити досліджувану тематику та отримати чіткі результати.

В роботі застосовано два фундаментальних наукових підходи: системний – з метою аналізу інформаційної сфери як цілісної системи, елементи якої взаємопов’язані та взаємозалежні; та структурно-функціональний, за допомогою якого автор досліджував обраний предмет крізь призму погляду на систему захисту персональних даних в контексті інформаційної безпеки як структуру з чітко вираженим функціоналом. Наукова новизна в даній роботі полягає у спробі пошуку автором оптимальних методів управління інформаційною безпекою та їх застосування в Україні на основі зарубіжного досвіду.

Структура та обсяг роботи. Магістерська робота складається зі вступу, трьох розділів, які поділені на три підрозділі в кожному з розділів, висновків, списку використаної літератури, анотацій українською та англійською мовами. Загальний осяг роботи становить 122 сторінок, 9 таблиць, 7 рисунків, в тому числі список використаної літератури складається з 126 найменувань.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ СИСТЕМ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ, СУСПІЛЬСТВА І ДЕРЖАВИ

1.1. Суть та значення інформаційної безпеки людини, суспільства і держави

Завдяки стрімкому розвитку інформаційних технологій доступ до каналів комунікації мають не лише організації, держава в загальному, а й окрема фізична особа, яка може створювати та поширювати власні повідомлення, що будуть доступні необмеженій кількості користувачів. В сучасному світі, де розвинена цифровізація, суб'єкти інформації повинні розуміти коло своїх користувачів для захисту своїх даних та непоширенню їх зловмисникам. Адже деякі фізичні особи, надаючи свої персональні дані, навіть не замислюються, що користувачі інформації (компанії чи організації) порушують законодавство, яке регулює питання захисту персональних даних. Саме тому потрібно розуміти свої права, які в майбутньому дозволять обґрунтовано та якісно відстоювати свої інтереси в разі несанкціонованого доступу сторонніх осіб до особистих даних, в разі питань, пов'язаних з державною безпекою, боротьбою зі злочинністю та для запобігання правопорушень.

Так, відповідно до Закону України «Про захист персональних даних» персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [75]. Тоді як захист персональних даних можна трактувати як сукупність організаційно-правових та технічних заходів, які спрямовані на недопущення неправомірних дій із забезпеченням конфіденційності персональних даних, який прямо пов'язаний з питанням інформаційної безпеки кожного громадянина та держави в цілому.

Відповідно до статті 32 Конституції України ніхто не може зазнавати втручання в його особисте та сімейне життя; не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, і лише в інтересах національної безпеки, економічного добробуту й прав людини [37].

Для кращого сприйняття поняття інформаційної безпеки розглянемо історичні періоди становлення та розвитку системи персональних даних та позитивні та негативні моменти на кожному з етапів (табл. 1.1).

Таблиця 1.1

Хронологія подій процесу становлення та розвитку персональних даних

Етапи становлення	Характеристика
I етап	Переваги: 1996-1998 рр. - підготовка першої версії та восьми наступних версій Закону України «Про захист персональних даних» [4], які вдосконалювалися з кожним роком і, як наслідок, остаточна версія 27 грудня 1998 року була направлена до Кабінету Міністрів України. Недоліки: - відсутність послідовності та системності в організації роботи у зв'язку зі зміною виконавців та керівництва державних структур та незнанням працівників предмета законопроекту та мети суспільних відносин; - неврахування положень Конвенції Ради Європи та статті 3 Конституції України щодо законності збирання та реалізації даних [9, с. 36].
II етап	Переваги: до липня 2000 року Закон України «Про захист персональних даних» був погоджений Міністерством фінансів України, Міністерством економіки, Міністерством освіти і науки, Міністерством внутрішніх справ, Міністерством закордонних справ, при цьому повторно законопроект був поданий на розгляд Кабінету Міністрів України та завдяки діючим народним депутатам даний закон було зареєстровано у Верховній Раді України та розглянуто в першому читанні
III етап	Переваги: створення в 2005 році робочої групи з представників Міністерства юстиції України та підготовки ними альтернативного законодавчого акту Закону України «Про захист персональних даних» Недоліки: вищезазначений нормативно-правовий акт було не прийнято та скасовано з причини невідповідності нормам європейського законодавства.
IV етап	Переваги: 16 березня 2006 року підтримка законопроєкту щодо захисту персональних даних 287 народними депутатами та прийняття закону в другому читанні, основною метою якого був захист приватного життя людини в умовах інформаційних технологій.

	Недоліки: Президент України наклав «вето» на законопроєкт щодо захисту персональних даних у зв'язку з непідтримкою працівників Міністерства юстиції України норми щодо «права власності людини на свої персональні дані».
V етап	Переваги: для зміни законопроєкту щодо захисту персональних даних щодо вилучення норми стосовно «права власності людини на свої персональні дані» було створено робочу групу Верховною Радою України, що в результаті сприяло підтримці даного акту 329 народними депутатами. Недоліки: в черговий раз проєкт Закону України «Про захист персональних даних» був повернутий на доопрацювання у зв'язку з невідповідністю проєкту статті 32 Конституції України та міжнародно-правовим актам, що полягає в конфіденційності інформації про особу.
VI етап	Переваги: за пропозиціями народних депутатів у 2008 році був зареєстрований новий законопроєкт щодо захисту персональних даних та в 2009 році прийнятий Верховною Радою України у першому читанні, а вже 1 червня 2010 року як Закон, який набрав чинності з 01.01.2011 року.
VII етап	Переваги: протягом наступних 2011-2016 років відбулися значні зміни до закону: було створено Державну службу України з питань захисту персональних даних, Департамент з питань захисту персональних даних, що входив до складу Секретаріату Уповноваженого Верховної Ради України з прав людини; було розширено повноваження «Омбудсмена» щодо надання права на здійснення перевірок та визначення порядку їх проведення [66, с. 39] кримінальних покарань, а також про вільне переміщення таких даних»

Джерело: складено автором на основі [4, 9, 66]

Відповідно до табл.1.1. бачимо, що законодавство в сфері захисту персональних даних мало значний розвиток і проходило декілька етапів на правомірність, затвердження та використання різноманітними верствами населення, державою чи підприємствами. На сьогоднішній день система захисту персональних даних з урахуванням законодавства та інших нормативно-правових актів виглядає наступним чином (рис. 1.1).

Інформаційна безпека – це життєво важлива складова національної безпеки, яка спрямована на забезпечення національних інтересів, та є самостійною складовою частиною поряд з інформаційними ресурсами, інформаційною структурою та інформаційними технологіями. На інформаційну безпеку впливають як ендогенні, так і екзогенні фактори, такі

як: економічний, соціальний та інформаційний стан країни, політична ситуація в країні.

Рис. 1.1. Система захисту персональних даних

Джерело: складено автором на основі [75]

Інформаційну безпеку можна розглядати як:

– як складову національної безпеки;

– як стан захищеності інформаційного середовища, в тому числі національних інтересів від можливих загроз [6, с.44];

– як стан держави, що забезпечує національну безпеку країни в цілому [7, с..97].

Інтереси особи в інформаційній сфері полягають в:

– забезпеченні вільного доступу до відкритої інформації, її правдивості, реалізації конституційних прав людини на доступ до інформації;

– забезпеченні захищеності конфіденційної інформації громадян відповідно до юридичних норм.

Інтереси суспільства в інформаційній сфері передбачають:

– створення правової соціальної демократії;

– досягнення та підтримка суспільного спокою;

– зміцнення демократії; забезпечення інтересів громадян.

Інтереси держави в інформаційній сфері зводяться до наступних пунктів:

– створення умов для розвитку державної інфраструктури;

– створення умов для реалізації конституційних прав і свобод людини і громадянина в сфері забезпечення суверенітету та територіальної цілісності держави, економічної, соціальної та політичної стабільності;

– забезпечення законності та правопорядку;

– розвиток та проведення міжнародного співробітництва.

Національна безпека України в інформаційній сфері включає персональну, суспільну, комерційну та державну безпеки.

Далі розглянемо поняття «інформаційна безпека» з точки зору різноманітних дослідників (табл. 1.2).

Як бачимо з табл. 1.2 дослідники мають схожу думку щодо визначення інформаційної політики і трактують, що система забезпечення інформаційної безпеки складається з таких елементів:

– суб’єкти безпеки – особистості, організації, підприємства, державні інститути, що забезпечують безпеку об’єкта при виконанні практичних дій та введенні їх в дію;

– об’єкти безпеки – це те, на що спрямована дія суб’єкта /безпеки (економіка держави або конкретного регіону, галузі народного господарства, особистості, фірми чи підприємства);

– механізм забезпечення безпеки – алгоритм дій та їх обґрунтування щодо забезпечення національної безпеки.

Таблиця 1.2

Дефініція поняття «інформаційна безпека»

Науковець	Визначення
В. С. Цимбалюк, А. В. Бабінської [105, с.23]	Стан захищеності держави, її національних інтересів в інформаційній сфері, які визначаються сукупністю збалансованих інтересів особи, суспільства і держави
Л. О. Кочубей [39, с.221-222]	Стан захищеності життєво важливих інтересів особи, суспільства, за якого жодні інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб’єктів
В. В. Шемчук [110, с. 34]	Правовідносини, які виникають під час здійснення превентивних і захисних заходів в інформаційному середовищі людини, суспільства і держави
О. А. Ніщименко [52, с.19]	Стан захищеності національних інтересів в інформаційній сфері, що складаються з сукупності збалансованих інтересів особи, суспільства та держави від внутрішніх і зовнішніх загроз, що відповідає принципу забезпечення національної безпеки інформаційній сфері

Джерело: створено автором на основі [105, 39, 110, 52]

В усі часи питання інформаційної безпеки займало важливе місце як в житті окремого громадянина, так і в державі в цілому. Саме тому потрібна ефективна система заходів щодо забезпечення інформаційної безпеки для попередження, виявлення потенційних загроз національним інтересам та в результаті запобігання збиткам у соціально-економічній сфері. Указом Президента України Про рішення національної безпеки і оборони України

«Про Стратегію інформаційної безпеки» від 28 грудня 2021 року визначено, що метою Стратегії є посилення спроможності забезпечення інформаційної безпеки держави, підтримка соціальної та політичної стабільності, захист державного суверенітету, оборона держави, забезпечення територіальної цілісності України та захист прав свобод кожного громадянина країни [84].

Відповідно до Указу Президента України Про рішення національної безпеки і оборони України «Про Стратегію інформаційної безпеки» цілями реалізації Стратегії інформаційної безпеки є:

1) протидія дезінформації, зокрема держави-агресора, що проявляється в порушенні суверенітету та територіальної цілісності, ліквідації незалежності, вчиненні терористичних актів, посяганні на права і свободи людини;

2) забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності;

3) підвищення рівня медіаграмотності та медіакультури суспільства;

4) забезпечення дотримання прав особи на збирання, зберігання, використання та поширення інформації; захисту приватного життя; доступу

5) до достовірної інформації; свободи у вираженні своїх поглядів на ті чи інші питання; захисту прав журналістів, гарантії їх безпеки та найголовніше – протидії поширенню незаконного контенту;

6) інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих та на прилеглих до них територіях України, до загальноукраїнського інформаційного простору;

7) створення ефективної системи стратегічних комунікацій, метою якої є гарантування ефективної комунікації між органами державної влади, органами місцевого самоврядування та суспільством;

8) розвиток інформаційного суспільства та підвищення рівня культури діалогу [84].

Для виконання вищезазначених цілей ставляться такі завдання:

– створення системи протидії дезінформації, що дозволяє запобігати, видко виявляти та реагувати державі та суспільству на інформаційні загрози,

а також вжиття заходів щодо запобігання та протидії поширенню дезінформації, в тому числі відповідальність за поширення неправдивої інформації;

– розвиток спроможностей складових сил оборони щодо протидії загрозам в інформаційному просторі та проведення силами оборони операцій та заходів, що дають змогу дати відсіч агресії Російської Федерації проти України;

– проведення заходів щодо недопущення розміщення забороненої законом інформації в мережі Інтернет, в тому числі заборона розповсюдження та показу інформаційної продукції, заборона проведення будь-яких заходів, які пов’язані з популяризацією держави-агресора, створенням позитивного образу держави-агресора, вчиненням терористичних актів;

– ефективна взаємодія всіх залучених осіб, пов’язаних із забезпеченням інформаційної безпеки при реалізації державної політики в інформаційній сфері;

– забезпечення використання державної мови в усіх сферах на всій території України;

– забезпечення розвитку українського кіно, теле- і радіо продукції;

– підтримка вітчизняного книговидання;

– сприяння вільному використанню та захисту мов національних меншин, а також вивчення іноземних мов, які є міжнародними;

– зміцнення зв’язків з українською діаспорою, що дасть змогу зберегти етнокультурну ідентичність;

– залучення ветеранів війни для забезпечення національної безпеки і оборони;

– проведення тренінгів з медіаграмотності, що забезпечує розвиток критичного мислення, навчання щодо визначення маніпуляційних технік, знання в сфері інтернет-технологій;

– стимулювання розвитку соціально відповідального бізнесу серед засобів масової інформації;

– внесення змін в законодавстві у сфері реклами щодо посилення відповідальності за показ прихованої реклами;

– внесення змін в законодавстві щодо вдосконалення доступу до публічної інформації відповідно до норм міжнародних актів;

– вдосконалення нормативних актів щодо захисту персональних даних та забезпечення їх реалізації [84];

– захист журналістів та їх сімей при провадженні професійної діяльності та внесення змін щодо цього в законодавстві;

– захист українського інформаційного простору від несанкціонованої інформації;

– забезпечення прав і свобод військовослужбовців та інших представників, які захищають Україну;

– забезпечення громадянами України підтримки відновлення територіальної цілісності України;

– збільшення та поширення частки українського інформаційного простору на тимчасово окупованих територій;

– визначення системи взаємодії щодо питання реагування на кризову ситуацію;

– вдосконалення взаємодії між органами державної та виконавчої влади, обласними державними адміністраціями, громадськістю щодо встановлення єдиної позиції стосовно кризової ситуації та забезпечення систематичного діалогу між державою та засобами масової інформації, журналістами щодо вищезазначеного питання;

– забезпечення стабільного функціонування системи іномовлення України шляхом створення та поширення інформаційного продукту каналами супутникового, ефірного наземного аналогового і цифрового мовлення;

– використання знака (бренду) України «Ukraine Now»з метою популяризації та просування інтересів України у світі;

– обговорення на публіці сучасних актуальних проблем суспільного розвитку;

– забезпечення стабільного функціонування національного телебачення та радіомовлення, поширення українського інформаційного контенту;

– визначення механізмів регулювання роботи підприємств телекомунікацій, видавництв, телерадіоцентрів з закладами культури, засобами масової інформації, в тому числі заборона роботи приймально-передавальних радіостанцій особистого та колективного користування в питанні передачі інформації.

Для досягнення вищезазначених цілей та виконання вищезазначених завдань потрібний ефективний менеджмент здійснення інформаційної безпеки на наступних рівнях:

1) рівень окремих (переважно малих фірм), що забезпечують інформаційний захист власними силами, тобто власними інформаційними ресурсами відповідно до положення відповідного підприємства, цілей, стратегії та власних чи залучених коштів організації;

2) рівень великих компаній, що здійснюють інформаційну безпеку, яка в подальшому має вплив на суспільство та на різні елементи інформаційної інфраструктури;

3) державний рівень чи не найголовніший рівень задля здійснення та забезпечення інформаційної безпеки країни в цілому, що має значний впив на економіку країни, її розвиток, технології, правову систему та звісно ж на громадян країни;

4) міжнародний рівень пов’язаний з сферою інформаційних технологій, телекомунікацій та інформаційної безпеки [7, с. 98].

Для забезпечення інформаційної безпеки дії суб’єктів безпеки повинні відповідати наступним функціям:

– попереджувальна – це функція, що пов’язана з недопущенням негативних моментів в інформаційній політиці, а також здійсненні заходів щодо попередження та нейтралізації загроз;

– прогностична, пов’язана з аналізом ситуації в державі, на конкретному підприємстві чи в суспільстві, що прогнозує та визначає внутрішні чи зовнішні загрози;

– управлінська – це одна з важливих функцій, що передбачає ефективне управління інформаційними ресурсами за рахунок створення сприятливих умов та можливостей.

Таким чином, в даному підрозділі було висвітлено значення та важливість інформаційних технологій, сутність персональних даних, їх захист та історія становлення на всіх етапах розвитку, було охарактеризовано систему захисту персональних даних, а також визначено сутність інформаційної безпеки, її трактування з різних точок зору та її склад, визначено цілі реалізації Стратегії інформаційної безпеки та поставлено завдання для досягнення поставлених цілей, охарактеризовано функції інформаційної безпеки, рівні, на яких може здійснюватися інформаційна безпека.

1.2. Інформаційні загрози в системі захисту персональних даних

Безпечне існування особи, суспільства та держави та їх вільне функціонування залежить від захищеності інформаційної сфери від екзогенних та ендогенних загроз. У зв’язку з широким використанням інформаційно-комунікаційних технологій все більшого значення набуває недобросовісне використання таких технологій, що в результаті призводить до порушення прав людини. Тому виникає проблема співвідношення інформаційної безпеки і прав людини. Ще вагомою проблемою в захисті персональних даних є неможливість забезпечення захисту інформації при широкому використанні Інтернет-ресурсів.

Інформаційні загрози та виклики – це можливі дії, процеси, явища, які мають негативний вплив на психічний стан та свідомість людини, які призводять до завдання їй шкоди в умовах глобального інформаційного суспільства [45, с.27]. В загальному інформаційні загрози можна поділити на такі групи:

І група – загрози, що мають певні цілі. Даний вид загроз включає:

– загрози, що мають вплив на свідомість людини, що формують екстремістські погляди в молоді;

– загрози, що мають деструктивний вплив на здоров'я людини (до прикладу розповсюдження неліцензованих лікарських засобів);

– загрози щодо використання особистої інформації третіми особами у протиправних цілях;

– загрози, які пов'язані з фінансовим шахрайством.

ІІ група – загрози спеціального використання та поширення інформації, що є в обмеженому доступі: загрози розповсюдження інформації, яка є забороненою в Україні.

ІІІ група – загрози в мережі Інтернет, що включають в себе шахрайські сайти, спам-розсилки, фішингові сайти з метою виманювання коштів в громадян або поширення кіберсуїциду.

Вищезазначені загрози несуть за собою небезпечні інформаційні дії, які в свою чергу поділяються на:

1) дії, пов'язані з втратою цінної інформації (розголошування державної таємниці, спеціальні засоби для прослуховування);

2) дії, пов'язані з впровадженням негативної інформації (маніпулювання громадською думкою, ліквідація наслідків комп'ютерних атак).

На інформаційні загрози та виклики впливають політичні, економічні та організаційно-технічні фактори (рис. 1.2) [18, с.22].

Рис. 1.2. Фактори загроз інформаційній безпеці

Загроза інформаційній безпеці є потенційною можливістю порушення режиму інформаційної безпеки. Причиною інформаційних загроз може бути неконтрольований доступ до персональних комп'ютерів або неліцензійне програмне забезпечення. Наприклад, розробники Microsoft постійно вносять зміни в програмне забезпечення, але є проблема, адже є проміжок часу між виявленням проблеми та її ліквідацією, що в майбутньому призведе до того, що зловмисник зможе завдати непоправної шкоди. Саме тому найчастіше використовується інший спосіб захисту інформації – спосіб попереджувального захисту, який полягає у своєчасному виявленні потенційних загроз [92, с. 264].

Для попередження, визначення, ліквідації та ефективного управління загрозами інформаційної безпеки потрібно розуміти джерела загроз, які в

свою чергу включають джерела загроз інформаційній безпеці особистості, суспільства та держави [23, с. 117].

Інтереси особистості в інформаційній безпеці полягають в забезпеченні прав і свобод громадян на доступ до відкритої інформації, на її використання під час здійснення діяльності в межах законодавства та на захист інформації для забезпечення особистої безпеки, духовного та інтелектуального розвитку.

Найбільш небезпечне джерело загроз в інформаційній безпеці особистості є маніпулювання свідомістю людини шляхом створення «віртуального інформаційного простору», адже інформаційна структура в сучасному світі є основним джерелом інформації для людини та має вплив на потреби людей відповідно до піраміди Маслоу (задоволення першочергових потреб, потреб безпеки, соціальних потреб, потреб в повазі та самовираженні). Наразі існує залежність окремого громадянина від інших співробітників, які пов’язані з інформаційними технологіями, адже останні формують для людини інформаційний фон, умови, вирішують життєві проблеми. Саме тому важливо знайти оптимальне співвідношення між безпекою людини та інформаційною структурою. Не менш ризикованою є загроза інформаційній сфері особистості в частині використання персональних даних без згоди їх власників, що суперечить конституційним нормам і не забезпечує конфіденційність приватної або сімейної інформації.

Інтереси суспільства в інформаційній сфері передбачають захист конституційних прав і свобод людини і громадянина на рівні демократичного суспільства, для підвищення творчої активності населення або для підтримання суспільної злагоди.

Джерелами загроз інтересам суспільства в інформаційній сфері є:

– безперервне ускладнення інформаційних систем і мереж зв’язку критично важливих інфраструктур забезпечення життя суспільства (наприклад, навмисні чи ненавмисні помилки, збої техніки, програмного забезпечення в енергетичній, транспортній сферах);

– концентрація засобів масової інформації у руках невеликої групи власників, що проявляється в маніпуляції суспільною думкою в суспільно значимих подіях, або нав'язування чужої думки;

– розширення масштабів комп'ютерної злочинності (шахрайські операції з використанням інформаційно-телекомунікаційних систем, одержання неправомірного доступу до банківської інформації, відмивання грошей, одержаних злочинним шляхом) [51, с. 26].

Інтереси держави в інформаційній сфері полягають в реалізації конституційних прав і свобод громадян для зміцнення конституційного ладу, суверенітету та територіальної цілісності країни, забезпеченні політичної і соціальної стабільності, економічного процвітання та подальшої міжнародної співпраці у всіх сферах [31, с.30].

Найгіршою загрозою держави в інформаційній сфері є розголошення державної таємниці та іншої конфіденційної інформації, розкриття якої несе значні збитки державі. Найнебезпечнішою загрозою даного інтересу є неконтрольоване розповсюдження інформаційної зброї, яка визначається сукупністю засобів та методів, що мають вплив на інформаційну сферу протилежної сторони для руйнування її інформаційної інфраструктури, системи управління державою. Завданнями, які можуть вирішуватися за допомогою інформаційної зброї, є:

– маніпулювання суспільною думкою та свідомістю соціальних груп населення;

– створення атмосфери негативного відношення до культурної спадщини протилежної сторони;

– дезінформація населення про роботу державних органів;

– ініціювання страйків, масових заворушень в соціальній, політичній, релігійній чи економічній сферах, що в майбутньому може призвести до нанесення значних втрат життєво важливим інтересам держави;

– підрив міжнародного авторитету держави, її співробітництва з іншими країнами;

– конфлікти між політичними партіями, розпалювання недовіри, загострення політичної боротьби.

Визначивши джерела загроз особистості, суспільства, держави, наведемо види інформаційних загроз за різними класифікаційними ознаками (табл.1.3) [98].

Таблиця 1.3

Види інформаційних загроз

Класифікаційні ознаки	Види загроз
За причиною виникнення	– загрози, що виникли у зв'язку з нестачею засобів технічного захисту; – загрози, що виникли у зв'язку з нестачею організаційних заходів
За походженням	– антропогенні; – техногенні; – природні
За розміром нанесеної шкоди	– незначні; – значні; – критичні
За видом інформації, що порушується	– загрози конфіденційності (витік, копіювання, викрадення, розголошення); – загрози цілісності (втрата, знищення, модифікація); – загрози доступності (блокування)
За тяжкістю порушення	незначні помилки; дрібне хуліганство; серйозний злочин
За характером порушення	– порушення конфіденційності даних; – порушення працездатності мережевого обладнання; – незаконне втручання в роботу мережевого обладнання, робочих станцій
За передбаченням наслідків порушника	– умисне порушення; – ненавмисне порушення
За мотивацією	– зловмисне порушення; – незловмисне порушення
За закінченістю	– закінчені; – незакінчені

Джерело створено автором на основі [98]

Різні автори досліджували види інформаційних загроз. Відповідно є й інші види загроз [38, с. 94]:

1. За сферою походження:

– ендогенні – порушення системи перебуває в самій системі;

– екзогенні – порушення системи перебуває поза її межами.

2. За джерелами походження:

– природні загрози – загрози, що передбачають небезпечні геологічні, метеорологічні явища, природні пожежі, зміна стану водних ресурсів, масове ураження сільськогосподарських рослин і тварин хворобами чи шкідниками;

– техногенні загрози пов’язані з катастрофами, пожежами, вибухами;

– антропогенні загрози – це загрози, які виникають внаслідок дій людини із руйнування інформаційних систем.

3. За ступенем можливої шкоди:

– загроза – це явні чи потенційні дії, що унеможливлюють здійсненню національних інтересів в інформаційній сфері та створюють небезпеку в питанні державного управління;

– небезпека пов’язана з нестабільністю функціонуванням системи державного управління.

4. За повторюваністю вчинення:

– повторювані – це загрози, що мали місце в минулому;

– продовжувані – це загрози, що виникають з певною періодичністю та мають спільну мету.

5. За значенням:

– допустимі загрози, виникнення яких не вплине на загальний стан системи;

– недопустимі загрози – це загрози, що мають значний вплив як на окремого громадянина, так і на державу в загальному і можуть призвести до дестабілізації системи.

6. За характером реалізації:

реальні загрози – активізація алгоритмів дестабілізації є неминучою і не обмежена часовим інтервалом;

– потенційні – активізація алгоритмів дестабілізації можлива за певних умов середовища функціонування органу державного управління;

– здійснені – загрози, які вже відбулися;

– уявні – несправжність виконання алгоритмів дестабілізації.

7. За об’єктом впливу: на державу, на людину, на суспільство.

Життєво важливим в інформаційній безпеці є інтереси держави. Тому розглянемо виклики та загрози на національному рівні.

Відповідно до Указу Президента України Про рішення національної безпеки і оборони України «Про Стратегію інформаційної безпеки» існують наступні загрози та виклики в інформаційній безпеці (табл. 1.4) [84].

Таблиця 1.4

Загрози та виклики в інформаційній сфері

Вид виклику або загрози	Характеристика
Глобальні виклики та загрози	
Величезна кількість та подальше збільшення дезінформаційних кампаній	Дезінформаційні кампанії, що маніпулюють окремими людьми або групами, та загрожують розвитку держави та міжнародній стабільності
Інформаційна політика Російської Федерації	Спеціальні інформаційні операції РФ спрямовуються на ключові демократичні інституції, а спеціальні служби держави-агресора служать для посилення протиріч між Україною та іншими демократичними державами. Саме тому наша держава запроваджує санкції для протидії активностям РФ
Соціальні мережі, що мають суттєвий вплив в інформаційному просторі	Широке розповсюдження соціальних мереж призводить до загрози гарантії прав людини на приватність, тому постає питання балансу приватності та інформаційної безпеки держави
Низький рівень медіаграмотності, незважаючи на стрімкий розвиток цифрових технологій	У зв'язку з недостатнім рівнем медіакультури зростає вплив дезінформації та деструктивної пропаганди, що в майбутньому чинить загрози економічній та політичній стабільності держави
Національні виклики та загрози [84]	
Інформаційний вплив Російської Федерації на населення України	РФ має негативний вплив на населення України: проведення спеціальних інформаційних операцій, що спрямовані на підрив національної безпеки, національних інтересів, знищення української державності та ідентичності
Інформаційне домінування РФ на тимчасово окупованих територіях України	В зв'язку з окупацією територій України РФ держава-агресор застосовує методи тотального придушення свобод слова; намагається створити викривлену інформаційну реальність; здійснює регулярні репресії стосовно незалежних журналістів; переслідує людей за перегляд українського контенту, а найголовніше –

Продовження табл. 1.4

	чинить інформаційний тиск на дітей, які є вразливими від впливу інформаційних кампаній
Обмежені можливості реагувати на дезінформаційні кампанії	В Україні не створена розвинена інформаційна інфраструктура, що обмежує можливість належним чином протидіяти інформаційній агресії з метою захисту національної безпеки та реалізації національних інтересів України
Несформованість системи стратегічних комунікацій	В даному напрямку здійснено низку заходів у сфері стратегічних комунікацій, однак немає ефективного механізму координації і взаємодії між органами державної влади, що послаблює можливості до розбудови комплексного стратегічного планування інформаційного потоку
Недосконалість у сфері захисту професійної діяльності журналістів	Недосконалість у даній сфері перешкоджає розвитку медіаринку, загрожує творчій діяльності журналістів, що має вплив на неможливість інформування суспільства щодо суспільно важливих подій
Спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України	У Стратегії національної безпеки України європейська та євроатлантична інтеграція визначена одним із пріоритетів національних інтересів і національної безпеки. Переважна більшість громадян підтримує реалізацію європейського та євроатлантичного курсу України. Водночас здійснюються спроби маніпуляції свідомістю громадян України шляхом поширення міфів та дезінформаційних стереотипів
Доступ до інформації на всіх рівнях	Місцеві друковані засоби масової інформації, зазвичай є політично заангажованими від місцевих еліт
Недостатній рівень медіаграмотності в суспільстві	Низький рівень медіакультури в суспільстві створює підґрунтя для маніпулювання громадською думкою, проведення деструктивних інформаційних операцій, яке призводить до потенційних чи реальних загроз інформаційній безпеці держави

Джерело: сформовано автором на основі [84]

Щодо захисту персональних даних фізичні особи повинні дотримуватися наступних принципів [17, с. 6]:

– персональні дані мають збиратися і оброблятися відповідно до законодавства і лише компетентними спеціалістами в своїй сфері;

– персональні дані повинні бути точні, обмежені за термінами і оброблятися лише після згоди їх володільців;

– персональні дані повинні бути доступні суб'єктам цих даних для внесення уточнення в ці дані.

Отже, в даному підрозділі було охарактеризовано сутність та значення інформаційних загроз, їх види за різними класифікаційними ознаками, було висвітлено небезпечні інформаційні дії, а також фактори, загрози інформаційної безпеки та їх джерела відповідно до інтересів особистості, суспільства та держави в сфері інформаційної безпеки, було наведено глобальні та національні виклики і загрози в інформаційній сфері.

1.3. Методологічні підходи дослідження інформаційної безпеки людини, суспільства і держави

Процес інформатизації є одним з основних факторів суспільного розвитку та є глобальним, всеохоплюючим, який проникає в усі сфери життєдіяльності та впливає як в загальному на суспільство, так і на життя окремого громадянина. Така залежність стосується усіх держав, всіх людей та всього світу, що залучені у процес виробництва, зберігання та використання інформації в ході інформаційного обміну та інформаційної взаємодії. Суспільний розвиток на основі глобальної інформатизації породжує нові виклики, загрози та ризики інформаційній безпеці, саме тому актуальним залишається питання ефективного здійснення інформаційної безпеки як на локальному, так і на глобальному рівнях.

Для здійснення ефективного управління за інформаційною безпекою людини, суспільства і держави потрібно шукати нові підходи, аналізувати діючі, модернізуючи їх та розробляти нові моделі забезпечення

інформаційної безпеки. Серед науковців поняття «інформаційна безпека» передбачає різні погляди, водночас думка представників державної влади є однаковою і відповідає європейському стандарту щодо соціальних явищ.

Аналіз поняття «інформаційна безпека» включає в себе розгляд наступних чинників [6, с. 44]:

– потреби громадян, суспільства, держави і світового співтовариства;

– вплив інформаційних технологій на індивідів, суспільство і державу;

– наявність загроз і небезпек, якими повинна управляти система забезпечення інформаційної безпеки.

Поняття «інформаційна безпека» з'явилося наприкінці 80-х років завдяки працям німецького вченого Г. Одермана, який пояснював інформаційну безпеку як важливу інформаційну складову у міжнародній безпеці, а у вітчизняній літературі у 1991-1992 роках спостерігалася тенденція дослідження інформаційної безпеки.

Основними теоретичними підходами розуміння інформаційної безпеки є:

1) науково-правовий метод, який пояснює інформаційну безпеку як засіб соціальної діяльності, що спрямована на пізнання та функціонування суспільства, а також для запровадження нових концепцій на практиці [49, с. 95];

2) інший підхід говорить, що інформаційна безпека – це явище суспільного життя [2, с. 23].

Поняття «інформаційна безпека» можна розглядати й в широкому розумінні:

– як науково-теоретичний підхід;

– як професійно-практичний підхід;

– як буденно-повсякденний підхід.

Якщо розглядати поняття «інформаційна безпека» через призму політологічної науки, то слід зауважити, що дане поняття недостатньо

розвинуте та потребує вдоконалення в питанні проблеми демократії, політичного режиму, структур, ідеологій та цінностей.

Науковець З. Коваль зазначає, що інформаційна безпека держави – це захищеність інформації та забезпечення цілісності й надійності критичної нформаційної інфраструктури держави від випадкових та навмисних впливів природного чи штучного характеру; інформаційна безпека особи та суспільства – це захищеність психіки і свідомості від небезпечних інформаційно-психологічних впливів: маніпулювання, дезінформації, спонукання до запланованих противником дій [36, с. 11].

Дослідник О. Кісілевич-Чорнойван пояснює інформаційну безпеку як складову частину національної безпеки, яка відображає стан захищеності життєво важливих інтересів особи, суспільства і держави, за якого зводиться до мінімуму нанесення шкоди через неповність, несвоєчасність та недостовірність інформації або негативного інформаційного впливу через негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації; як стан захищеності інформаційного середовища, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави [34, с. 13].

Вчений В. Богуш пояснює інформаційну безпеку як стан захищеності інформаційного середовища, що відповідає інтересам держави та з допомогою якого забезпечується формування, використання і можливості розвитку незалежно від впливу внутрішніх та зовнішніх загроз [114, с. 35].

Дослідник В.А. Ліпкан зазначає, що інформаційна безпека – це стан захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, несвоєчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації [44, с. 35].

Науковець Я.М. Жарков стверджує, що інформаційна безпека – це стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну

наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни [22, с. 11].

На думку О.І. Барановського інформаційна безпека – це стан захищеності національних інтересів України в інформаційному середовищі, за якого не допускається завдання шкоди особі, суспільству, держав через неповноту, несвоєчасність, недостовірність інформації й несанкціонованого поширення й використання, а також через негативний інформаційний вплив та негативні наслідки функціонування інформаційних технологій [5].

Науковець Р. Калюжний зазначає, що інформаційна безпека – це стан захищеності інформаційного простору, який забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави [33, с. 110].

Існують наступні підходи до визначення інформаційної безпеки:

1. Герменевтичний підхід – це підхід, який полягає в різному тлумаченні одного й того самого поняття в залежності від перекладу з різних мов. Наприклад, інформаційна безпека (від англ. Information security), що можна перекласти з англійської мови як інформаційна безпека або як безпека інформації.

2. Підхід з точки зору соціальної філософії трактує інформаційну безпеку як структуру інформаційної безпеки, що включає системи інформаційних зв’язків, які визначаються великою кількістю інформаційних потоків. У зв’язку з тим, що наша держава потерпає від значних агресивних дій з боку держави-агресора, завданням протидії інформаційним атакам є управління економічною, політичною, соціальною, військовою інформацією як інструментом міждержавної взаємодії на найвищому рівні [99, с. 11].

3. Феноменологічний, політико-філософський підхід передбачає власну відповідальність кожного громадянина в питанні інформаційної захищеності власної держави і народу, тобто сьогодні потрібно говорити не лише про засоби забезпечення інформаційної захищеності організацій, а й світоглядні питання такої захищеності [26].

4. Концептуально-теоретичний системний підхід – це підхід, що пов’язаний з глобальними тенденціями, діджиталізацією політики та всіма сферами життєдіяльності.

5. Інтегральний підхід. Вчений В. Ліпкан пов’язує інформаційну безпеку з динамікою інформаційних систем і становленням не лише інформаційного суспільства, а й інформаційної цивілізації [42, с. 35].

6. Політико-правовий підхід інформаційної безпеки розглядається як частина глобального інформаційного суспільства; сукупність принципів нормального, безпечного та законодавчо окресленого соціуму. Так, дослідник В. Гурковський вважає, що інформаційна безпека держави – це відносини, пов’язані з захистом життєво важливих інтересів людини, суспільства та держави від потенційних або реальних загроз в інформаційному просторі, що є необхідною умовою збереження та примноження духовних і матеріальних цінностей нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів [43, с. 35].

7. Синергетичний підхід – це підхід, який полягає у виявленні різноманітних взаємозв’язків між природою, суспільством, культурою та людиною. Охоплення вищезазначених сфер дає можливість упорядкувати інформаційну систему шляхом синергії та врахуванням внутрішніх та зовнішніх чинників.

8. Історичний підхід пов’язаний з переходом від індустріальної до постіндустріальної стадії розвитку в питанні дослідження проблем інформаційної безпеки в суспільстві. На етапі становлення інформаційної безпеки дане поняття відображалося у двох знакових наукових правотворчих ініціативах. У 2012 році в Концепції кодифікації інформаційного законодавства України було визначено сучасні виклики та загрози інформаційній безпеці людини, суспільства і держави та їх своєчасне виявлення та реагування з використанням правових, організаційних,

технічних та інших засобів. Розробка Інформаційного кодексу України була передбачена Законом України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» та Стратегією розвитку інформаційного суспільства в Україні. Дослідник Б.А. Кормич у 2011 році пояснював, що проблематика інформаційної безпеки базувалася на інформаційному впливі та трактувалася як захищеність від цих впливів.

9. Формально-логічний метод – це підхід, що пов'язаний з можливістю вивчення логічних конструкцій норм, що встановлені для правового забезпечення інформаційного права та інших галузях.

10. Технологічний підхід – це підхід, який базується на забезпеченні конфіденційності, цілісності та доступності інформації [50, с. 35].

11. Інформаційний підхід – це підхід, який пов'язаний із захистом від інформаційних загроз, що можуть призвести до руйнування традиційних духовно-моральних цінностей суспільства, розмивання ідентичності особистості, дестабілізації політичної системи та втрати державного суверенітету [65, с. 85].

12. Міждисциплінарний підхід є найважливішим серед всіх підходів, що передбачає трактування поняття з точки зору різних наук. Щодо інформаційної безпеки залучені наступні сфери: інформаційні технології, психологія, соціологія масової комунікації та безпека. Інформаційні технології вивчають канали та способи технічної передачі інформації, дозволяють розуміти особливості технічних каналів поширення негативної інформації та вибирати ефективні способи впливу на них. Наука психологія пов'язана з механізмом роботи індивідуальної та колективної психіки та з психологічними знаннями, що дають змогу виявити потенційну небезпеку певної інформації для визначених груп та категорій осіб. Соціологія масової комунікації допомагає обирати інструментарій для ліквідації загроз інформаційної безпеки та їх джерел та має вплив на соціум, досліджуючи інформаційне середовища суспільства. Безпека – це поняття, що включає

реальні явища, процеси, відносини, попередження чи усунення загроз, що є метою та змістом політики безпеки [104, с. 11].

Визначивши методологічні підходи дослідження інформаційної безпеки людини, суспільства і держави, розглянемо основні принципи, а яких базується аналіз інформаційної безпеки:

– принцип розвитку, який передбачає системність, саморозвиток, відображає вектори соціальної динаміки;

– принцип цілісності; відповідно до якого інформаційна безпека – це система, яка включає в себе невід'ємні атрибути;

– принцип системності – це принцип, що вказує на те, що інформаційна безпека є системним та багатофакторним поняттям, що має особистісні, громадянські, професійні та соціальні характеристики.

Сфера інформаційної безпеки пов'язана з об'єктами деструктивного інформаційного впливу, якими є:

– загроза безпеці;

– правопорушення (адміністративно правопорушення, злочини);

– форми зловживання правом на інформацію та свободою масової інформації;

– виду співучасті у скоєнні злочину;

– пом'якшувальні обставини;

– підстави для визнання недійсності правочину.

У Стратегії інформаційної безпеки об'єктом захисту від деструктивного інформаційно-психологічного впливу є суспільство, яке представлене окремим громадянином, групою людей, суспільством, державою, психологічними складовими (психіка та свідомість) [84]. Тому на даному етапі є три рівня деталізації, що характеризуються трьома різними об'єктами інформаційної безпеки:

І рівень. На першому рівні об'єктами інформаційної безпеки є особа, малі чи великі соціальні групи. Людина – це особистість, що схильна до інформаційних факторів, які, змінюючись через поведінку, несуть

несприятливий вплив на соціальні групи. Соціальні групи – це група осіб, які пов'язані між собою колективною ідентичністю, соціальними відносинами та взаємодіями та поділяються на малі, великі, первинні, вторинні, неформальні, формальні, нестійкі, стійкі, закриті та відкриті. Велика суспільна група (соціальні верстви, етнічні групи, гендерні або вікові групи) – це реальна, значна за розмірами, організована сукупність людей, які залучені в спільній справі та схожій діяльності. Мала соціальна група (клас, сім'я, трудовий колектив, спортивна команда) – це нечисленна група людей, які об'єднані спільною соціальною діяльністю, та перебувають в особистому спілкуванні, що є основою виникнення емоційних відносин і групових процесів. Також в умовах розвитку цифровізації з'являються віртуальні групи, що виникли завдяки розвитку соціальних Інтерне-ресурсів.

ІІ рівень визначає психіку людини об'єктом інформаційної безпеки, яка охоплює свідоме і несвідоме та включає як індивідуальну, так і колективну свідомість.

ІІІ рівень включає дрібні психічні компоненти індивідуальної та групової психіки, які є об'єктом інформаційного впливу.

Дослідники О.Д. Довгань та Т.Ю. Ткачук зазначають, що негативний інформаційно-психологічний вплив – це вплив на особу чи групу осіб, що здійснюється на психіку, навіть всупереч їх волі, та із застосуванням спеціальних методів, що в майбутньому призводить до шкідливих наслідків для людини, суспільства чи держави [21, с. 89].

Чинники забезпечення інформаційної безпеки держави є:

– гарантування безпеки інформації, що є у вільному доступі, безпеки інформації мереж зв'язку, інформаційно-телекомунікаційних систем, технічних та програмних засобів виконання маніпуляцій з інформацією;

– гарантування конфіденційної інформації з обмеженим доступом;

– гарантування захищеності особи, суспільства й держави від шкідливого впливу певних видів інформації.

Важливим в інформаційній безпеці є державне регулювання. Так, відповідно до Закону України «Про Національну програму інформатизації» визначено наступні поняття:

– інформаційна технологія – це цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування;

– інформаційний суверенітет держави – це здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою дотримання законів України, прав і свобод громадян, гарантування національної безпеки держави [81].

Далі розглянемо законодавство в сфері інформаційної безпеки (табл. 1.5).

Таблиця 1.5

Законодавство в сфері інформаційної безпеки

Закон або нормативно-правовий акт	Що регулює
Конституція України [37]	визначає загальні засади держави, права, обов'язки та свободи громадян, регулює органи законодавчої, виконавчої та судової влади, а також органи місцевого самоврядування
Указ Президента України Про рішення Ради національної безпеки і оборони України «Про Стратегію інформаційної безпеки» [84]	аналізує загрози та виклики інформаційної безпеки (глобальні та національні); описує стратегічні цілі та напрями реалізації Стратегії інформаційної безпеки та завдання для досягнення зазначених цілей
Закон України «Про національну безпеку України» [80]	визначає засади національної безпеки України, регулює сектор безпеки і оборони, принципи планування у сферах національної безпеки і оборони
Закон України «Про національну програму інформатизації» [81]	координує формування і виконання національної програми інформатизації, в тому числі в питанні фінансового забезпечення та економічного стимулювання; здійснює державний контроль за формуванням та виконанням національної програми інформатизації, а також регулює питання міжнародного співробітництва при виконанні національної програми інформатизації
Закон України «Про доступ до публічної інформації»[73]	визначає, що відноситься до публічної інформації, її види; зазначає гарантії, принципи забезпечення права на доступ до публічної інформації; визначає порядок доступу до інформації; регулює відносини суб'єктів публічної інформації у сфері

Продовження табл. 1.5

	доступу до неї; координує реалізацію права на доступ до інформації за інформаційним запитом; визначає як правильно оскаржити рішення, дії чи бездіяльність розпорядників інформації
Закон України «Про захист персональних даних» [75]	розповідає про сутність персональних даних, об'єкти, суб'єкти захисту персональних даних, загальні та особливі вимоги до обробки персональних даних, права суб'єктів персональних даних; регулює збирання, накопичення, зберігання, використання та поширення персональних даних, а також їх видалення та знищення; регулює питання порядку доступу до персональних даних
Закон України «Про інформацію» [77]	визначає основні принципи інформаційних відносин, їх суб'єкти і об'єкти, види інформації (про фізичних осіб, інформація довідково-енциклопедичного характеру, екологічна інформація, інформація про товари, роботи, послуги, науково-технічна інформація, податкова, правова, статистична, соціологічна, критична технологічна інформація); координує діяльність журналістів, медіа, їх працівників; встановлює відповідальність за порушення законодавства про інформацію
Закон України «Про державну таємницю» [72]	визначає сутність державної таємниці, яка інформація відноситься до державної таємниці; пояснює засекречування та розсекречування матеріальних носіїв інформації; регулює охорону державної таємниці, регулює контроль за її забезпеченням, регулює відповідальність за порушення законодавства про державну таємницю
Закон України «Про захист інформації в інформаційно-комунікаційних системах» [74]	регулює об'єкти захисту в системі, суб'єкти відносин, відносини між володільцем інформації та власником системи, між власником системи та користувачем, між власниками систем, координує забезпечення захисту інформації в системі
Закон України «Про Національну систему конфіденційного зв'язку» [82]	визначає склад Національної системи конфіденційного зв'язку; регулює управління Національною системою конфіденційного зв'язку; визначає надання послуг конфіденційного зв'язку; регулює фінансове забезпечення Національної системи конфіденційного зв'язку, а також пояснює про міжнародне співробітництво в даній сфері
Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» [71]	регулює статус Державної служби спеціального зв'язку та захисту інформації України; визначає основні завдання Державної служби спеціального зв'язку та захисту інформації України; пояснює загальну структуру, чисельність та організацію діяльності Державної служби спеціального зв'язку та захисту інформації України; регулює особовий склад, його правовий і соціальний захист, повноваження Державної служби спеціального зв'язку та захисту інформації; пояснює фінансове та матеріально-технічне забезпечення діяльності організації; координує контроль і нагляд за діяльністю Державної служби спеціального зв'язку та захисту інформації та визначає відповідальність за порушення законодавства в даній сфері

Джерело: створено автором на основі [37, 84, 80, 81, 73, 75, 77, 72, 74, 82, 71]

Таким чином, в даному підрозділі було визначено методологічні підходи щодо визначення інформаційної безпеки, принципи аналізу інформаційної безпеки.

Висновки до розділу 1

Інформаційна безпека – це життєво важлива складова національної безпеки, яка спрямована на забезпечення національних інтересів, та є самостійною складовою частиною поряд з інформаційними ресурсами, інформаційною структурою та інформаційними технологіями. На інформаційну безпеку впливають як ендогенні, так і екзогенні фактори, такі як: економічний, соціальний та інформаційний стан країни, політична ситуація в країні. Інформаційну безпеку можна розглядати як:

– як складову національної безпеки;

– як стан захищеності інформаційного середовища, в тому числі національних інтересів від можливих загроз;

– як стан держави, що забезпечує національну безпеку країни в цілому.

Цілями реалізації Стратегії інформаційної безпеки є:

1) протидія дезінформації, зокрема держави-агресора, що проявляється в порушенні суверенітету та територіальної цілісності, ліквідації незалежності, вчиненні терористичних актів, посяганні на права і свободи людини;

2) всебічного розвитку української культури та утвердження української громадянської ідентичності;

3) підвищення рівня медіаграмотності та медіакультури суспільства;

4) забезпечення дотримання прав особи на збирання, зберігання, використання та поширення інформації; захисту приватного життя; доступу до достовірної інформації; свободи у вираженні своїх поглядів на ті чи інші питання; захисту прав журналістів, гарантії їх безпеки та найголовніше – протидії поширенню незаконного контенту;

5) інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих та на прилеглих до них територіях України, до загальноукраїнського інформаційного простору;

6) створення ефективної системи стратегічних комунікацій, метою якої є гарантування ефективної комунікації між органами державної влади, органами місцевого самоврядування та суспільством;

7) розвиток інформаційного суспільства та підвищення рівня культури діалогу.

Загроза інформаційній безпеці є потенційною можливістю порушення режиму інформаційної безпеки. Причиною інформаційних загроз може бути неконтрольований доступ до персональних комп'ютерів або неліцензійне програмне забезпечення. Наприклад, розробники Microsoft постійно вносять зміни в програмне забезпечення, але є проблема, адже є проміжок часу між виявленням проблеми та її ліквідацією, що в майбутньому призведе до того, що зловмисник зможе завдати непоправної шкоди. Саме тому найчастіше використовується інший спосіб захисту інформації – спосіб попереджувального захисту, який полягає у своєчасному виявленні потенційних загроз.

Інформаційні загрози поділяються на різні види в залежності від класифікаційних ознак, таких як: за сферою походження, за джерелами походження, за ступенем можливої шкоди, за повторюваністю вчинення, за значенням, за характером реалізації, за об'єктом впливу.

Методологічні підходи дослідження інформаційної безпеки:

– герменевтичний підхід;

– підхід з точки зору соціальної філософії;

– феноменологічний, політико-філософський підхід;

– інтегральний підхід;

– синергетичний підхід;

– історичний підхід;

– формально-логічний підхід;

– технологічний підхід;

– інформаційний підхід;

– міждисциплінарний підхід.

РОЗДІЛ 2
СУЧАСНИЙ СТАН ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ, СУСПІЛЬСТВА І ДЕРЖАВИ

2.1. Забезпечення інформаційної безпеки в мережі Інтернет

Забезпечення інформаційної безпеки в мережі Інтернет – це важлива задача, адже інтернет-простір є вразливим до різноманітних загроз, а саме кібератак, крадіжок інформації, злому облікових записів, шахрайства та інших неправомірних дій.

Найважливіші правила в забезпеченні безпеки в мережі Інтернет відображені на рис. 2.1 [40, с. 89].

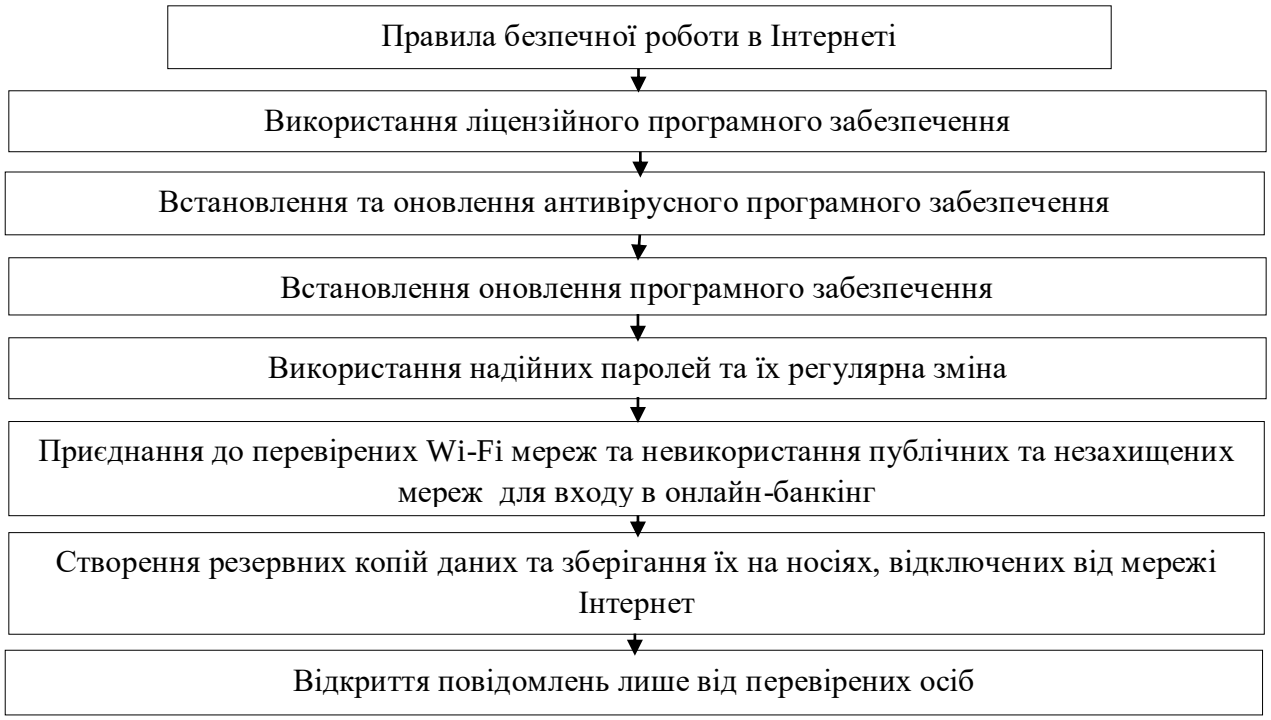


Рис. 2.1. Основні правила безпечної роботи в Інтернеті

Зберігання та передача даних – це один з найважливіших напрямків захисту даних, адже недотримання правил безпеки працівниками органів державної влади, органів місцевого самоврядування може призвести до втрат або крадіжки магнітних носіїв інформації, персональних ноутбуків. Через

здійснення несанкціонованого доступу до інформації з обмеженим доступом, копіювання важливої інформації з допомогою використання публічних мереж, використання USB-флеш накопичувачів, підключення до комп'ютерних систем із допомогою Bluetooth, призначених для каналів зв'язку з мережами загального користування, незахищеність інформаційних систем за допомогою актуальних версій антивірусного програмного забезпечення виникають кіберзагрози в інформаційно-телекомунікаційних системах. Для захисту даних потрібно:

– встановити паролі на всі пристрої та встановити коди доступу на всі облікові записи;

– здійснювати регулярно резервне копіювання важливої інформації;

– блокувати пристрої в разі невикористання [57].

Наступним популярним напрямком, де може відбутися витік персональних даних, є соціальні мережі, адже в світі майже всі громадяни своїх країн використовують різноманітні соціальні мережі, при чому можуть мати не один обліковий запис, а кілька, саме тому під час входу, користування та поширення такої інформації потрібно пам'ятати наступні моменти:

– встановити надійний пароль для входу в облікові записи різних соціальних мереж, при чому пароль має різнитися в різних акаунтах;

– використовувати функції подвійної авторизації, тобто при вході з іншого пристрою система запитуватиме пароль або підтвердження на номер телефону, що дійсно власник даного облікового запису бажає здійснити вхід;

– здійснити додаткові налаштування профілю в соціальних мережах з метою отримання інформації щодо несанкціонованого доступу до ресурсів з невідомого пристрою або Інтернет-браузера;

– використовувати електронну пошту надійних сервісів для реєстрації в соціальних мережах як логін при вході;

– не здійснювати авторизацію особистих чи робочих, корпоративних профілів з незнайомих чи незахищених пристроїв. Існує ймовірність, що

після завершення роботи не буде здійснено вихід із облікового запису або пристрій запам'ятає вказаний при вході логін та пароль. Крім того, існує ймовірність ураження такого пристрою шкідливим програмним забезпеченням, що може здійснювати збір та передачу відомостей щодо паролів та логінів зацікавленим особам;

– не відкривати повідомлення та не переходити за посиланням від незнайомих осіб [120];

– не публікувати в соціальних мережах особисту інформацію, що може становити загрозу життю особи чи її оточення та обмежити доступ до приватної інформації в налаштуваннях конфіденційності;

– бути уважним при додаванні друзів до соціальних мереж, адже можуть бути фейкові сторінки, а також перевіряти вже наявний список друзів;

– членам сімей військовослужбовців не публікувати фото- та відеоматеріали, за допомогою яких можна визначити їх місцезнаходження, отримати дані про озброєння та діяльність військової частини, окремих збройних військових формувань, що беруть участь у проведенні операції об'єднаних сил на сході України, що може загрожувати життю та здоров'ю людей;

– не використовувати російські соціальні мережі та російські пошукові системи.

Все таки є користувачі, які не довіряють соціальним мережам і перед тим, як наприклад, внести кошти на рахунок особи, що здійснює збір на дрони або на лікування когось, перевіряють дану інформацію, а потім вже роблять свій внесок. Так, базовими основними параметрами для забезпечення захисту інформації є:

– автентичність, яка пояснюється гарантією того, що власник інформації справжній і є автором повідомлення;

– цілісність – гарантія збереження повідомлення в первинному вигляді та гарантія того, що поширення, передача такої інформації буде здійснюватися без змін;

– конфіденційність, тобто інформація буде надаватися лише обмеженому колу користувачів – тих, кому така інформація призначається.

Для захисту від загроз потрібно здійснювати наступні дії [116]:

1) слід реєструватися не у всіх підряд соцмережах, а лише в тих, які викликають довіру та пропонують надійні механізми аутентифікації і розмежування доступу до особистої інформації користувача;

2) авторизацію в соцмережі необхідно виконувати, вводячи її URL в адресний рядок браузера вручну або використовуючи заздалегідь збережені вкладки чи посилання;

3) якщо є сумніви щодо знайомства з користувачем, який подав заявку в друзі, потрібно дочекатися підтвердження його особистості через інші джерела;

4) обов'язково час від часу необхідно змінювати паролі на всіх своїх сторінках; бажано використовувати окремі паролі для кожного акаунту – тоді, в разі зламу однієї сторінки, інші залишаться в безпеці;

5) потрібно пам'ятати, що будь-яка інформація, розміщена в Інтернеті, з великою ймовірністю залишається там назавжди, навіть у разі її видалення автором, адже може бути збережена або поширена іншими користувачами;

6) особливу увагу необхідно приділяти посиланням, які надходять від інших користувачів – вони можуть бути частиною фішингової атаки.

Враховуючи широке використання смартфонів та завантаження різноманітних додатків на нього потрібно бути уважним, адже, завантажуючи застосунок на телефон, відповідна система телефону просить надати доступ до телефонної книги, геолокації, галереї і багато іншого. Саме тому завантаження таких додатків потрібно робити лише з перевірених та надійних джерел. Рекомендаціями щодо завантаження додатків є:

– заборонити операційній системі автоматично завантажувати додатки з ненадійних джерел;

– завантажувати додатки лише з перевірених та надійних джерел;

– періодично видаляти дані з застосунків, якими не користуєтеся.

В наш час поширеним способом передачі та обміну інформацією є електронні листи засобами електронної пошти. Щоб уникнути витоку персональних даних, необхідно:

– увімкнути двофакторну автентифікацію за допомогою мобільного пристрою; в такому випадку під час спроби отримання паролю до поштової скриньки сторонніми особами буде надходити попередження на мобільний телефон у вигляді SMS-повідомлення про спробу злому;

– встановити надійний пароль [13];

– не використовувати для відновлення паролю російські сервіси;

– не запускати на пристроях вкладення підозрілих листів, що містять виконуваний файл з такими розширеннями як «.exe», «.bat», «.cmd», «.vbs», «.docm», «.xlsm» тощо;

– державні службовці повинні пам’ятати, що службові електронні скриньки не слід використовувати для приватного листування.

Мережа Інтернет – це мережа, яка заполонила весь світ, яка допомагає навчанню, роботі та дозвіллю.

Щоб уникнути перехоплення даних сторонніми особами, необхідно:

– під час здійснення доступу до мережі використовувати лише ті точки Wi-Fi, які мають протоколи безпеки для захисту безпровідного з’єднання WPA чи WPA-2;

– у публічних місцях найкраще користуватись особистим Wi-Fi модемом або здійснювати доступ до мережі Інтернет з мобільного пристрою за передплаченим пакетом послуг мобільного оператора;

– на комп’ютерах, мобільних пристроях та планшетах необхідно вимкнути функцію «Автоматичне підключення до Wi-Fi».

Для захисту мережі потрібно активізувати механізм захисту, що вбудований в обладнання, яке надає сервіс бездротових мереж. На сьогодні налаштування захисту обладнання бездротових мереж вимагає введення пароля. В деяких випадках (наприклад, недосвідчений користувач) пароль може бути найбільш уразливим місцем усієї системи. Все обладнання завжди має певні налаштування за замовчуванням. Інформація про ці налаштування повинна бути в інструкції до цього обладнання. Іншими словами, така інформація є загальновідомою. Якщо користувач не змінить налаштування пароля для точки доступу, зловмисник зможе легко підібрати пароль і отримати доступ до всієї мережі. Також важливим чинником є складність пароля. Загальновідомо, що чим довший і складніший пароль, тим вищу він має криптостійкість, і для його підбору потрібно більше часу. Тому рекомендують використовувати випадково згенеровані паролі достатньої довжини. Рекомендують також змінювати пароль через певні проміжки часу.

Використовують наступні технології для захисту бездротових мереж [40, с. 76]:

– технологія WEP (Wired Equivalent Privacy), в якій використовується алгоритм RC4 на статичному ключі; для підвищення захисту частина ключа є статичною, а інша частина – динамічною, що змінюється в процесі роботи мережі, при чому весь процес взлому становить 5–10 хвилин, тому не рекомендують застосовувати цей алгоритм захисту за будь-яких умов;

– технологія WPA (Wi-Fi Protected Access): за шифрування даних у WPA відповідає протокол TKIP, який, хоча і використовує самий алгоритм шифрування – RC4 –що й у WEP, але на відміну від останнього, використовує динамічні ключі (тобто ключі часто змінюються). Він застосовує більш довгий вектор ініціалізації і використовує криптографічну контрольну суму для підтвердження цілісності пакетів;

– технологія WPA2 працюють у двох режимах аутентифікації: персональному та корпоративному режимі; в персональному режимі генерується 256-розрядний ключ PSK (PreShared Key) спільно з

ідентифікатором SSID (Service Set Identifier), який використовують для генерації тимчасових сеансових ключів PTK (Pairwise Transient Key), для взаємодії бездротових пристроїв;

– технологія VPN (Virtual Private Network) дозволяє створити у межах будь-якої мережі або декількох мереж віртуальну персональну мережу, яка надає широкі можливості щодо забезпечення конфіденційності клієнтів [40, с. 78].

Попередньо охарактеризували найрозповсюджені напрямки використання Інтернет-технологій населенням, громадянами. Зараз поговоримо про рекомендації державному службовцю при виконанні своїх функціональних обов'язків, якими є:

– прес-службам державних органів під час суспільно-політичних подій в країні необхідно надавати коментарі та роз'яснення рішень на випередження,

щоб уникнути інтерпретацій та викривлень у ході обговорення тієї чи іншої ситуації в загальнодоступних та соціально- орієнтованих ресурсах мережі Інтернет;

– державним органам, установам необхідно розробити та затвердити чіткий план дій для оприлюднення представниками їхніх прес-служб інформації у випадку виникнення резонансних інцидентів;

– офіційні представники органів державної влади повинні оприлюднювати суспільно значущу інформацію, якщо вона не належить до тієї категорії, що не підлягає оприлюдненню. Не варто забувати, що приховування такої інформації від суспільства може знизити довіру до них;

– представникам органів державної влади під час надання коментарів, інтерв'ю, брифінгів не рекомендується використовувати оціночні судження, що можуть призвести до неоднозначного тлумачення наданої інформації її споживачами;

– органам державної влади необхідно розробити правила використання офіційних сторінок та акаунтів у соціальних мережах для уникнення

непорозумінь з користувачами та окреслення формату комунікації через соціальні мережі;

– держслужбовцям, а також іншим особам, які відповідно до своїх функціональних обов’язків працюють з інформацією з обмеженим доступом, необхідно пам'ятати, що під час оформлення допуску до державної таємниці при заповненні відповідних анкет вони повинні вносити достовірні дані про свої контакти з іноземними громадянами, наявність власних електронних скриньок, сайтів, профілів у соціальних мережах та тематичних форумах [119].

В мережі Інтернет вагомим аспектом є захист персональних даних. Для запобігання витоку персональних даних можна використовувати наступні засоби:

1. Фізичні засоби захисту – це засоби, які необхідні для зовнішнього захисту та призначені для створення перешкод для несанкціонованого доступу до інформаційних систем.

2. Апаратні засоби захисту – це засоби, як включають різноманітні електронні пристрої та які вмонтовуються в серійні блоки електронних систем оброблення та передавання даних для внутрішнього захисту засобів обчислювальної техніки: терміналів, пристроїв введення та виведення даних.

3. Програмні засоби захисту – це засоби, які включаються в програмне забезпечення системи та необхідні для виконання логічних функцій захисту.

4. Апаратно-програмні засоби захисту пов’язані з використанням програмних та апаратних засобів захисту.

5. Законодавчі засоби захисту – це засоби захисту, які представлені законами та нормативно-правовими актами, що регулюють роботу співробітників, які мають доступ до секретної інформації, визначають зону відповідальності за втрату чи крадіжки такої інформації.

6. Організаційні заходи захисту – це заходи, що включають заходи щодо підбору, перевірки та навчання персоналу, який задіяний в інформаційному просторі.

Отже, для забезпечення інформаційної безпеки в мережі Інтернет потрібно здійснювати наступні дії [100]:

1) оновлювати програмне забезпечення до найновіших версій задля виправлення виявлених вразливостей;

2) встановлювати та регулярно оновлювати надійне антивірусне програмне забезпечення, що дозволяє виявляти та блокувати віруси або шкідливі програми;

3) використовувати складні паролі, які складаються з літер, цифр, спеціальних символів, та регулярно замінювати паролі, і не використовувати один і той самий пароль для різних облікових записів;

4) використовувати двоетапну аутентифікацію, яка полягає у використанні двох або більше типів захисту (використання пароля разом з біометричною аутентифікацією);

5) не відкривати небезпечні посилання та не завантажувати будь-які файли з ненадійних джерел;

6) використовувати віртуальні приватні мережі в роботі з важливою інформацією, які забезпечують безпеку шляхом шифрування трафіку;

7) захищати свої облікові дані, не ділитися інформацією з невідомими особами та в загальному бути обережними при використанні соціальних мереж;

8) здійснювати резервне копіювання важливої інформації в разі витоку даних;

9) постійно моніторити стан інформаційного інтернет-простору, розуміти питання кібербезпеки, основних форм загроз задля успішного запобігання кібератак.

Не омине увагою й застосування соціальної інженерії шахраями, що використовується для маніпуляції свідомістю для збирання відомостей про підприємство, фізичну особу, одержання конфіденційної інформації, одержання прямого доступу до системи. За статистикою 55 % збитків, пов’язані з порушеннями інформаційної безпеки, виникають із вини

працівників, які мали вплив від соціальних інженерів. Метою соціальної інженерії є спонукання людей робити певні дії, які вони за звичних умов ніколи не вчинили, наприклад, розголошувати власну конфіденційну інформацію, переходити на невідомі сайти та за сумнівними посиланнями. Вся система соціальної інженерії базується на тому факті, що саме людина є найслабкішою ланкою будь-якої системи інформаційної чи кібербезпеки. Саме тому, за умови, що технічно одержати конфіденційну інформацію хакерам досить важко, вони впливають безпосередньо на користувача – найслабше місце в системі інформаційної безпеки.

Техніки соціального інжинірингу [112, с. 117]:

1. Фішинг – це вид інтернет-шахрайства, метою якого є одержання доступу до конфіденційних даних користувачів шляхом відправлення повідомлень та посилань від імені банків або від імені соціальних мереж.

2. Вішинг - техніка заснована на використанні системи попередньо записаних голосових повідомлень, метою яких є відтворення «офіційних дзвінків» від банківських та інших IVR систем.

3. Претекстинг – це техніка, яка передбачає використання голосових засобів, таких як телефон, «Skype» тощо для одержання потрібної інформації. Зазвичай називаючись третьою особою або вдаючи, що хтось потребує допомоги, соціальний інженер просить жертву повідомити йому пароль або авторизуватися на фішинговій веб-сторінці, тим самим змушуючи зробити необхідну дію або надати певну інформацію.

4. Фармінг – це техніка, яка передбачає перенаправлення жертви за помилковою інтеренет-адресою.

5. Послуга за послугу – цей вид атаки має на увазі дзвінок соціального інженера в організацію з корпоративного (внутрішнього) телефону. Здебільшого соціальний інженер відрекомендовується співробітником технічної підтримки, який виробляє опитування на виникнення технічних проблем. Під час процесу «рішення» технічних проблем соціальний інженер

«змушує» вводити команди, які дозволяють йому запустити або встановити шкідливе ПЗ на комп'ютер користувача.

6. Збирання інформації з відкритих джерел. Застосування технік соціального інжинірингу вимагає не лише знання психології, а й уміння збирати про людину необхідну інформацію. Відносно новим способом одержання такої інформації стало її збирання з відкритих джерел, в основному з соціальних мереж [40, с. 78].

7. Human denial service (HDoS. Людська відмова в обслуговуванні) – суть атаки полягає в тому, щоб змусити людину (непомітно для нього) не реагувати на будь-які ситуації. Тобто робиться так, щоб кожне слово соціального інженера сприймається як правда беззастережно і без осмислення. До такого роду атак належать і відволікання уваги. Соціальний інженер здійснює хибне уявлення про виконання однієї операції, а насправді виконує зовсім іншу. Отже, поки жертва зайнята одним, іншого вона не помічає. Атаки такого роду виконуються досить складно, тому що необхідно добре прорахувати психологію жертви, її знання і реакції на такі дії [40].

Таким чином, в даному підрозділі були описані правила безпечної роботи в Інтернеті, охарактеризовані рекомендації щодо захисту інформаційної безпеки в соціальних мережах, в сфері збирання на накопичення даних, в електронному листуванні, в органах державної влади при здійсненні функціональних обов'язків працівниками, а також був охарактеризований найпоширеніший тип шахрайства – соціальна інженерія та її техніки.

2.2. Державне управління інформаційною безпекою в системі електронного врядування

В наш час досить швидко розвиваються інформаційні технології як в житті кожного громадянина, так і в державному управлінні в цілому. Так, в Україні почало швидко розвиватися електронне урядування, а автоматизація

окремих процесів публічного управління сприяє економію ресурсів та часу, що сприяє виникненню ризик та загроз щодо захисту персональних даних.

В XXI столітті виявили витік персональних даних осіб, які зареєструвалися на сайті для проходження конкурсу на державну служб та персональні дані даних громадян були у вільному доступі. Задля усунення вищезазначеної проблеми Уповноваженим з прав людини було ініційовано створення робочої групи з реагування на кіберінциденти й протидії атакам на державні інформаційні ресурси і, як наслідок, було відновлено коректну роботу державного сайту. В травні 2020 року спостерігалася ситуація витоку персональних даних в чат-боті телеграму: поширювалися персональні дані з банківських реєстрів, зокрема дані з АТ КБ «Приватбанк» до його націоналізації, логіни й паролі з соціальних мереж [94]. Витік інформації й відбувся в 2016 році під назвою «Панамські папери», який полягав у розкритті міжнародних схем ухилення від податків через секретні рахунки в офшорних зонах [124]. Розвиток інформаційних технологій потребує впровадження ефективних механізмів захисту прав і свобод носіїв персональних даних на рівні органів державної влади. Система інформаційної безпеки держави відображена на рис. 2.2 [7, с. 98].

Інформаційна безпека держави – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди. Відповідно до законодавства проблеми інформаційної безпеки можуть вирішуватися за допомогою:

– створення інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

– підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці;

– вдосконалення нормативно-правової бази щодо захисту інформаційних ресурсів, захисту персональних даних, протидії комп’ютерній злочинності;

– розвитку Національної системи конфіденційного зв’язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

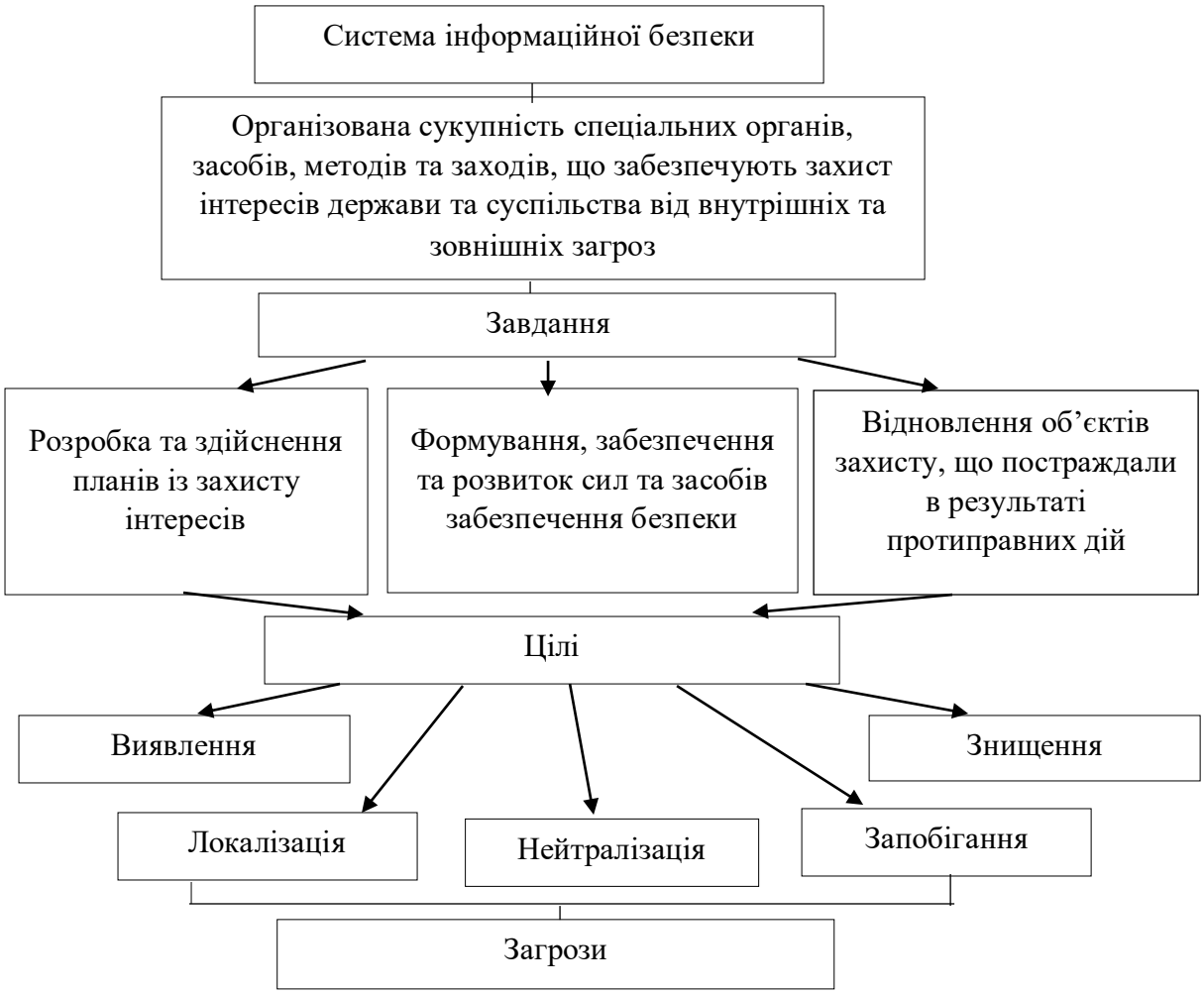


Рис. 2.2. Система інформаційної безпеки держави [53, с. 12]

Державні органи – це головні суб’єкти в забезпеченні інформаційної безпеки держави та формуються з:

– відповідних підрозділів спецслужб держави;

– Державної служби спеціального зв’язку та захисту інформації України;

– Національного координаційного центру кібербезпеки;

– Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України

До державних органів забезпечення інформаційної безпеки в системи електронного врядування відносять:

– Державне агентство з питань електронного врядування в Україні;

– Державну службу спеціального зв'язку та захисту інформації України;

– Міністерство юстиції України в частині питання роботи з електронним цифровим підписом;

– підрозділ з інформаційного забезпечення органу публічного управління.

Основною метою захисту інформації в електронному врядуванні є забезпечення інформаційної безпеки систем електронного врядування, службовців та громадян, які користуються такими системами, та систем публічного управління в цілому. Мету буде досягнуто в разі застосування комплексу заходів щодо забезпечення захищеності інформації від несанкціонованого доступу, використання, поширення чи знищення даних [91, с. 9]. Так, основними завданнями у сфері захисту інформації в інформаційно-телекомунікаційних системах є:

1) керування доступом користувачів в інформаційних системах для захисту від неправомірного втручання в роботу і несанкціонованого доступу до програмних ресурсів персоналу та третіх осіб;

2) захист даних, які передаються каналами зв'язку;

3) захист інформації від спеціальних впливів;

4) захист інформації з обмеженим доступом від витоку;

5) обов'язкового та ретельного контролю адміністраторами роботи користувачів системи та в разі несанкціонованого доступу повідомляти адміністраторів;

6) контроль і підтримка цілісності критичних ресурсів системи захисту і середовища виконання прикладних програм;

7) забезпечення функціонування програмно-технічних комплексів з метою захисту інформації від впровадження у роботу потенційно небезпечних програм і засобів подолання системи захисту;

8) керування та моніторинг засобів захисту інформації.

Державне управління в системі електронного врядування є важливою складовою забезпечення безпеки даних, які обробляються в державних структурах, що дає конфіденційність, цілісність та доступність даних та забезпечує довіру населення до електронного урядування, та включає такі аспекти [91, с. 13]:

1) виконання положень та стандартів інформаційної безпеки, яка містить правила щодо використання інформаційних систем, доступу до них, а також обмеження прав доступу до даних систем;

2) організація навчань та тренінгів для співробітників щодо інформаційної безпеки, що дає можливість підвищити обізнаність та зменшити ризики в інформаційній сфері;

3) впровадження та здійснення заходів технічного захисту інформації – систем захисту від несанкціонованого доступу, запобігання злому;

4) проведення аналізу і оцінка ризиків потенційних загроз в інформаційній безпеці системи електронного врядування;

5) управління різноманітними випадками в разі порушення безпеки даних (виявлення, розслідування та відновлення після інцидентів безпеки).

У Стратегії кібербезпеки України сказано, що загрози кібербезпеці актуалізуються через дію деяких чинників, зокрема, як [85]:

– невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;

– недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;

– безсистемність заходів кіберзахисту критичної інформаційної інфраструктури;

– недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів;

– недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;

– недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

Відповідно до Закону України «Про інформацію» основними принципами державної інформаційної політики України є [77]:

– забезпечення доступу кожного до інформації;

– забезпечення рівних можливостей у створенні, збиранні, одержанні, зберіганні, використанні, поширені, охороні, захисту інформації;

– створення умов для формування інформаційного суспільства;

– забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;

– розвиток електронного врядування поряд зі створенням інформаційних систем і мереж інформації;

– забезпечення інформаційної безпеки України;

– сприяння міжнародній співпраці в інформаційній сфері та входження України до світового інформаційного простору [85].

Державне управління інформаційною безпекою в системі електронного врядування з практичної точки зору регулюється Законом України «Про захист інформації в інформаційно-телекомунікаційних системах», а саме в питанні відносин у сфері захисту інформації в інформаційних системах, визначення об'єктів захисту та суб'єктів відносин, порядку доступу до інформації в системі, повноважень державних органів та відповідальності за порушення законодавства, регулювання міжнародної співпраці.

Відповідно до Закону України «Про Національну програму інформатизації» Національна програма інформатизації – це комплекс

завдань, програм, проектів, робіт з інформатизації, спрямованих на розвиток інформаційного суспільства шляхом концентрації та раціонального використання фінансових, матеріально-технічних та інших ресурсів, виробничого і науково-технічного потенціалу держави, координації діяльності державних органів, органів місцевого самоврядування, а також підприємств, установ, організацій незалежно від форми власності та спрямована на забезпечення наступних завдань:

1) розробка, впровадження та застосування інформаційно-комунікаційних технологій в органах державного управління, місцевого самоврядування та в суспільному житті;

2) впровадження та реалізація заходів щодо розвитку електронного врядування;

3) створення та розвиток системи державних інформаційних ресурсів;

4) підвищення освіченості громадян щодо роботи в інформаційно-комунікаційних технологіях;

5) вдосконалення процедури надання електронних публічних послуг;

6) організація взаємодії органів державної влади та органів місцевого самоврядування в системі електронного документообігу;

7) створення систем інформаційної та аналітичної підтримки діяльності державних органів та органів місцевого самоврядування;

8) підвищення ефективності вітчизняного виробництва шляхом використання інформаційно-комунікаційних та цифрових технологій.

Завдання із захисту інформаційних ресурсів пов’язане з тим, що системи електронного урядування використовують публічні службовці та різні категорії населення, що здійснюють:

– операції щодо функціональних обов’язків державних службовців і комунікацією з населенням та бізнесом;

– збереження та обробку даних;

– виконання доступу до внутрішніх та зовнішніх інформаційних ресурсів.

У системі електронного врядування для протидії інформаційним загрозам на програмно-технічному рівні застосовуються такі механізми безпеки як ідентифікація і аутентифікація користувачів, управління доступом, аудит, криптографія, екранування каналів зв'язку, забезпечення високої доступності (рис. 2.3) [40, с. 41].

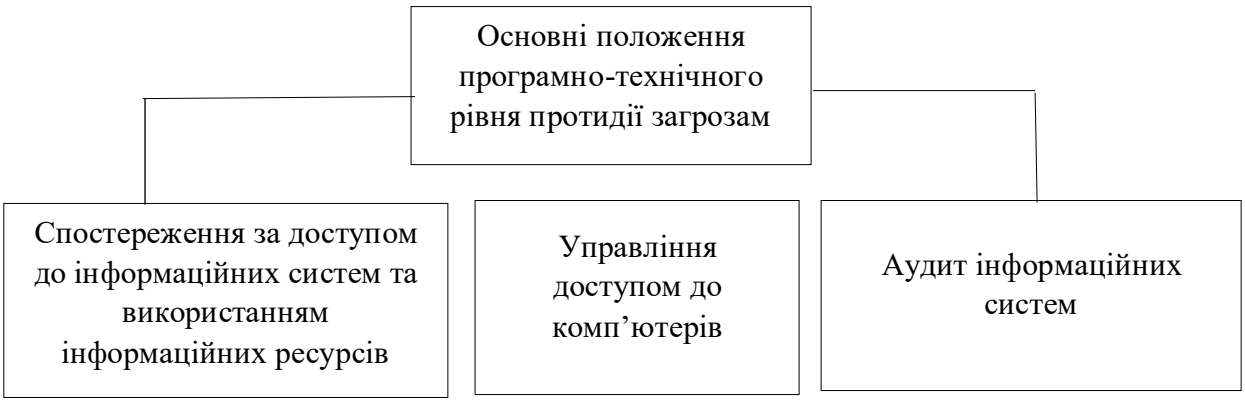
Управління доступом до комп'ютерів пов'язане з тим, що доступ надається лише зареєстрованим користувачам і має певні вимоги [3, с. 15]:

– ідентифікувати і перевіряти особистості користувачів;

– фіксувати випадки успішного або неуспішного входу до інформаційної системи;

– надати систему управління паролями, що забезпечує вибір надійних паролів;

– обмежити час підключення користувачів до інформаційних систем.



Джерело: розроблено автором на основі [40]

Рис. 2.3. Основні положення програмно-технічного рівня протидії загрозам інформаційній безпеці

Спостереження за доступом до інформаційних систем та використанням інформаційних ресурсів необхідне для визначення вжитих заходів. Усі надзвичайні події, пов'язані з порушенням режиму безпеки, та успішні входи необхідно реєструвати в контрольному журналі, де записи зберігаються протягом певного проміжку часу для надання допомоги в майбутніх розслідуваннях і здійсненні контролю за доступом до інформаційних систем. Усі дії, пов'язані з спостереженням, повинні бути

формально дозволені керівництвом. Для забезпечення точності ведення контрольних журналів, що можуть знадобитися для розслідувань або як свідчення під час судових розглядів і при накладенні дисциплінарних стягнень, важливо правильно встановити системний годинник комп'ютерів.

Аудит інформаційних систем проводиться з урахуванням наступних моментів: вимоги до аудиту ІС повинні бути погоджені з відповідним керівництвом; масштаб перевірок необхідно погодити і контролювати; перевірки повинні бути обмежені доступом до даних і програм тільки на читання; інші типи доступу (відмінні від доступу тільки на читання) повинні бути дозволені для окремих копій системних даних, які необхідно стерти по завершенні процесу аудиту; необхідно явно ідентифікувати інформаційні ресурси для проведення перевірок і зробити їх доступними; необхідно визначити вимоги щодо спеціальної чи додаткової обробки даних і погодити їх з постачальниками послуг; усі випадки доступу необхідно відслідковувати і фіксувати в контрольному журналі для перевірок.

Ідентифікація та аутентифікація користувачів представлена електронним цифровим підписом, який є видом електронного підпису, що отриманий за результатами криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписанта. Важливість електронного цифрового підпису полягає в наданні юридичної сили електронному документу. ЕЦП є ефективним засобом контролю походження та цілісності інформації на всіх рівнях інфраструктури суспільства: від персональної інформаційної безпеки людини до інформаційної безпеки держави.

Особистий ключ ЕЦП формується на підставі випадкових чисел. Друга частина ЕЦП – відкритий ключ обчислюється з особистого ключа таким чином, щоб одержати закритий ключ з відкритого було неможливо. Документ підписується ЕЦП тільки за допомогою особистого ключа, який існує у його власника. Також, є поняття Сертифіката, що підтверджує

приналежність відкритого ключа певній особі. Крім самого відкритого ключа, Сертифікат містить в собі персональну інформацію про його власника, унікальний реєстраційний номер та термін дії Сертифіката.

З метою забезпечення цілісності представлених у Сертифікаті даних він ще підписується особистим ключем Центру сертифікації ключів (ЦСК). Акредитований центр сертифікації ключів виконує всі зобов'язання та вимоги, встановлені законодавством для ЦСК та для надання послуг використовує надійні засоби електронного цифрового підпису [40, с. 42].

З точки зору інформаційної безпеки існують програмно-технічні архітектури, які складають з чотирьох рівнів протидії інформаційній безпеці (табл. 2.1).

Таблиця 2.1

Рівні протидії інформаційній безпеці

Рівень	Опис	Приклад
Рівень прикладного програмного забезпечення	Використовують публічні службовці або споживачі сервісів електронного врядування	Текстовий редактор Word, редактор електронних таблиць Excel, поштова програма Outlook, програми обміну повідомленнями Skype, різноманітні браузери та антивірусні програми
Рівень системи управління базами даних	Відповідає за зберігання і обробку даних систем електронного врядування	MS Access, MS SQL, MySQL, PostgreSQL
Рівень операційної системи	Відповідає за системи електронного врядування, інформаційних систем, баз даних і прикладного програмного забезпечення	мережеві серверні та клієнтські операційні системи Linux, FreeBSD, Sun Solaris, Microsoft Windows та інші
Транспортний рівень корпоративної мережі	відповідає за взаємодію окремих вузлів системи електронного урядування	стеки протоколів TCP/IP, IPS/SPX, SMB/NetBIOS, VPN та інші

Джерело: складено автором на основі [40]

Далі проаналізуємо програмні продукти та послуги, що пов’язані з захистом персональних даних, які замовляють державні органи (табл. 2.2) [86].

Відповідно до табл. 2.2 надавачами таких послуг є, як правило, приватні структури та станом на 12.11.2023 року наведена статистика тендерів.

Таблиця 2.2

Програмні продукти та послуги, що пов’язані з захистом персональних даних, які замовляють державні органи

Вид послуги	Кількість тендерів
Послуги, пов’язані з програмним забезпеченням	2914
Послуги з програмування та консультаційні послуги з питань програмного забезпечення	1824
Послуги у сфері інформаційних технологій, консультування, розроблення програмного забезпечення, послуги мережі інтернет і послуги з підтримки	10
Послуги з розробки пакетів програмного забезпечення	2736
Послуги у сфері управління даними	416
Послуги з обробки даних	10000
Послуги з розробки системного й користувацького програмного забезпечення	94
Послуги, пов’язані з роботою з електронними таблицями	1
Послуги з перетворення даних	250
Послуги з розробки прикладного програмного забезпечення	153
Послуги з розробки галузевого програмного забезпечення	22

Джерело: створено автором на основі [86]

Таким чином, для захисту інформації на вебпорталах органів державної влади необхідно:

1) створення органу на рівні держави, який розробляв би програмне забезпечення для захисту персональних даних та контролював б якість захисту виготовленої програми;

2) встановлення жорсткіших вимог, штрафів за витік персональних даних;

3) проведення навчання працівників, які пов’язані з опрацюванням персональних даних та передбачення відповідальності за дії особи, яка вчинила витік інформації;

4) знищення даних про особу після їх обробки; прикладом слугує подача кредитної заявки фізичною особою до банку, в разі відмови

банківської установи в кредиті, банк зобов'язаний знищити дані; або особа подає заявку на конкурс на державну службу і не проходить відбір, то далі потрібно знищити персональні дані;

5) розроблення механізму відповідно до якого суб'єкт захисту персональних даних зміг змінювати інформацію, переглядати або знищувати її.

Отже, в даному підрозділі була описана система інформаційної безпеки, її мета, завдання, проблеми та шляхи вирішення, були зазначені державні органи, які задіяні в процесі забезпечення інформаційної безпеки держави, а також охарактеризовані ключові аспекти державного управління інформаційної безпеки в системі електронного врядування.

2.3. Основи захисту персональних даних у комерційних установах на прикладі банківської системи

Банківська система – це частина економіки, яка відіграє важливу роль як в житті громадянина, так і для країни в цілому. На банківську систему впливають багато чинників, зокрема і розвиток інформаційних та телекомунікаційних технологій. В цьому аспекті провідне місце займають Інтернет-послуги, що надаються банківськими установами. В сучасному світі мережа Інтернет є своєрідним міжнародним інформаційним простором, тому дана мережа приваблює керівників провідних країн, міжнародних організацій, бізнес-партнерів [113, с. 96].

За останні 15 років Інтернет став доступним, зручним та універсальним засобом комунікації, який дозволяє здійснювати величезну кількість операцій дистанційно з використанням сучасних Інтернет-технологій в найрізноманітніших галузях і сферах, зокрема й в банківській. Комерційні банки – установи, які одні з перших почали використовувати інтернет-операції, за допомогою яких фізична особа може поповнити мобільний телефон, оплатити комунальні послуги або інші, здійснити перекази між своїми рахунками або на рахунок інших осіб, перевіряти свій стан

банківського рахунку, здійснювати операції щодо запровадження або скасування лімітів при проведенні трансакцій, оформляти депозитні або накопичувальні рахунки, здійснювати обмін валюти (при наявності карт в різних валютах), збільшувати або зменшувати кредитні ліміти. Звичайно цей список з кожним роком доповнюється, адже інформаційні технології не стоять на місці та й банки, конкуруючи з іншими банківськими установами, прагнуть задовольнити діючих клієнтів та залучити все більшу кількість фізичних та юридичних осіб. Щодо юридичних осіб можна сказати, що найпоширенішою банківською послугою, якою вони користуються, є клієнт-банк, який дозволяє нараховувати заробітну плату своїм працівникам, робити виписки по рахунку, формувати платіжні доручення, здійснюючи оплату контрагентам за товари, роботи, послуги.

Різновиди банківських послуг, котрі надаються банком через мережу Інтернет [109]:

1. Інформаційні послуги – це послуги, що пов’язані з інформуванням споживачів щодо банківських продуктів та послуг, їх характеристики, умови, порядок оформлення, розміщених на сайтах банківських установ. В даному аспекті варто зазначити, що відповідно до законодавства банки або інші фінансово-кредитні установи зобов’язані розміщувати на сайті повну інформацію про той чи інший банківський продукт чи послугу, без приховування будь-якої інформації, невигідної для клієнта.

2. Комунікаційні послуги передбачають взаємодію між банком та клієнтом через Інтернет-сервіс. Наприклад, клієнт хоче отримати кредит, при цьому немає часу підійти до відділення, тому скористається даною послугою дистанційно, а саме є можливість подати заявку на кредит, зазначивши свої дані для зворотного зв’язку.

3. Трансакційні послуги пов’язані з проведенням платежів з допомогою веббанкінгу або мобільного банкінгу, тобто здійснення всіх можливих транзакцій дистанційно без відвідування відділення банківської установи. Так, в Україні існує Монобанк – банк в телефоні, який немає відділень, тому

всі питання вирішуються через мобільний додаток або онлайн-помічників. Всі інші банки надають традиційні банківські послуги як в офлайн, так і в онлайн-режимах. Відповідно до цього найпоширенішими моделями банківського обслуговування в мережі Інтернет є:

– інтегрована модель, яка передбачає поєднання надання послуг у відділенні з наданням послуг з допомогою мобільних додатків банків;

– модель автономного інтернет-банкінгу пов'язана з наданням послуг дистанційно та призначена для банківських установ, які займають невелику частку на ринку банківських послуг та такі установи мають нижчі витрати, якби наймали персонал.

Використання Інтернет-технологій дає можливість зменшити витрати на обслуговування клієнтів, збільшити дохід, утвердитися як професіоналу на банківському ринку, розширити клієнтську базу, підвищити конкурентоспроможність. Проте у всьому позитивному є й негативні моменти, а саме ризики та загрози, які можуть виникнути, а саме ризики та загрози, які пов'язані з фішинговими сайтами, Інтернет-шахрайством, використання одноразових паролів третіми особами, несанкціоноване заволодіння третіми особами коштів фізичних чи юридичних осіб. Найпоширенішою та найголовнішою проблемою є ризик отримання зловмисниками паролів та доступу до коштів клієнтів та їх рахунків [108, с. 65].

Відповідно до статистики в 2022 році сума збитків від незаконних операцій з платіжними картками становила 481 млн. грн., що на 46% перевищує даний показник в порівнянні з 2021 роком. Директор Департаменту платіжних систем та інноваційного розвитку Національного банку України Андрій Поддєрьогін зазначив, що в 2022 році 86% шахрайських операцій було здійснено в мережі інтернет, а решта 14% - з допомогою фізичних пристроїв (банкоматів, терміналів самообслуговування, торговельних мереж). Також Поддєрьогін зазначив, що регулятор Національний банк України в 2022 році виявив більше 4,5 тисяч фішингових

ресурсів, а за 4 місяці 2023 року було виявлено понад 8 тисяч шахрайських доменів, тобто в середньому близько 100 ресурсів щодня, зокрема дві третини фішингових сайтів з Росії. Саме тому для боротьби з кіберзлочинністю Національний банк України разом з Радою національної безпеки і оборони розробили проєкт з протидії фішингу, який дозволяє користувачам бачити попередження, що сайт використовується зловмисниками [28].

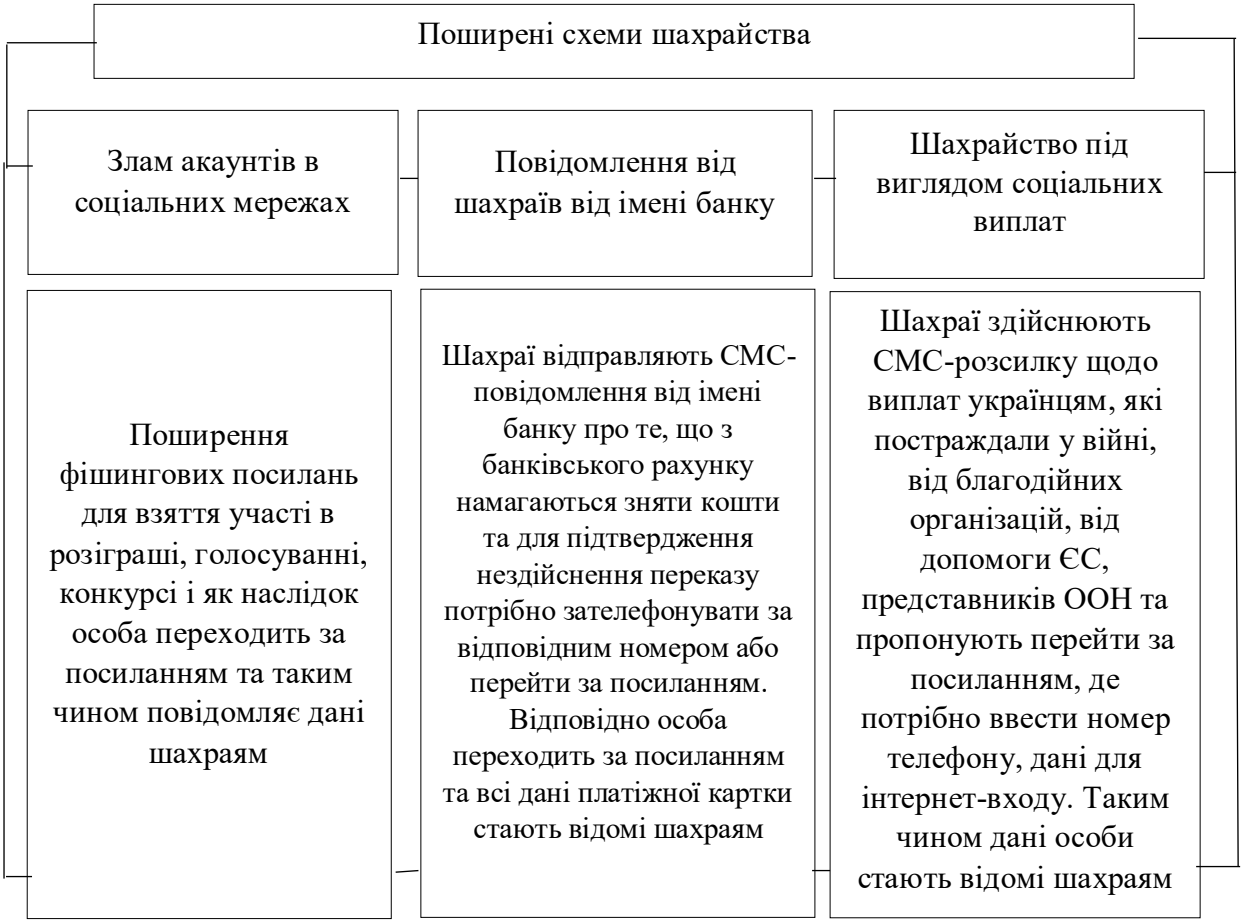


Рис. 2.4. Основні схеми шахрайства

Джерело: розроблено автором на основі [57]

Так, основні схеми шахрайства, які використовуються злочинцями відображені на рис. 2.4.

Для захисту персональних даних в банку потрібно дотримуватися наступних правил:

1. Зберігати в таємниці всі реквізити платіжної картки та контролювати рух коштів по рахунку. Виняток – коли клієнт сам телефонує на гарячу лінію

для вирішення питань, то оператор контактного центру може спитати перші 6 та останні 4 цифри картки. Та при отриманні переказу на картку достатньо назвати відправнику 16 цифр карти, але не називати CVV/CVC-коди, одноразові паролі та PIN-коди.

2. Підключити сповіщення щодо руху коштів по рахунку, встановити індивідуальні ліміти по карті в залежності від здійснення різних видів транзакцій та використовувати віртуальну картку для розрахунків в Інтернету, перераховуючи необхідну суму з основної картки на віртуальну перед здійсненням покупки.

3. Не переходити за посиланням незнайомців та друзів. В першому випадку це будуть фішингові сайти, які викрадають інформацію, персональні дані з акаунта, зокрема карткові реквізити, другий випадок пов'язаний з доступом шахраїв до акаунтів друзів. Краще передзвонити другові та уточнити дану інформацію.

4. Вводити дані платіжної карти лише на санкціонованих та перевірених сайтах для оплати товару чи оплати наданої послуги. Сайт, що починається з http ненайдійний, а той, який починається з https – надійний, лише спочатку потрібно перевірити даний сайт пошуковій системі. Також на сайті Кіберполіції є розділ, де можна перевірити посилання сумнівних сайтів.

5. Якщо все ж таки шахраю вдалося заволодіти даними картки психологічним методом, потрібно негайно телефонувати на номер гарячої лінії, який вказаний на звороті картки.

6. Захистити свій акаунт, створивши складні паролі, які зазвичай містять 8 і більше символів, великі та малі літери, цифри та спеціальні символи. При реєстрації в мобільному додатку будь-якого банку висвічується вікно, в якому вказується відповідна кількість цифр, літер чи символ для створення надійного пароля.

7. Створити додаткових захист акаунта за допомогою багатофакторної аутентифікації, який може бути у вигляді пароля, що приходить на телефон, для підтвердження входу.

8. Запам’ятати пароль до картки та не записувати PIN-код на картці чи зберігати написаним разом з карткою.

9. Рекомендувати змінювати PIN-код до картки 1 раз на 3 місяці [57].

Захист персональних в банківській системі є важливим, адже персональні дані містять конфіденційну інформацію про клієнтів: імена, адреси, банківські рахунки, кредитні картки та інші персональні дані, тому банки обов’язково мають зберігати конфіденційність, цілісність та доступність таких даних.

Банки – це головні фінансові установи, які працюють заради отримання прибутку та задля утримання та залучення величезної кількості клієнтів. Банківські установи розуміють, що для них є важливим доступність послуг та забезпечення збереження коштів на рахунках клієнтів. Саме тому для захисту даних менеджери банків впроваджують різноманітні системи, механізми, алгоритми, які б покращували оцінку ризиків, підвищували безпеку Інтернет-технологій та гарантували б недоторканість коштів клієнтів. Так, такі інструменти захисту відображені в табл. 2.3.

Безпека діяльності банку залежить не лише від банку, а й від клієнтів. Причиною шахрайства може бути необачність та неуважність клієнтів, які своїми діями привертають увагу зловмисників. Саме тому співробітники банків рекомендують зберігати паролі в надійному місці або взагалі не записувати, а запам’ятати та змінювати паролі час від часу.

Зловмисники все частіше використовують метод «фішинг-повідомлення», який ґрунтується на провокації одержувачів відправити свої справжні дані або пропонують перейти за посиланням на фішинговий сайт. Але з розвитком інформаційних технологій шахраї також почали створювати копії сайтів Інтернет-банкінгу, які є схожими на реальні сайти і мають однакове найменування, посилання та інтерфейс.

Таблиця 2.3

Інструменти захисту персональних даних в банківській системі

Інструмент	Опис
Одноразові СМС-паролі	застосовується при здійсненні банківської операції та передбачає наявний фінансовий номер телефону, який має бути зазначений в базі даних банківської установи; переваги: – швидкість проведення транзакції; – немає прив'язки до конкретного комп'ютера чи банкомата; – підтвердження, що саме власник рахунку здійснює банківську операцію; – не потрібно запам'ятовувати пароль, так як він є одноразовим; недоліки: – клієнт загубив телефон – і шахрай з легкістю використовує паролі Рекомендація: – у випадку втрати телефона негайно зателефонувати на гарячу лінію банку з проханням заблокувати всі картки та рахунки; – не здійснювати вхід в обліковий запис інтернет-банкінгу через телефон
Одноразові паролі	Застосовується при підтвердженні банківських операцій або авторизації в інтернет-банкінг, які клієнт отримує з банкомату Переваги: – наявність самої картки та введення повністю всіх її реквізитів; – отримання пароля в моніторі терміналу, можливість друку чеку з паролем Недоліки: – постійно зберігання чеку при здійсненні наступних транзакцій; – в разі втрати чеку потрібно знову повторити дію, беручи нові паролі в терміналі; – всі доступні паролі були введені, том потрібно знову йти до банкомату для отримання нових; – такими паролями можуть заволодіти шахраї Рекомендація: – зберігання такого чеку в конкретно визначеному місці, щоб випадково не викинути; – не зберігати чек разом з карткою; – не записувати логін та пароль в блокнотах, а запам'ятати
Шифрування даних	Застосування криптографічного протоколу шифрування даних відповідно до якого одна сторона шифрує дані, а інша – розшифровує Рекомендація: не відповідати на підозрілі сповіщення та не натискати на підозрілі посилання
Електронний цифровий підпис (ЕЦП)	Застосування: переважно для корпоративних клієнтів Переваги: – ЕЦП дозволяє розпізнати користувача Недоліки: – може піддаватися «злому» зловмисниками шляхом завантаження шкідливих програм на ПК Рекомендація: – періодичне оновлення антивірусних програм; – зберігання ЕЦП на флеш-пам'яті
Зовнішні електронні пристрої	Застосування: здійснення генерації одноразових паролів; працює через USB-порт, що підключається до комп'ютера клієнта без застосування спеціального програмного забезпечення Недоліки: клієнт немає доступу до своїх рахунків, якщо немає біля себе ключа від акаунта
Введення обмеження власного сертифікату	Дає змогу використовувати електронний ключ лише на тому комп'ютері, на якому він був згенерований
Обмеження тривалості сесії	Якщо клієнт неактивний в інтернет-банкінгу протягом 5-10 хвилин, банк закриває сесію і для роботи в системі потрібно заново авторизуватися

Джерело: складено автором на основі [47]

Також клієнт може здійснити розрахунок за товари, надані послуги, відправивши кошти на неправильні банківські реквізити. Банки в такому випадку у своїх системах Інтернет-банкінгу зазначають, що клієнти відповідають за правильність заповнення реквізитів.

Розглянемо системи безпеки Інтернет-банкінгу, які використовують банки, для гарантування захищеності своїх клієнтів (табл. 2.4).

Таблиця 2.4

Системи безпеки Інтернет-банкінгу в українських банках

Банк	Система безпеки
ПАТ КБ «Приватбанк»	Одноразові СМС-паролі, обмеження тривалої сесії, електронний цифровий підпис
АТ «Ощадбанк»	Одноразові СМС-паролі, одноразові паролі, обмеження тривалої сесії, електронний цифровий підпис
АТ «Укрексімбанк»	Одноразові паролі, електронний цифровий підпис
АБ «Укргазбанк»	Одноразові паролі, електронний цифровий підпис
ПУМБ	Одноразові СМС-паролі
Universal Bank	Особистий цифровий сертифікат

Джерело: розроблено автором на основі [58, 59, 60, 61, 63, 64]

Всі банки задля захисту персональних даних клієнтів на своїх сайтах розмішують наступні рекомендації:

– повідомити банк, зателефонувавши на гарячу лінію установи, або звернутися до відділення для блокування всіх рахунків;

– перевірити всі гаджети на наявність антивірусного програмного забезпечення та видалити всі шкідливі програми;

– періодично змінювати паролі до облікових записів;

– повідомити правоохоронні органи в разі списання коштів з рахунків та написати заяву у відділенні банківської установи, хоча в разі шахрайських дій банк нічим не зможе допомогти клієнтові, адже відстежити рух коштів досить важко [57].

Основними принципами захисту персональних даних в банківській системі є:

1. Конфіденційність, тобто забезпечення конфіденційності персональних даних шляхом використання технологічних заходів захисту

(шифрування даних, доступ до даних тільки зареєстрованим особам, контроль та права доступу до таких даних).

2. Відповідність законодавству в сфері захисту персональних даних, пов'язана з дотриманням усім вимог та норм в питанні обробки та зберіганні персональних даних, тобто використання внутрішніх правил, положень, виконання зобов'язань перед клієнтами, дотримання відповідних законодавчих актів (Закон України «Про захист персональних даних», Загальний регламент щодо захисту даних в ЄС – General Data Protection Regulation).

3. Доступність – це принцип, дотримання якого дає можливість забезпечити доступність персональних даних для авторизованих користувачів без зайвих затримок. При цьому банківська установа повинна використовувати надійні системи зберігання даних, робити резервне копіювання в разі потреби відновлення даних та мати налагоджену систему відновлення роботи системи в разі виникнення аварійних ситуацій.

4. Цілісність – це принцип відповідно до якого комерційні установи повинні гарантувати збереження та передавання персональних даних в первинному вигляді без будь-яких змін чи втрат шляхом застосування цифрових підписів.

5. Повідомлення про порушення конфіденційності. Банківські установи розуміють, що є відповідальними за захист персональних даних клієнтів в разі можливого порушення конфіденційності їх персональних даних. Якщо виникла така ситуація, комерційна установа зобов'язана повідомити відповідний орган задля захисту даних споживачів та вжити заходів для відновлення захисту даних.

Важливим при дотриманні всіх принципів є використання не лише технологічних засобів, але й присутність культурної атмосфери в організації, яка пов'язана з навчанням співробітників комерційної установи щодо правил та процедур обробки даних, впровадженню внутрішніх аудитів та постійного

моніторингу задля забезпечення належного рівня захисту персональних даних в банківській системі.

Саме тому розглянемо забезпечення банківської таємниці, яка відноситься до інформації з обмеженим доступом та регулюється Законом України «Про банки і банківську діяльність» та є інформацією щодо діяльності та фінансового стану клієнта, що стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку [70].

Банківська таємниця включає наступні види інформації;

– інформація про фінансовий стан клієнтів;

– інформація щодо системи охорони банку та клієнтів;

– відомості про банківські рахунки клієнтів;

– інформація щодо операцій, які були проведені на користь чи за дорученням клієнта;

– інформація щодо звітності по окремим напрямкам діяльності за винятком тієї, що підлягає опублікуванню;

– інформація про кредитоспроможність фізичної особи, яка має намір укласти кредитний договір;

– інформація про клієнтів, яка формується під час проведення банківського або валютного нагляду.

В свою чергу банк має право надавати інформацію, що містить банківську таємницю, приватним особам чи організаціям для забезпечення виконання ними своїх функцій чи надання послуг, при цьому останні не можуть розголошувати отриману інформацію або використовувати її на свою користь чи користь третіх осіб.

Банківські установи для збереження банківської таємниці виконують наступні дії [76]:

1) обмежують коло осіб, які мають доступ до банківської таємниці; ними переважно є інсайдери банку;

2) організовують спеціальне діловодство для реєстрації, обліку та зберігання таких документів;

3) застосовують найсучасніші технічні засоби для запобігання несанкціонованому доступу до електронних та інших носіїв інформації;

4) застосовують застереження щодо збереження банківської таємниці та відповідальності за її розголошення у договорах і угодах між банком і клієнтом; працівники банку, які влаштовуються на роботу підписують зобов'язання щодо нерозголошення інформації, що містить банківську таємницю.

Є ряд випадків, коли банки можуть розкривати банківську таємницю:

– на письмовий запит юридичної чи фізичної особи;

– за рішенням суду;

– органам прокуратури на письмовий запит щодо конкретної фізичної чи юридичної особи;

– на запит центральних органів виконавчої влади, що реалізують державну політику у сфері запобігання та протидії легалізації доходів, одержаних злочинним шляхом або фінансуванню тероризму, щодо фінансових операцій, які пов'язані з протидією відмиванню доходів, одержаних злочинним шляхом;

– на запит органів виконавчої служби, приватним виконавцям з питань виконання рішень суду [76].

Вимога відповідного державного органу на отримання інформації, яка містить банківську таємницю, повинна бути викладена на бланку державного органу встановленої форми, надана за підписом керівника державного органу (чи його заступника), скріпленого гербовою печаткою, містити передбачені Законом «Про банки і банківську діяльність» підстави для отримання цієї інформації, посилання на норми закону, відповідно до яких державний орган має право на отримання такої інформації, містити прізвище, ім'я, по батькові та реєстраційний номер облікової картки платника податку клієнта банку - фізичної особи або серію та номер паспорта/номер паспорта у формі картки

(для фізичних осіб, які через свої релігійні переконання відмовилися від прийняття реєстраційного номера облікової картки платника податків, повідомили про це відповідний контролюючий орган і мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта, або для фізичних осіб - нерезидентів), або найменування та ідентифікаційний код в Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань клієнта банку – юридичної особи. В разі смерті клієнта – власника рахунку юристи надають запити в банківські установи щодо рахунків, які були в померлої людини. Банк не має права надавати інформацію спадкоємцям, які ще не зареєстровані, як такі. Юрист формує спадкову справу після звернення спадкоємців та через 6 місяців видає свідоцтво про право на спадщину на рахунки в банківських установах і після цього спадкоємець має доступ до банківських рахунків, депозитних рахунків, індивідуального банківського сейфу в разі наявності.

Відповідно до Постанови Національного банку України «Про затвердження Правил зберігання, захисту, використання та розкриття банківської таємниці» банки повинні дотримуватися наступних правил для захисту інформації, що містить банківську таємницю [76]:

1) встановити спеціальний порядок ведення діловодства з документами, що містять банківську таємницю, зокрема визначити: порядок реєстрації вихідних документів, роботи з документами, що містять банківську таємницю, відправлення та зберігання документів, які містять банківську таємницю, а також особливості роботи з електронними документами, які містять банківську таємницю;

2) під час опрацювання вихідних документів виконавець документа визначає потребу проставляння на ньому грифу «Банківська таємниця», який проставляється в правому верхньому куті першого аркуша документа і не проставляється на документах, які банки надають клієнтам - власникам інформації, що містить банківську таємницю;

3) реєструвати вихідні документи, що містять банківську таємницю, в системі документообігу або/та журналі реєстрації (обліку) документів з грифами обмеження доступу, при цьому вихідні документи реєструються в день їх підписання або не пізніше наступного робочого дня.

4) забезпечити зберігання таких документів у сейфах або шафах, які надійно замикаються і до яких не мають доступу треті особи;

5) забезпечити гарантовану доставку та конфіденційність відправлення інформації, що містить банківську таємницю [75].

Таким чином, в даному підрозділі були охарактеризовані банківські послуги, які надаються з використанням Інтернет-технологій, моделі банківських послуг в мережі Інтернет, було показано статистику шахрайських операцій з платіжними картками, були наведені найпоширеніші схеми шахрайства та як від них захиститися. Також були проаналізовані інструменти захисту персональних даних в банківській системі, їх переваги, недоліки, застосування, рекомендації щодо недопущення витоку персональних даних, основні принципи захисту персональних даних. В даній частині роботі було висвітлено суть, значення, види банківської таємниці, трактування даного поняття в законах та нормативно-правових актах, а також було чітко визначено правила зберігання, захисту або використання банківської таємниці в окремих випадках.

Висновки до розділу 2

Забезпечення інформаційної безпеки в мережі Інтернет – це важлива задача, адже інтернет-простір є вразливим до різноманітних загроз, а саме кібератак, крадіжок інформації, злому облікових записів, шахрайства та інших неправомірних дій. Для забезпечення інформаційної безпеки в мережі Інтернет потрібно здійснювати наступні дії:

1) оновлювати програмне забезпечення до найновіших версій задля виправлення виявлених вразливостей;

2) встановлювати та регулярно оновлювати надійне антивірусне програмне забезпечення, що дозволяє виявляти та блокувати віруси або шкідливі програми;

3) використовувати складні паролі, які складаються з літер, цифр, спеціальних символів, та регулярно замінювати паролі, і не використовувати один і той самий пароль для різних облікових записів;

4) використовувати двоетапну аутентифікацію, яка полягає у використанні двох або більше типів захисту (використання пароля разом з біометричною аутентифікацією);

5) не відкривати небезпечні посилання та не завантажувати будь-які файли з ненадійних джерел;

6) використовувати віртуальні приватні мережі в роботі з важливою інформацією, які забезпечують безпеку шляхом шифрування трафіку;

7) захищати свої облікові дані, не ділитися інформацією з невідомими особами та в загальному бути обережними при використанні соціальних мереж;

8) здійснювати резервне копіювання важливої інформації в разі витоку даних;

9) постійно моніторити стан інформаційного інтернет-простору, розуміти питання кібербезпеки, основних форм загроз задля успішного запобігання кібератак.

Інформаційна безпека держави – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди. Відповідно до законодавства проблеми інформаційної безпеки можуть вирішуватися за допомогою:

– створення інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

– підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці;

– вдосконалення нормативно-правової бази щодо захисту інформаційних ресурсів, захисту персональних даних, протидії комп'ютерній злочинності;

– розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Для захисту інформації на вебпорталах органів державної влади необхідно:

1) створення органу на рівні держави, який розробляв би програмне забезпечення для захисту персональних даних та контролював б якість захисту виготовленої програми;

2) встановлення жорсткіших вимог, штрафів за витік персональних даних;

3) проведення навчання працівників, які пов'язані з опрацюванням персональних даних та передбачення відповідальності за дії особи, яка вчинила витік інформації;

4) знищення даних про особу після їх обробки; прикладом слугує подача кредитної заявки фізичною особою до банку, в разі відмови банківської установи в кредиті, банк зобов'язаний знищити дані; або особа подає заявку на конкурс на державну службу і не проходить відбір, то далі потрібно знищити персональні дані;

5) розроблення механізму відповідно до якого суб'єкт захисту персональних даних зміг змінювати інформацію, переглядати або знищувати її.

Для захисту персональних даних в банку потрібно дотримуватися наступних правил:

1. Зберігати в таємниці всі реквізити платіжної картки та контролювати рух коштів по рахунку. Виняток – коли клієнт сам телефонує на гарячу лінію для вирішення питань, то оператор контактного центру може спитати перші 6

та останні 4 цифри картки. Та при отриманні переказу на картку достатньо назвати відправнику 16 цифр карти, але не називати CVV/CVC-коди, одноразові паролі та PIN-коди.

2. Підключити сповіщення щодо руху коштів по рахунку, встановити індивідуальні ліміти по карті в залежності від здійснення різних видів транзакцій та використовувати віртуальну картку для розрахунків в Інтернету, перераховуючи необхідну суму з основної картки на віртуальну перед здійсненням покупки.

3. Не переходити за посиланням незнайомців та друзів. В першому випадку це будуть фішингові сайти, які викрадають інформацію, персональні дані з акаунта, зокрема карткові реквізити, другий випадок пов’язаний з доступом шахраїв до акаунтів друзів. Краще передзвонити другові та уточнити дану інформацію.

4. Вводити дані платіжної карти лише на санкціонованих та перевірених сайтах для оплати товару чи оплати наданої послуги. Сайт, що починається з http ненайдійний, а той, який починається з https – надійний, лише спочатку потрібно перевірити даний сайт пошуковій системі. Також на сайті Кіберполіції є розділ, де можна перевірити посилання сумнівних сайтів.

5. Якщо все ж таки шахраю вдалося заволодіти даними картки психологічним методом, потрібно негайно телефонувати на номер гарячої лінії, який вказаний на звороті картки.

6. Захистити свій акаунт, створивши складні паролі, які зазвичай містять 8 і більше символів, великі та малі літери, цифри та спеціальні символи. При реєстрації в мобільному додатку будь-якого банку висвічується вікно, в якому вказується відповідна кількість цифр, літер чи символ для створення надійного пароля.

7. Створити додаткових захист акаунта за допомогою багатофакторної аутентифікації, який може бути у вигляді пароля, що приходить на телефон, для підтвердження входу.

8. Запам’ятати пароль до картки та не записувати PIN-код на картці чи зберігати написаним разом з карткою.

9. Рекомендувати змінювати PIN-код до картки 1 раз на 3 місяці.

РОЗДІЛ 3
НАПРЯМКИ ВДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

3.1. Основні тенденції зарубіжного досвіду у сфері інформаційної безпеки на прикладі країн ЄС

При вивченні питання інформаційної безпеки важливим аспектом є врахування досвіду міжнародних країн, зокрема країн з розвинутою економікою та країн, що входять до Європейського Союзу для ефективного забезпечення інформаційною політикою особистості, суспільства та держави. Розробка та проведення інформаційної безпеки ведеться як на національному, так і на міжнародному рівнях. Враховуючи те, що все більша кількість користувачів користується соціальними мережами, а на глобальному рівні ми маємо досить слабкі засоби ідентифікації, що може призвести до витоку персональних даних та володіння особистої інформації третіми особами, держава має враховувати міжнародний досвід у проведенні інформаційної безпеки окремого громадянина, суспільства чи держави в цілому.

Аналізуючи досвід країн-партнерів, Україна може перейняти досвід, застосовуючи найуспішніші техніки та методи. Сучасне суспільство бажає отримати від держави та міжнародних організацій захист від інформаційних загроз, захист персональних даних, безпеки забезпечення прав і свобод, адже інформаційний простір є важливим новим етапом суспільного розвитку, новим виміром геополітичного суперництва, що має значний вплив на безпеку громадян та розвиток суспільства [46, с. 25].

Однією із перешкод забезпечення безпеки в даній сфері є висока вразливість національної та міжнародної інформаційної інфраструктури, неможливість або відсутність встановлення обмеження збору інформації, не порушуючи особисті кордони та міжнародну стабільність.

За визначенням ООН міжнародна інформаційна безпека – це захищеність глобальної інформаційної системи від терористичних, злочинних і військово-політичних загроз. Дослідник І.М. Забара характеризує міжнародну інформаційну безпеку як значення інформаційних технологій, їх взаємодію в кіберпросторі; як необхідність захисту національних, глобальних інформаційно-комунікаційних мереж і систем; чисельність та важливість загроз; неефективності існуючих стратегій; забезпечення безпеки та цілісності держав; необхідність співпраці в розробці міжнародних стратегій зменшення ризиків в інформаційній сфері [25].

Вчений Є.А. Макаренко вважає, що міжнародна інформаційна безпека – це взаємодія акторів для підтримки сталого миру на основі захисту інформаційної сфери, інфраструктури на глобальному рівні, суспільної відповідальності й свідомості світової спільноти від інформаційних загроз.

При врахуванні міжнародного досвіду також потрібно брати до уваги міжнародні норми, що закріплені в Статуті ООН:

1) суверенна рівність держав – це принцип відповідно до якого всі учасники-члени мають рівні права щодо забезпечення інформаційного суверенітету, використання ресурсів, розробки міжнародних документів в інформаційній сфері;

2) мирне врегулювання міжнародних суперечок, тобто вирішення конфліктних ситуацій з допомогою діалогу, переговорів, використання превентивної дипломатії;

3) заборона застосування сили – це принцип, що пов’язаний з категоричною забороною використання інструментів інформації впливу проти держав, їх територіальної цілісності чи незалежності;

4) невтручання у внутрішні справи інших держав пояснюється неприпустимістю здійснення інформаційної пропаганди, проведення інформаційних кампаній, поширення деструктивної інформації;

5) самовизначення народів та націй пов’язаний із встановленням прав національних меншин на культурну самобутність та інформаційну діяльність;

6) дотримання базових прав і свобод громадян – це принцип, який передбачає визначення конституційних прав та свобод людини, вільного обороту інформації, свободи висловлення, незалежності, заборони цензури;

7) територіальна цілісність та недоторканість – це принцип, який пов’язаний з визначенням меж інформаційного простору та передбаченням заходів захисту від несанкціонованого зовнішнього втручання.

У зарубіжних країнах захист персональних даних на загальних принципах, таких як [111, с. 220]:

– збір та обробка інформації повинна здійснюватися відповідно до законодавства та уповноваженими органами в даній сфері;

– персональні дані повинні бути адекватними заздалегідь визначеним цілям і розпорядження ними повинно обмежуватися за термінами, відповідним зазначеним цілям;

– обробка та використання інформації лише за згодою суб’єкта таких даних;

– доступність персональних даних до суб’єктів таких даних для уточнення інформації;

– захищеність персональних даних.

Також для кращого розуміння міжнародного досвіду в забезпеченні інформаційної безпеки слід розглянути досвід Північноатлантичного альянсу та Європейського Союзу. У зв’язку з агресією Росії проти України співпраця з НАТО вийшла на новий рівень та передбачає такі напрямки регулювання в інформаційній сфері:

– забезпечення свободи слова;

– захист інтересів національних меншин, культурної спадщини, мови;

– захист інтелектуальної власності та недопущення плагіату;

– забезпечення конкурентного середовища, диверсифікація засобів масової інформації задля боротьби з монополією;

– протидія кіберзлочинності.

Основним принципом безпеки в системі Альянсу є зберігання захисту інформації, починаючи від джерела отримання і закінчуючи її використанням. Забезпечення даного принципу здійснює Комітет внутрішньої безпеки НАТО та національний уповноважений орган з питань безпеки інформації, який розробляє політику та забезпечує безпеку в інформаційній сфері.

Говорячи про країни Європейського Союзу, можна говорити про відсутність єдиної моделі національної системи забезпечення інформаційної безпеки, тому країни-члени ЄС мають власні моделі забезпечення інформаційної безпеки, протидії кібератакам. Варто враховувати, що переважна більшість європейських країн є одночасно членами Європейського Союзу та членами Організації Північноатлантичного договору та на них поширюються положення обох організацій щодо інформаційної безпеки. Основним принципом Європейського Союзу в інформаційній сфері є інформаційна відкритість державної влади країн-учасників та ретельний захист персональних даних, який передбачає [46, с. 26]:

– власник персональних даних має пріоритетність у розпорядженні особистими даними;

– використання персональних даних лише з дозволу власника таких даних;

– використання персональних даних третіми особами вимагає покарання відповідно до законодавства.

Німеччина є країною-членом Європейського Союзу, адміністративно-правовий порядок інформаційної безпеки якої здійснюється за умов суворого дотримання інформаційної повноправності особи. З 1997 року діє Закон Федеративною Республікою Німеччини «Про захист персональних даних», який визначає порядок використання персональних даних у федеральних

органах влади, органах влади земель та прийнято Закон «Про основи надання інформаційних та комунікаційних послуг», який встановлює адміністративно-правові засади захисту інформації у інформаційно-телекомунікаційних мережах загального користування. Відповідно до Закону Німеччини «Про мультизасоби інформації» збирання, обробка та використання інформації дозволяється лише у випадках, коли воно дозволене законом або здійснюється за наявності згоди користувача обслуговування. Національним органом Німеччини, що забезпечує інформаційну безпеку, є Федеральне управління з інформаційної безпеки, яке регулює питання захисту від кібернетичних атак [121]. Кіберпростір Німеччини є відкритим для приєднання інших мереж передачі даних. Для захисту інформації в даній країні існують такі структури [107, с. 28]:

– Національний центр кіберзахисту, який створений для налагодження співробітництва між усіма державними установами та поліпшення координації заходів з кібербезпеки;

– Федеральна розвідувальна служба виконує завдання з попередження, припинення, ліквідації наслідків кібернетичних загроз; відповідає за безпеку комп'ютерних додатків, Інтернету, захист державної інформаційної критичної інфраструктури.

Франція – держава, в якій державне регулювання інформаційної безпеки є схожим до німецького регулювання та полягає в забезпеченні кібернетичної безпеки і безпеки даних Інтернет. В загальному в даній країні немає актів, які б законодавчо регулювали дану сферу, зате передбачена кримінальна відповідальність в разі розголошення державної чи комерційної таємниць. Національна модель інформаційної безпеки Франції розглядається як в цивільному, так і у військовому аспектах, при чому цивільний компонент передбачає більш широкий спектр застосування спеціальних заходів, спрямованих на недопущення втручання в бази даних державних підприємств, організацій, недопущення розголошення персональних даних. Протидія загрозам інформаційному середовищу у Франції може

здійснюватися на місцях поліцейськими управліннями, де існує спеціальний відділ щодо боротьби зі злочинами в інформаційній сфері та залучені до цього процесу й вузькопрофільні спеціалісти (фінансисти, юристи, аудитори). Слід зазначити, що дана модель є дороговартісною, але ефективною, адже у Франції практично не вчиняються шахрайські дії з банківськими картками [115].

Польща ще одна високорозвинена країна, яка є членом Європейського Союзу, де для регулювання інформаційної безпеки залучається громадянське суспільство, зокрема у 2017 році було створено неурядову організацію, яка аналізувала та здійснювала пошук системного підходу до ідентифікації та протидії дезінформації. Даний досвід можна використати в Україні проти інформаційних загроз з боку держави-агресора [96, с. 114].

В Румунії можемо спостерігати активний процес розбудови кібернетичної безпеки держави, де даним питанням займається контррозвідувальний орган – Румунська служба інформації [35].

Можемо перейняти досвід не лише країн-учасників Європейського Союзу, а й могутніх країн. Так, в США інформаційна безпека держави є запорукою безпеки кожного громадянина. Вперше в найбільш впливовій в політико-економічному і військовому аспектах країні було запроваджене електронне врядування з використанням найновітніших інформаційних технологій та створена специфічна система захисту інформаційного суверенітету і безпеки інформаційних ресурсів. В США забезпеченням інформаційної безпеки займаються кілька організацій: Агентство національної безпеки (здійснює розвиток співпраці з приватним сектором задля протидії загрозам), Національне управління кібербезпеки міністерства внутрішньої безпеки США, Федеральне бюро розслідувань, Центральне розвідувальне управління (ЦРУ). Найважливішою інституцією в регулюванні інформаційною безпекою виступає Президент США. Основними моментами, що потрібно зазначити в політиці інформаційної безпеки США, є:

1. Забезпечення інформаційної безпеки складається з федеральних законів і законів штатів. У всі часи розвитку інформаційної безпеки законами та нормативно-правовими актами, що регулювали інформаційну безпеку були: закон «Про доступ до інформації про діяльність ЦРУ», закон «Про охорону особистих таємниць», закон «Про таємницю», закон «Про право на фінансову таємницю», закон «Про свободу інформації» та інші.

2. США вперше запровадило поняття «інформація обмеженого доступу», що передбачало важливу, але несекретну інформацію уряду та інформаційні дані, які формуються і обробляються в інформаційно-телекомунікаційних системах фірм та корпорацій, що працюють на замовлення уряду.

3. Правовими нормами США були визначені складові частини інформаційної війни: психологічний вплив на супротивника, оперативна безпека, введення супротивника в оману, електронне втручання, інформаційна розвідка, виведення з ладу системи управління вірогідного супротивника, інформаційний захист власної системи управління під час бойових зіткнень. США – держава, яка допускає ведення інформаційних війн, що включає в себе планування і проведення активних інформаційно-психологічних операцій, хоча мирні відносини все одно зберігаються між державами.

4. За президенства Джорджа Буша були запроваджені урядові програми захисту національного інформаційного середовища у комп'ютерних мережах, що мають на меті створення умов для добування та обробки інформації щодо інформаційних загроз в публічному управлінні з боку інших держав та громадян. В даних програмах значна увага приділяється аналізу відкритих джерел і добуванню інформації з конфіденційних баз даних з використанням комп'ютерного обладнання, що сприяло формуванню нормативно-правової бази протидії кіберзлочинності, які регулюють аспекти забезпечення безпеки електронних інформаційних мереж і ресурсів та визначають взаємодію державних інституцій з питань протидії загрозам кібербезпеки [120].

5. В 2009 році в США був розроблений проєкт, що стосувався кібербезпеки, в якому було зазначено повноваження представників уряду щодо обмеження доступу до Інтернету в місцевостях США, де існує загроза інформаційній безпеці.

Канада – держава, яка також значну увагу приділяє регулюванню забезпеченості інформаційної безпеки. Інформаційна безпека Канади є невід'ємною частиною побудови інформаційного суспільства в державі, ще з 1990-х років спостерігався розвиток комп'ютеризації та інформатизації суспільних і управлінських процесів [115].

У 1993 році було розроблено «Канадські критерії безпеки комп'ютерних систем», що передбачали розробку єдиного визначення критеріїв різноманітних специфічних комп'ютерних систем, їх обробку, ступінь безпеки та характеристику. Нормативно-правові акти Канади спрямовані на збереження автентичності інформації, що міститься в інформаційних мережах, виробничій сфері, наданні публічних приватних послуг. Основним об'єктом охорони системи забезпечення інформаційної безпеки Канади є електронний уряд, що дає можливість взаємодіяти з державою за допомогою рівноцінного доступу до публічних послуг.

У 1997 році Канада прийняла федеральні закони про позитивний доступ в Інтернеті і про збереження конфіденційності в Інтернеті, а в 2001 році був створений спеціальний підрозділ Міністерства оборони – Група інформаційних операцій Канадських збройних сил, завданням якого була розробка канадської моделі інформаційної протидії для досягнення цілей інформаційної безпеки. В 2010 році була запроваджена Канадська стратегія кібербезпеки, яка регламентувала захист урядових інформаційних систем, забезпечення безпеки місцевих жителів, обмін інформацією між федеральними міністерствами і відомствами, угоди з міжнародними партнерами.

До прикладу в Грузії є спеціалізоване оперативно-технічне агентство, яке може таємно прослуховувати і записувати телефонні розмови,

контролювати соціальні мережі, здійснювати приховані відеозйомки, перевіряти поштові посилки в разі загрози безпеки держави.

Основними тенденціями міжнародного досвіду у сфері інформаційної безпеки є [103, с. 112]:

– зростання кількості кібератак, що пояснюється тенденцією до збільшення атак, фішингових сайтів, яке потребує розробки нових методів захисту інформації;

– посилення уваги до кібербезпеки на рівні країни, що говорить про пріоритетність даної сфери, що пояснюється створенням спеціальних організацій та регуляторних установ;

– зростання співпраці та обміну інформацією між державами, організаціями та приватним сектором задля боротьби з кіберзлочинністю та покращенням безпеки;

– розвиток кіберпрофесій та освіти, що означає популярність та важливість питання кібербезпеки, яке проявляється в зростанні попиту на фахівців в цій галузі.

Враховуючи досвід зарубіжних країн-членів ЄС в сфері захисту від кібератак та кіберзагроз, основними тенденціями є:

1. Законодавство та регулювання: більшість країн ЄС мають спеціальні закони та нормативно-правові акти, що регулюють забезпечення належного рівня захисту інформації.

2. Створення спеціалізованих центрів, що здійснюють аналіз, виявлення та реагування на кіберзагрози та співпрацюють з приватним сектором та академічною спільнотою для спільної боротьби з кіберзлочинністю.

3. Забезпечення безпеки критичної інфраструктури передбачає необхідність захисту критичної інфраструктури (фінансова сфера, транспорт, електроенергетика, телекомунікаційні мережі), для яких встановлюють єдині чіткі жорсткі критерії безпеки та вимоги до організацій, що здійснюють управління цими системами.

4. Інформаційні кампанії щодо кібергігієни, які передбачають поради та рекомендації щодо захисту персональних даних.

5. Міжнародне співробітництво: країни Європейського Союзу активно співпрацюють на міжнародному рівні для обміну інформацією про кіберзагрози та розробки спільних стратегій боротьби з кіберзлочинністю. Наприклад, Європейська агенція з мережевої та інформаційної безпеки (ENISA) сприяє співробітництву між країнами ЄС у цій сфері. Ці тенденції демонструють необхідність особливої уваги до інформаційної безпеки і підтверджують значення спільних зусиль у боротьбі з кіберзагрозами. Країни ЄС є прикладом ефективного управління інформаційною безпекою та успішно впроваджують стратегії та ініціативи для захисту своїх систем та громадян від кібернебезпек [67, с. 35].

Таким чином, в даному підрозділі було проаналізовано досвід країн Європейського Союзу та високо розвинутих країн, що не є членами Європейського Союзу, трактування питання «міжнародна інформаційна безпека» з різних точок зору, було описано міжнародні норми, що стосуються інформаційної сфери, принципи, на яких базується захист персональних даних, а також охарактеризовано основні тенденції міжнародного досвіду в сфері інформаційної безпеки.

3.2. Перспективні напрями вдосконалення системи захисту персональних даних

Розвиток інформаційних технологій має значний вплив на економіку, політику, соціальні процеси в державі. Захист особистих даних сьогодні – фундаментальне та досить комплексне поняття, яке, з одного боку, відображає прагнення захистити недоторканність особистого життя, з іншого – визначає його як інформацію, яка відображає участь особистості в суспільних та соціальних відносинах, що робить особисте життя доволі уразливим об’єктом щодо отримання особистих даних іншими особами. Воно відображає цілий комплекс дій з отримання та обробки інформації, яка

дозволяє ідентифікувати конкретну особу. Інститут захисту персональних даних є елементом державної системи захисту інформації, що забезпечує особисту безпеку, підтримує баланс інтересів особистості, суспільства та держави у сфері обробки інформації.

Важливим для України є використання зарубіжного досвіду, зокрема General Data Protection Regulation, або Загальне положення про захист даних – закону Європейського Союзу про конфіденційність даних, в якому передбачається [46]:

– демонстрація (доведення) відповідності вимогам GDPR;

– підвищення рівня безпеки персональних даних;

– запровадження контролю за передачею персональних даних за межі Європейського економічного простору;

– обмеження можливості використання хмарних сховищ для розміщення персональних даних;

– загальне підвищення рівня приватності;

– вдосконалена процедура повідомлення про витік даних;

– зміцнення контролю у відносинах між контролерами та обробниками;

– обмеження можливості залучення субобробників.

Серед основних прав, які були вдосконалені законом, можемо виділити:

1. Право бути поінформованим. Якщо інформація збирається безпосередньо від індивіда, необхідним є його оповіщення про це та отримання однозначної згоди. Згода повинна бути відкритою, явно вираженою та незавуальованою (наприклад, на практиці може виражатися як проставляння галочки біля кожного пункту персональних даних, що вводяться у мобільному додатку виклику таксі). Згода не може бути мовчазною та повинна бути відділена від інших умов договору (в тому числі приєднання як terms and conditions в соціальних мережах).

2. Право на видалення (право бути забутим). За запитом суб’єкта, вся інформація про нього повинна бути видалена. Цього правила можна не

дотримуватися, якщо інформація необхідна для реалізації права на інформацію, виконання норм чинного законодавства, забезпечення громадського здоров'я, наукової, історичної чи статистичної мети, вирішення правових спорів. Компанії, які можуть розміщувати інформацію користувачів онлайн, повинні за запитом особи видаляти не лише інформацію, а й посилання на неї чи будь-які можливі копії.

3. Право на заборону обробки. Компанія зобов'язана відмовитися від обробки персональних даних на вимогу суб'єкта. Методами, за допомогою яких компанія може це здійснити, є унеможливлення доступу третіх осіб до даних, видалення їх із веб-сайту тощо.

Перспективами вдосконалення в захисті персональних даних є [25]:

– юридичне супроводження захисту персональних даних у мережі Internet, оскільки ця незахищеність сьогодні стає вагомим важелем впливу на діяльність суб'єктів персональних даних;

– чітка фіксація відповідальності володільців персональних даних у випадках, коли ці дані стають загальновідомими (через санкції, притягнення до адміністративної відповідальності та інші)

Основними напрямками вдосконалення системи захисту персональних даних є:

1. Постійне навчання та підвищення кваліфікації є одним з ефективних способів підвищення кваліфікації фахівців, які займаються захистом персональних даних. У зв'язку з розвитком інформаційних технологій співробітники даної сфери повинні вдосконалювати свої знання та навички, щоб бути готовими до викликів в системі захисту персональних даних.

2. Використання існуючих систем аутентифікація та впровадження нових задля зберігання персональних даних в зашифрованому вигляді. Біометрична система аутентифікація представлена сканерами відбитків пальців, розпізнаванням обличчя чи голосу, що має на меті забезпечити високий рівень безпеки користувачів.

3. Розвиток системи обміну цифровими ідентифікаторами є важливим напрямом вдосконалення сфери захисту персональних даних, який забезпечує безпечний обмін персональними даними. Цифровими ідентифікаторами можуть виступати електронні паспорти або спеціальні програми для ідентифікації користувача в мережі.

4. Створення технологічних рішень для шифрування даних – це важливий напрямок вдосконалення системи захисту персональних даних, який включає відкриті ключі, асиметричні алгоритми та інші інноваційні методи, які забезпечують високий рівень захисту від несанкціонованого доступу до особистих даних громадян.

5. Застосування блокчейн-технологій – системи зберігання даних, що гарантує безпеку і недоступність для несанкціонованого доступу, та застосовується для зберігання та обробки персональних даних, що забезпечує надійний захист та контроль за використанням таких даних [25].

3.3. Формування культури інформаційної безпеки в епоху глобальної цифрової трансформації

В епоху цифрової трансформації зростає потреба у забезпеченні інформаційної безпеки особистості, суспільства та держави. З урахуванням збільшення використання інтернет-мереж все більшої актуальності набувають кіберзагрози, інформаційні війни та атаки на державні та приватні структури, які є критично важливими для суспільства та держави. У сучасному інформаційному суспільстві основним атрибутом є інтелектуальний потенціал, який неможливо створити без стабільної роботи та розвитку науки, освіти, професійних, політичних і управлінських структур на основі новітніх інформаційних технологій. Виникло усвідомлення інформаційних процесів в широкому соціокультурному контексті, і тепер вони прямо співвідносяться з культурою людства і з основними тенденціями її подальшого розвитку.

В умовах посилення цифрової трансформації зростає значення адаптації громадян до нових реалій в умовах цифрового середовища, підвищення поінформованості та набуття навичок протистояння інформаційним загрозам та ризикам. Водночас в умовах інформаційної війни, яку проводить Російська Федерація, основна увага в державній політиці надається боротьбі з загрозами інформаційної безпеки. Це правильно, оскільки завдання держави полягає в тому, щоб максимально захистити особу та соціум від деструктивного впливу інформаційних ризиків. Однак донині в експертній спільноті склалося розуміння того, що в інформаційному середовищі не можна уникнути будь-яких факторів, що утворюють загрози. Це зумовлено багатьма причинами: складністю виявлення загроз інформаційній безпеці, латентним характером дії, чисельністю джерел загроз інформаційній безпеці, обмеженою ефективністю методів припинення поширення деструктивної інформації. Не можна забувати про те, що в правовій демократичній державі ступінь втручання в суспільне життя, у тому числі в духовну сферу, має бути лімітованим [89, с. 25].

Вагомим аспектом є те, що сучасні інформаційні технології впливають на психологічний стан користувача, тому існує необхідність введення інформаційної безпеки до складу інформаційної культури.

Під культурою інформаційної безпеки суспільства можна розуміти сукупність певних знань, умінь, навичок і високий рівень свідомості, в тому числі й правової, в інформаційній сфері. Зазначимо. що тут в якості спеціальних знань, умінь і навичок виступають, зокрема:

– здатність реалізації інтересів кожного члена інформаційного суспільства;

– чітке бачення переваг від використання інформаційно-комунікаційних технологій;

– уміння критично оцінювати одержувану інформацію з точки зору її достовірності, корисності або шкідливості, актуальності, повноти тощо;

– навички ефективного протистояння можливим викликам і загрозам глобального інформаційного простору.

Під інформаційною культурою суспільства зазвичай мають на увазі здатність ефективно використовувати його інформаційні ресурси і засоби інформаційних комунікацій, а також застосовувати для цих цілей передові досягнення в області розвитку засобів інформатизації і інформаційних технологій [29].

Основними чинниками розвитку інформаційної культури суспільства та особистості є:

– система освіта, яка пов’язана з визначенням інтелектуального розвитку громадян, їх духовних та матеріальних потреб;

– інформаційна інфраструктура суспільства пов’язана з можливістю отримувати, передавати, використовувати необхідну інформацію між членами суспільства, здійснюючи інформаційну комунікацію;

– демократизація суспільства визначає правові гарантії з доступу до інформації, розвиток засобів масового інформування населення, а також можливості громадян використовувати альтернативні, у тому числі зарубіжні джерела інформації;

– розвиток економіки держави, від якого залежать матеріальні можливості здобуття людьми необхідної освіти, а також придбання і використання сучасних засобів телекомунікацій;

– оволодіння різними гаджетами та інформаційними технологіями;

– вміння формулювати свою потребу в інформації та спроможність здійснювати пошук всіх видів потрібної інформації;

– адекватність у відборі та оцінюванні інформації, її переробки та правильному використанні з отриманням максимального ефекту;

– особистість повинна володіти етикою спілкування та інформаційною культурою в інформаційному середовищі.

Формування культури інформаційної безпеки суспільства неможливо без якісного та ефективного контролю за цим процесом з боку держави. Для

досягнення цього необхідна розробка, впровадження і реалізація відповідними уповноваженими державними органами заходів, які сприятимуть розвитку культури інформаційної безпеки та будуть орієнтовані, в першу чергу, на найбільш «незахищені» верстви інформаційного суспільства. Основи державної культурної політики в цьому напрямку містять наступні завдання, які відображені на рис. 3.1.

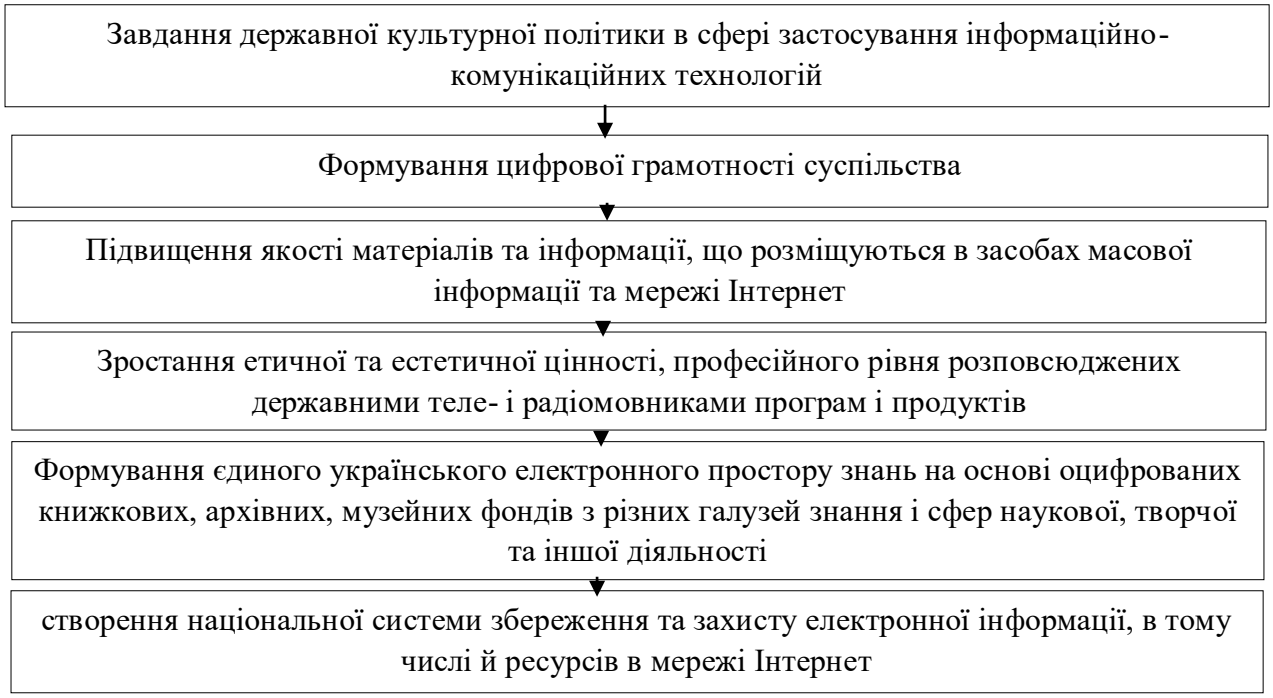


Рис. 3.1. Завдання державної культурної політики в сфері інформаційної безпеки суспільства

Складено автором на основі [29, 116]

Далі розглянемо функції культури інформаційної безпеки суспільства, якими є:

1. Безпекова передбачає формування безпечного інформаційного середовища на основі популяризації інформаційних ресурсів, що сприяють поширенню традиційних духовно-моральних та етичних цінностей нашої країни та можливість впровадження заходів щодо запобігання антидержавним або сепаратиським настроям в інформаційному суспільстві України

2. Нормативно-правова функція забезпечує нормативно-правове регулювання відносин в області інформаційної безпеки особистості та створює нормативно-правову базу, спрямовану на захист національних інтересів.

3. Соціально-економічна, пов'язана із забезпеченням основ для формування та розвитку свідомості та відповідального ставлення інформаційного суспільства до питань безпечного застосування інформаційно-комунікаційних технологій, у тому числі із формуванням споживчої та користувацької культури, розробкою механізмів та впровадженням заходів щодо запобігання будь-яким соціально-економічним правопорушенням в інформаційному просторі держави.

4. Допоміжна полягає в створенні та розвитку системи інформаційно-консультативної, технологічної та технічної допомоги з виявлення, попередження та ліквідації наслідків прояву загроз інформаційній безпеці суспільства; впровадженні заходів щодо запобігання та ліквідації загроз національній безпеці в інформаційній сфері [118, с. 44].

В кожній сфері є певні проблеми, з якими стикаються її суб'єкти. Винятком не є інформаційна культура, проблеми в якій можна сформувати в такі групи:

1. Проблеми інформаційної безпеки гуманітарного характеру, що виникають у зв'язку з безконтрольним використанням і поширенням персональних даних, вторгненням в приватне життя, наклепом.

2. Проблеми інформаційної безпеки економічного і юридичного характеру, що виникають в результаті витоку, спотворення і втрати комерційної і фінансової інформації, крадіжок інтелектуальної власності, промислового шпигунства.

3. Проблеми інформаційної безпеки політичного характеру, що виникають через інформаційні війни, спроби розкриття державної таємниці, атаки на інформаційні системи важливих оборонних, транспортних, промислових об'єктів.

Вирішуючи вищезазначені проблеми, обов'язковим елементом є навчання відповідних фахівців та користувачів комп'ютерів та комплексність, системність, яка повинна здійснюватися на наступних рівнях:

– нормативний – створення нормативно-правового базису, що враховує всі аспекти проблеми інформаційної безпеки;

– інституційний – узгоджена діяльність різних соціальних інститутів, пов'язаних з вихованням і соціалізацією;

– особистісний – самовиховання, самоосвіта, засвоєння знань використання інформаційних технологій в інтересах законного задоволення інформаційних потреб, фізичного, духовного, інтелектуального розвитку, досягнення високого рівня інформаційної культури як частини загальної культури особистості з метою формування необхідних якостей для забезпечення її інформаційного самозахисту.

Позначимо головні структуроутворюючі компоненти забезпечення інформаційно-психологічної безпеки особистості з точки зору культури інформаційної безпеки:

– усвідомлення впливу інформаційних процесів і технологій на розвиток особистості;

– розуміння своїх інформаційних потреб, міри їх задоволення, знання надійних джерел здобуття необхідної інформації;

– уміння роботи з інформацією на основі нових технологій, використання її як інструменту в різних видах діяльності;

– необхідність забезпечення інформаційно-психологічної безпеки особистості;

– здатність до визначення видів інформаційно-психологічної загрози; володіння навичками інформаційно-психологічного самозахисту.

Основними напрямками розвитку культури інформаційної безпеки в епоху глобальної трансформації є [29]:

1. Освіченість громадян та представників органів державної влади та органів місцевого самоврядування в питанні цифрової грамотності. Цифрова

освіта має стати важливою частиною навчання, адже кожний громадянин, член суспільства, співробітник, представник влади повинен вміти відрізняти реальний сайт з фейковим сайтом та вміти боротися з різними схемами шахрайства (фішингом, вішингом та іншими відомими схемами шахрайства з використанням соціальної інженерії).

Медіаграмотність – це комплекс знань, навичок і вмінь, що дозволяють розуміти, аналізувати та критично оцінювати медіа та їхні сюжети та статті, визначається як грамотне використання інструментів, що забезпечують доступ до інформації, розвиток критичного аналізу змісту інформації та прищеплення комунікативних навичок. З появою та зростанням популярності Інтернету дослідники почали говорити про «цифрову грамотність» як здатність критично розуміти та використовувати інформацію, одержувану за допомогою комп'ютера в різних форматах із широкого діапазону джерел.

Цифрова грамотність – це наявність навичок, необхідних для життя, навчання і роботи в суспільстві, де спілкування і доступ до інформації здійснюється за допомогою цифрових технологій (інтернет-платформи, соціальні мережі, мобільні пристрої тощо) [97, с. 50]. Істотне зростання можливостей Інтернету та входження у повсякденне життя людини привели дослідників до акцентування уваги на понятті цифрової компетентності.

Цифрова компетентність – здатність впевнено, ефективно, критично та безпечно обирати та застосовувати інформаційно-комунікаційні технології у різних сферах життєдіяльності (інформаційне середовище, комунікації, споживання, технічна сфера), готовність до такої діяльності. За останні десятиліття в країні підготовлено комплекс наукових та методичних праць, присвячених формуванню інформаційної (медійної, цифрової) грамотності та культури інформаційної безпеки. Виділяють чотири різновиди цифрової компетентності: інформаційна та медіакомпетентність, комунікативна, технічна та споживча компетентність.

Іншою стороною використання інтернет-технологій є використання різноманітних платформ для навчання, адже починаючи з 2020 року з

початком розповсюдження COVID-19 більшість навчальних закладів перейшли на дистанційну або змішану форму навчання. З використанням інтернет-мережі в учнів чи студентів може змінюватися світогляд, їх духовно-моральні позиції та поведінка в реальному світі.

2. Регулювання інформаційної безпеки в законодавстві та створення політик як зовнішньої, так і внутрішньої на основі внутрішніх положень організацій, підприємств, банку.

3. Наявність сучасних технічних засобів є важливим напрямком в інформаційній безпеці. Компанії, організації, держава повинні використовувати надійне програмне забезпечення та ефективні апаратні засоби для захисту від хакерських атак, шифрування інформації та інші заходи безпеки.

4. Міжнародне співробітництво, країни-держави між собою повинні ділитися досвідом в сфері інформаційної безпеки, співпрацювати між собою в сфері обміну інформацією щодо загроз, щодо розробки спільних стандартів безпеки, щодо координації заходів проти кіберзлочинності.

Національна безпека багатьох країн залежить від стану інформаційної безпеки, який вже кілька десятиліть відпрацьовується провідними країнами світу шляхом використання різних стратегій та тактик. Концепції інформаційних війн передбачають створення засобів небезпечного впливу на інформаційні сфери інших країн світу, порушення нормального функціонування інформаційно-телекомунікаційних систем, одержання несанкціонованого доступу до інформаційних ресурсів. Протиправне застосування спеціальних засобів впливу на індивідуальну, групову і суспільну свідомість формує особливу небезпеку.

5. Взаємодія всіх учасників, які задіяні в процесі забезпечення інформаційної безпеки. Лише спільними зусиллями можна досягнути ефективного результату шляхом взаємодії урядових організацій, освітніх установ, бізнесу та громадськості.

Важливим аспектом інформатизації, яка впливає на культуру особистості, є психологічний аспект: патологічні захоплення комп'ютерними іграми, Інтернетом, програмуванням та в загальному інформаційними технологіями для вчинення різноманітних злочинів в даній сфері [20].

Таким чином, в даному підрозділі було висвітлено значення інформаційної культури в епоху глобальної цифрової трансформації, були охарактеризовані чинники розвитку інформаційної культури суспільства, особистості, їх функції, були описані завдання державної культурної політики, проблеми в інформаційній сфері та напрями розвитку в інформаційній культурі.

Висновки до розділу 3

При вивченні питання інформаційної безпеки важливим аспектом є врахування досвіду міжнародних країн, зокрема країн з розвинутою економікою та країн, що входять до Європейського Союзу для ефективного забезпечення інформаційною політикою особистості, суспільства та держави.

Розробка та проведення інформаційної безпеки ведеться як на національному, так і на міжнародному рівнях.

Основним принципом Європейського Союзу в інформаційній сфері є інформаційна відкритість державної влади країн-учасників та ретельний захист персональних даних, який передбачає:

– власник персональних даних має пріоритетність у розпорядженні особистими даними;

– використання персональних даних лише з дозволу власника таких даних;

– використання персональних даних третіми особами вимагає покарання відповідно до законодавства.

Враховуючи досвід зарубіжних країн-членів ЄС в сфері захисту від кібератак та кіберзагроз, основними тенденціями є:

1. Законодавство та регулювання: більшість країн ЄС мають спеціальні закони та нормативно-правові акти, що регулюють забезпечення належного рівня захисту інформації.

2. Створення спеціалізованих центрів, що здійснюють аналіз, виявлення та реагування на кіберзагрози та співпрацюють з приватним сектором та академічною спільнотою для спільної боротьби з кіберзлочинністю.

3. Забезпечення безпеки критичної інфраструктури передбачає необхідність захисту критичної інфраструктури (фінансова сфера, транспорт, електроенергетика, телекомунікаційні мережі), для яких встановлюють єдині чіткі жорсткі критерії безпеки та вимоги до організацій, що здійснюють управління цими системами.

4. Інформаційні кампанії щодо кібергігієни, які передбачають поради та рекомендації щодо захисту персональних даних.

5. Міжнародне співробітництво: країни Європейського Союзу активно співпрацюють на міжнародному рівні для обміну інформацією про кіберзагрози та розробки спільних стратегій боротьби з кіберзлочинністю. Наприклад, Європейська агенція з мережевої та інформаційної безпеки (ENISA) сприяє співробітництву між країнами ЄС у цій сфері. Ці тенденції демонструють необхідність особливої уваги до інформаційної безпеки і підтверджують значення спільних зусиль у боротьбі з кіберзагрозами. Країни ЄС є прикладом ефективного управління інформаційною безпекою та успішно впроваджують стратегії та ініціативи для захисту своїх систем та громадян від кібернебезпек.

Основними напрямками вдосконалення системи захисту персональних даних є:

1. Постійне навчання та підвищення кваліфікації є одним з ефективних способів підвищення кваліфікації фахівців, які займаються захистом персональних даних. У зв’язку з розвитком інформаційних технологій

співробітники даної сфери повинні вдосконалювати свої знання та навички, щоб бути готовими до викликів в системі захисту персональних даних.

2. Використання існуючих систем аутентифікація та впровадження нових задля зберігання персональних даних в зашифрованому вигляді. Біометрична система аутентифікація представлена сканерами відбитків пальців, розпізнаванням обличчя чи голосу, що має на меті забезпечити високий рівень безпеки користувачів.

3. Розвиток системи обміну цифровими ідентифікаторами є важливим напрямом вдосконалення сфери захисту персональних даних, який забезпечує безпечний обмін персональними даними. Цифровими ідентифікаторами можуть виступати електронні паспорти або спеціальні програми для ідентифікації користувача в мережі.

4. Створення технологічних рішень для шифрування даних – це важливий напрямок вдосконалення системи захисту персональних даних, який включає відкриті ключі, асиметричні алгоритми та інші інноваційні методи, які забезпечують високий рівень захисту від несанкціонованого доступу до особистих даних громадян.

5. Застосування блокчейн-технологій – системи зберігання даних, що гарантує безпеку і недоступність для несанкціонованого доступу, та застосовується для зберігання та обробки персональних даних, що забезпечує надійний захист та контроль за використанням таких даних.

Основними напрямками розвитку культури інформаційної безпеки в епоху глобальної трансформації є:

1. Освіченість громадян та представників органів державної влади та органів місцевого самоврядування в питанні цифрової грамотності. Цифрова освіта має стати важливою частиною навчання, адже кожний громадянин, член суспільства, співробітник, представник влади повинен вміти відрізняти реальний сайт з фейковим сайтом та вміти боротися з різними схемами шахрайства (фішингом, вішингом та іншими відомими схемами шахрайства з використанням соціальної інженерії).

2. Регулювання інформаційної безпеки в законодавстві та створення політик як зовнішньої, так і внутрішньої на основі внутрішніх положень організацій, підприємств, банку.

3. Наявність сучасних технічних засобів є важливим напрямком в інформаційній безпеці. Компанії, організації, держава повинні використовувати надійне програмне забезпечення та ефективні апаратні засоби для захисту від хакерських атак, шифрування інформації та інші заходи безпеки.

4. Міжнародне співробітництво, країни-держави між собою повинні ділитися досвідом в сфері інформаційної безпеки, співпрацювати між собою в сфері обміну інформацією щодо загроз, щодо розробки спільних стандартів безпеки, щодо координації заходів проти кіберзлочинності.

5. Взаємодія всіх учасників, які задіяні в процесі забезпечення інформаційної безпеки. Лише спільними зусиллями можна досягнути ефективного результату шляхом взаємодії урядових організацій, освітніх установ, бізнесу та громадськості.

ВИСНОВКИ

1. Дослідження суті та значення інформаційної безпеки людини, суспільства, держави дає підстави підсумувати, що становлення та розвиток персональних даних містив в собі сім етапів, на кожному з яких проєкти законів вдосконалювалися та перевірялися на правомірність, затвердження та використання різноманітними верствами населення державою чи підприємствами, що в майбутньому дало підставу прийняти 1 червня 2010 року Закон України «Про захист персональних даних», який регулював суб'єкти відносин, їх права, об'єкти захисту, особливості вимоги до обробки персональних даних.

Інформаційна безпека – це життєво важлива складова національної безпеки, яка спрямована на забезпечення національних інтересів, та є самостійною складовою частиною поряд з інформаційними ресурсами, інформаційною структурою та інформаційними технологіями. Інформаційну безпеку можна розглядати як складову національної безпеки, як стан захищеності інформаційного середовища, як стан держави.

2. Аналіз інформаційних загроз в системі захисту персональних даних засвідчив, що інформаційні загрози та виклики – це можливі дії, процеси, явища, які мають негативний вплив на психічний стан та свідомість людини, які призводять до завдання їй шкоди в умовах глобального інформаційного суспільства, які є різноманітними за різними класифікаційними ознаками. На загрози інформаційній безпеці мають вплив політичні фактори (інформаційна експансія розвинених країн, критичний стан захисту інформації, зміна геополітичної ситуації, розширення міжнародної співпраці), економічні фактори (розширення кооперації з зарубіжними країнами, перехід на ринкові відносини в економіці, критичний стан вітчизняних галузей промисловості), організаційно-технічні фактори (широке використання незахищених програмних комплексів, недостатнє регулювання державою інформаційних

процесів, зростання інформації, що передається відкритими каналами зв'язку).

3. Дослідження методологічних підходів інформаційної безпеки людини, суспільства, держави дають змогу підсумувати, що поняття «інформаційна безпека» з'явилося наприкінці 80-х років завдяки працям німецького вченого Г. Одермана, який пояснював інформаційну безпеку як важливу інформаційну складову у міжнародній безпеці, а у вітчизняній літературі у 1991-1992 роках спостерігалася тенденція дослідження інформаційної безпеки. Інформаційну безпеку можна розглядати через призму науково-теоретичного підходу, професійно-практичного, буденно-повсякденного, науково-правового методу, герменевтичного підходу, підходу з точки зору соціальної філософії, феноменологічого, концептуально-теоретичного системного підходу, інтегрального, політико-правового підходу, синергетичного, історичного, технічного, міждисциплінарного підходів, інформаційного, формально-логічного підходів та дослідження даного поняття маю включати розгляд таких чинників, як потреби громадян, суспільства, держави і світового співтовариства; вплив інформаційних технологій на індивідів, суспільство і державу; наявність загроз і небезпек, якими повинна управляти система забезпечення інформаційної безпеки.

4. Аналіз забезпечення інформаційної безпеки в мережі Інтернет показав, що основними правилами безпечної роботи в мережі Інтернет є: використання ліцензійного програмного забезпечення, встановлення та оновлення антивірусного програмного забезпечення, використання надійних паролей та їх регулярна зміна, приєднання до перевірених Wi-Fi мереж та невикористання публічних мереж для входу в онлайн-банкінг, створення резервних копій даних та зберігання їх на носіях, відключених від мережі Інтернет, відкриття повідомлень лише від перевірених осіб.

5. Вивчення засад державного управління інформаційною безпекою в системі електронного врядування продемонструвало, що в нашій державі та

світі були випадки витоку персональних даних, зокрема на сайті при проходженні конкурсу на державну службу, дані клієнтів АТ КБ «Приватбанк», «Панамські папери», що полягали в розкритті міжнародних схем ухилення від податків через секретні рахунки в офшорних зонах.

Проблеми інформаційної безпеки можуть вирішуватися за допомогою:

– створення інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

– підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці;

– вдосконалення нормативно-правової бази щодо захисту інформаційних ресурсів, захисту персональних даних, протидії комп'ютерній злочинності;

– розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Державне управління в системі електронного врядування є важливою складовою забезпечення безпеки даних, які обробляються в державних структурах, що дає конфіденційність, цілісність та доступність даних та забезпечує довіру населення до електронного урядування, та включає такі аспекти:

1) виконання положень та стандартів інформаційної безпеки, яка містить правила щодо використання інформаційних систем, доступу до них, а також обмеження прав доступу до даних систем;

2) організація навчань та тренінгів для співробітників щодо інформаційної безпеки, що дає можливість підвищити обізнаність та зменшити ризики в інформаційній сфері;

3) впровадження та здійснення заходів технічного захисту інформації – систем захисту від несанкціонованого доступу, запобігання злому;

4) проведення аналізу і оцінка ризиків потенційних загроз в інформаційній безпеці системи електронного врядування;

5) управління різноманітними випадками в разі порушення безпеки даних (виявлення, розслідування та відновлення після інцидентів безпеки).

6. Дослідження основ захисту персональних даних у комерційних установах на прикладі банківських установ показало, що все більша кількість фізичних та юридичних осіб переходять на дистанційні канали обслуговування, що потребує більшої пильності задля захисту персональних даних від шахраїв. Саме для захисту персональних даних в банку потрібно дотримуватися таких правил: не розголошувати дані платіжної картки, контролювати стан банківського рахунку, підключити сповіщення до рахунку для отримання повідомлення про зарахування чи зняття коштів, не переходити за сумнівними посиланнями від незнайомих осіб, вводити дані картки лише на перевірених сайтах при оплаті за товар, захистити свій обліковий запис складним паролем, який буде використовуватися один раз лише при вході в один обліковий запис, створити додатковий захист з допомогою багатофакторної аутентифікації, запам'ятовувати PIN-код до картки та змінювати його хоча б раз на три місяці та не записувати та зберігати його разом з карткою.

7. Аналіз основних тенденцій зарубіжного досвіду у сфері інформаційної безпеки на прикладі країн ЄС показав, що потрібно враховувати міжнародні норми, закріплені в Статуті ООН, дотримуватися загальних принципів захисту персональних даних на прикладі досвіду зарубіжних країн, розглянути та застосувати досвід Північноатлантичного альянсу та Європейського Союзу та взяти до уваги інформаційну політику Німеччини, Польщі, Румунії, США, Канади, Грузії, де кожний правитель має свою специфіку забезпечення ефективної інформаційної безпеки як на рівні держави, так і на рівні окремого громадянина. Основними тенденціями захисту персональних даних з урахуванням досвіду країн ЄС є: законодавство та регулювання, що регулюють забезпечення належного рівня

захисту інформації; створення спеціалізованих центрів для здійснення аналізу, виявлення та реагування на кіберзагрози; забезпечення безпеки критичної інфраструктури; наявність інформаційних кампаній щодо кібергігієни; міжнародне співробітництво.

8. Перспективними напрямками вдосконалення системи захисту персональних даних є:

1) постійне навчання та підвищення кваліфікації;

2) використання існуючих систем аутентифікація та впровадження нових задля зберігання персональних даних в зашифрованому вигляді;

3) розвиток системи обміну цифровими ідентифікаторами є важливим напрямом вдосконалення сфери захисту персональних даних, який забезпечує безпечний обмін персональними даними;

4) створення технологічних рішень для шифрування даних – це важливий напрямок вдосконалення системи захисту персональних даних, який включає відкриті ключі, асиметричні алгоритми та інші інноваційні методи, які забезпечують високий рівень захисту від несанкціонованого доступу до особистих даних громадян;

5) застосування блокчейн-технологій – системи зберігання даних, що гарантує безпеку і недоступність для несанкціонованого доступу, та застосовується для зберігання та обробки персональних даних, що забезпечує надійний захист та контроль за використанням таких даних.

9. Аналіз дослідження формування культури інформаційної безпеки в епоху глобальної цифрової трансформації показав, що в умовах посилення цифрової трансформації зростає значення адаптації громадян до нових реалій в умовах цифрового середовища, підвищення поінформованості та набуття навичок протистояння інформаційним загрозам та ризикам. Водночас в умовах інформаційної війни, яку проводить Російська Федерація, основна увага в державній політиці надається боротьбі з загрозами інформаційної безпеки. Це правильно, оскільки завдання держави полягає в тому, щоб максимально захистити особу та соціум від деструктивного впливу

інформаційних ризиків. Однак донині в експертній спільноті склалося розуміння того, що в інформаційному середовищі не можна уникнути будь-яких факторів, що утворюють загрози. Це зумовлено багатьма причинами: складністю виявлення загроз інформаційній безпеці, латентним характером дії, чисельністю джерел загроз інформаційній безпеці, обмеженою ефективністю методів припинення поширення деструктивної інформації. Не можна забувати про те, що в правовій демократичній державі ступінь втручання в суспільне життя, у тому числі в духовну сферу, має бути лімітованим. Основними напрямками розвитку культури інформаційної безпеки в епоху глобальної трансформації є: освіченість громадян та представників органів державної влади та органів місцевого самоврядування в питанні цифрової грамотності; регулювання інформаційної безпеки в законодавстві та створення зовнішньої та внутрішньої політик; наявність сучасних технічних засобів, міжнародне співробітництво; взаємодія всіх учасників, які задіяні в процесі забезпечення інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авдєєва Т. Відповідність блокування соціальних мереж європейським стандартам свободи вираження поглядів. 29.11.2021. URL. https://cedem.org.ua/analytics/social-media-blocking/

2. Антонюк В. В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України: дис. канд. з державного управління: спец.: 25.00.02. Київ, 2017. 218 с.

3. Баран М. В. Захист прав людини в умовах розвитку цифрових технологій і формування інформаційної безпеки. Теоретико-прикладні проблеми правового регулювання в Україні: матеріали V Всеукраїнської науково-практичної конференції (м. Львів, 10 грудня 2021 р.) / за заг. ред. І. В. Красницького. Львів: ЛьвДУВС, 2021. С. 13-16.

4. Баранов А. А., Брыжко В., Базанов Ю. Защита персональных данных. Киев: ВАТ КП ОТИ, 1998. 128 с.

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

6. Боднар Г.Л., Ракутіна Л.О. Інформаційна політика та інформаційна безпека. Публічне управління та адміністрування, №4 (23), 2019. – с. 42-49.

7. Бондаренко Р.В., Михальчук В.М. Інформаційна безпека держави/Р.В. Бондаренко, В.М. Михальчук// Інвестиції: практика та досвід №5/2021 – с. 95-101.

8. Бортник Н., Єсімов С. Відносини в мережі Інтернет як об’єкт правового регулювання. Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки. 2019. Випуск 22. С. 147-153.

9. Брижко В.М. Захист персональних даних: реалії та практика сучасності. Інформація і право 2013. №3(9). с. 31-48.

10. Брижко В. Правовий захист та безпека персональних даних: соціальний і комерційний аспекти. Інформація і право. № 3(26)/2018. С. 16-37.

11. Брижко В.М., Швець М.Я. е-боротьба в інформаційних війнах та інформаційне право: монографія / за ред. члена-кореспондента АПрН України, д.е.н., професора М. Швеця. Київ: НДЦПІ АПрН України, 2007 р. 236 с.

12. Брижко В. Сучасні основи захисту персональних даних в європейських правових актах. Інформація і право. № 3(18)/2016. С. 45-57.

13. Вас зламають за 1 секунду: названі найпопулярніші та найнебезпечніші паролі 2023 року https://minfin.com.ua/ua/2023/11/17/116186802/

14. Васєв В.О. Підвищення ефективності державного контролю в сфері захисту інформації. Реформування публічного управління та адміністрування: теорія, практика, міжнародний досвід : матеріали Всеукраїнської науково-практичної конференції за міжнародною участю. Одеса : ОРІДУ НАДУ, 2017. С. 214–216.

15. Вінник О. Цифровізація в ракурсі державної економіко-правової політики. Підприємництво, господарство і право. 2020. № 8. С. 61-70

16. Геворкян А. Ю. Формування основ культури інформаційної безпеки суспільства як фактор зміцнення національної безпеки. Вісник Національного університету цивільного захисту України. Серія «Державне управління». 2021. № 1 (14). С. 168-177.

17. Гнатюк С.Л. Особливості захисту персональних даних у сучасному кіберпросторі: правові та техніко-технологічні аспекти: аналіт. доп. Київ: НІСД. 2014. с. 52-55.

18. Гур’єв В.І. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур’єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук’яненко В.В. ТПК «Орхідея», 2018. – 166 с. : іл.

19. Дмитришин М.В., Жураківська М.І. Витік персональних даних в електронному урядуванні. Публічне управління і адміністрування в Україні. Випуск 20, 2020 – с. 111-119 (с.117).

20. Довгань О.Д. Теоретико-правові основи забезпечення інформаційної безпеки України: дис. ... д-ра юрид. наук. Київ, 2016. 453 с.

21. Довгань О. Д., Ткачук Т. Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. Інформація і право. 2018. № 2 (25). С. 73-85.

22. Жарков Я.М., Дзюба М.П., Замаруєва І.В. Інформаційна безпека особистості, суспільства, держави // Підручник – К. 2008. – с. 274.

23. Живко З.Б.. Живко М.О. Інформаційні загрози: суть і проблеми// Тези доповідей II міжнародної НПК «Безпека та захист інформації в інформаційних системах» - с. 116-118.

24. Жураковський Б. Ю., Зенів І. О. Технології Інтернету речей. Навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2021. 271 с.

25. Забара І.М. Міжнародна інформаційна безпека: сучасні концепції в міжнародному праві. Теорія і практика правознавства. 2013. Вип. 2

26. Захаренко К. В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири. / К. В. Захаренко. Київ. 2021.с.423.

27. Захарченко В. К. інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири: дис. д-ра політичних наук: спец. 23.00.02. Київ, 2021. 423 с.

28. Збитки від карткового шахрайства торік зросли на 46% – НБУ**:** Економічна правда: https://www.epravda.com.ua/news/2023/05/3/699747/.

29. Золотар О.О. Правові основи інформаційної безпеки людини: дис. д-ра юрид. наук. Київ, 2018. 499 с.

30. З яких соцмереж українці отримують інформацію? Опитування. 15.02.2022. URL. https://life.pravda.com.ua/society/2022/02/15/247467/

31. Ільницька Уляна. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам // Політичні науки. №1, 2016 – с. 27-32.

32. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с. : іл.

33. Калюжний Р. Питання концепції реформування інформаційного законодавства України / Калюжний Р., Говловський В., Цимбалюк В., Гузалюк М. // Збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». К.: НТУУ «КПІ», Міністерство освіти і науки України, СБУ. – К. – 2000. – С. 17-21.

34. Кісілевич-Чорнойван О. Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять // Юриспруденція: теорія і практика. 2009. № 8. С. 11–18.

35. Климчук О.О., Ткачук Н.А. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 3 (19). С. 75–83.

36. Коваль З. Політико-правові механізми державного управління інформаційно-психологічною безпекою України: автореф. дис. канд. н. з держ. упр. (спеціальність: 25.00.02 – механізми державного управління). Одеса. 2011. 22 с.

37. Конституція України [Електронний ресурс] // Відомості Верховної Ради України (ВВР). – 1996. – № 30. – с. 141. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

38. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: навч. посіб. К.: Кондор, 2008. 382 с.

39. Кочубей Л.О. (2015). Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-комунікаційних технологій у сучасному Донбасі). Наукові записки Інституту політичних і етнонаціональних досліджень імені І. Ф. Кураса. Вип. 3. 220—237

40. Кушнерьов О.С. Безпека інформації : конспект лекцій / укладач О. С. Кушнерьов. – Суми : Сумський державний університет, 2021. – 99 с.

41. Краковська А. Є., Бабик М. К. Цифровізація адміністративних послуг в Україні: проблеми та перспективи розвитку. Науковий вісник Ужгородського Національного Університету. Серія право. 2022. Випуск 70. С. 329-334.

42. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції: навч. посібник. Київ: КНТ, 2006. 280 с.

43. Ліпкан В.А. Національна безпека України: навч. посіб. К.: КНТ, 2009. 576 с.

44. Ліпкан В. А., Максименко Ю. С., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції. Київ: .КТН, 2006. 280 с.

45. Линник Г.М. Адміністративно-правове регулювання інформаційної безпеки України: автореф. дис., канд. юрид. наук: 12.00.07 - адміністративне право і процес; фінансове право; інформаційне право / Національний університет біоресурсів і природокористування України. Київ, 2013. 27 с.

46. Малик Я., Береза О. Забезпечення інформаційної безпеки України у контексті світового досвіду. Ефективність державного управління. 2012. № 32. С. 20 – 27.

47. Меджибовська Н. Банківські послуги та Інтернет / Н. Меджибовська // Банківська справа. – 2011. – № 5. – С. 41-43

48. Мельник К.С. Іноземний та вітчизняний досвід становлення інституту захисту персональних даних / К.С. Мельник //Інформаційна безпека людини, суспільства, держави. 2013. № 2(12). С. 97–103.

49. Мельник С.В. Понятійно-категоріальний апарат у системі професійної підготовки майбутніх фахівців з кібербезпеки. Інформаційні технології і засоби навчання. 2016. Т. 55. №5. С. 187–197.

50. Молодецька-Гринчук К. В. Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних Інтернет-сервісах: автореф. дис. д-ра технічних наук: спец.: 21.05.01. Київ, 2018. 42 с.

51. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.

52. Ніщименко О.А. (2016). Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. № 1. 17—23.

53. Олійник О.В. Інформаційна безпека України: доктрина адміністративно-правового регулювання: автореф. дис. …док. юрид. наук: 12.00.07 - адміністративне право і процес; фінансове право; інформаційне право / Інститут законодавства Верховної Ради України. Київ, 2013. – 34 с.

54. Оніщенко В.В. Захист персональних даних. URL: http://jrnl.nau.edu.ua/index.php/UV/article/viewFile/6540/7311.

55. Осадца Іван. (2014). Новітні тенденції на ринку Інтернет-реклами в Україні та світі: підходи до теми. Медіафорум : аналітика, прогнози, інформаційний менеджмент, Вип. 2-ий, С. 134-145. https://journals.chnu.edu.ua/index.php/mediaforum/issue/view/4/2

56. Осадца Іван. (2013). Правове регулювання виробництва, розповсюдження та споживання Інтернет-реклами в Україні. Історико-політичні проблеми сучасного світу, Т. 25-26, С. 107-110.

57. Офіційний сайт Національного банку України [Електронний ресурс]. – Режим доступу: www.bank.gov.ua.

58. Офіційний сайт ПАТ КБ «Приватбанк» [Електронний ресурс]. – Режим доступу: https://privatbank.ua/

59. Офіційний сайт АТ «Ощадбанк» [Електронний ресурс]. – Режим доступу: https://www.oschadbank.ua/

60. Офіційний сайт АТ «Укрексімбанк» [Електронний ресурс]. – Режим доступу: https://www.eximb.com/

61. Офіційний сайт АБ «Укргазбанк» [Електронний ресурс]. – Режим доступу: https://www.ukrgasbank.com/

62. Офіційний веб-сайт Міністерства інформаційної політики України URL :http://mip.gov.ua.

63. Офіційний сайт ПУМБ [Електронний ресурс]. – Режим доступу: https://www.pumb.ua/

64. Офіційний сайт Universal Bank [Електронний ресурс]. – Режим доступу: https://www.universalbank.com.ua/

65. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: дис. … канд. юрид. наук: спец.: 12.00.07. Львів, 2019. 268 с. – с.84-85

66. Пилипчук В.Г., Брижко В.М. Трансформація системи захисту персональних даних та приватності в контексті євроінтеграції України/ В.Г. Пилипчук, В.М. Брижко // Вісник Національної академії правових наук України № 3 (90) 2017 – с. 36-50.

67. Політанський В.С. Світові моделі та фундаментальні принципи інформаційного суспільства. Науковий вісник Ужгородського національного університету. Серія «Право». 2017. Вип. 43. Т. 1. С. 34–39.

68. Про авторське право і суміжні права: Закон України від 23.12.1993 р. № 3792-XII. URL. https://zakon.rada.gov.ua/laws/card/3792-12

69. Про адміністративні послуги: Закон України від 06.09.2012 р. № 5203-IV. URL. https://zakon.rada.gov.ua/laws/show/5203-17/conv#n43

70. Про банки і банківську діяльність [Електронний ресурс]: Закон України, від 07 грудня 2000 року №2121-III, із змінами і доповненнями / Верховна Рада України. – Режим доступу: zakon.rada.gov.ua.

71. Про Державну службу спеціального зв’язку та захисту інформації України : Закон України від 23.02.2006 р. № 3475-IV: https://zakon4.rada.gov.ua/

72. Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII: http://zakon.rada.gov.ua/

73. Про доступ до публічної інформації: Закон України від 13.01.11 р. № 2939-VI. URL: http://zakon3.rada.gov.ua/

74. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. №80/94-ВР: https://zakon.rada.gov.ua/

75. Про захист персональних даних [Електронний ресурс]: Закон України, від 01 червня 2010 року №2297-VI, із змінами і доповненнями / Верховна Рада України. – Режим доступу: zakon.rada.gov.ua

76. Про затвердження Правил зберігання, захисту, використання та розкриття банківської таємниці: Постанова Правління Національного банку України від 06 вересня 2023 року №z0935-06, із змінами і доповненнями / Верховна Рада України. – Режим доступу: zakon.rada.gov.ua.

77. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII: http://zakon.rada.gov.ua/

78. Про хмарні послуги: Закон України від 17.02.2022 р. № 2075-IX. URL. https://zakon.rada.gov.ua/laws/show/2075-20#Text

79. Про критичну інфраструктуру: Закон України від 16.11.2021 р. №1882-IX. URL. https://zakon.rada.gov.ua/laws/show/1882-20/conv#n410

80. Про національну безпеку: Закон України від 21.06.18 р. № 2469-19. URL: http://zakon2. rada.gov.ua/laws/show/2469-19.

81. Про Національну програму інформатизації [Електронний ресурс]: Закон України, від 01 грудня 2022 року №2807-IX, із змінами і доповненнями / Верховна Рада України. – Режим доступу: zakon.rada.gov.ua.

82. Про Національну систему конфіденційного зв’язку [Електронний ресурс]: Закон України, від 10 січня 2022 року №2919-III, із змінами і доповненнями / Верховна Рада України. – Режим доступу: zakon.rada.gov.ua.

83. Про Службу безпеки України : Закон України від 25.03.1992 р. № 2229-XII. : https://zakon.rada.gov.ua/

84. Про Стратегію інформаційної безпеки [Електронний ресурс]: Указ Президента України від 28 грудня 2021 року №685/2021/ Верховна Рада України. – Режим доступу: zakon.rada.gov.ua

85. Про Стратегію кібербезпеки України [Електронний ресурс]: Указ Президента України від 26 серпня 2021 року №447/2021 / Верховна Рада України. – Режим доступу: zakon.rada.gov.ua.

86. Портал prozorro.gov.ua : вебпортал. URL:https://prozorro.gov.ua Рогова О.Г. Захист персональних даних у законодавстві Європейського союзу. URL: http://www.kbuapa.kharkov.ua/e-book/tpdu/2011-3/doc/5/05.pdf.

87. Про публічні електронні реєстри: Закон України від 18.11.2021 р. № 1907-IX. URL. https://zakon.rada.gov.ua/laws/show/1907-20/conv#n472

88. Половинчак Ю. Особливості інтерактивного простору соціальних медіа в контексті реалізації маніпулятивних технологій. 2018. URL. https://ipiend.gov.ua/wp-content/uploads/2018/07/polovynchak_osoblyvosti.pdf

89. Рамський Ю.С. Формування інформаційної культури особи – пріоритетне завдання сучасної освітньої діяльності. // Науковий часопис НПУ імені М.П. Драгоманова. Серія №2: Комп'ютерно-орієнтовані системи навчання. – К.: НПУ імені М.П. Драгоманова, 2004. – № 8 (1). – С. 19–42.

90. Ронжес О. Є. Визначення рівня цифрової компетентності як необхідної навички в умовах переходу до цифрової держави. Проблеми політичної психології. 2021. Випуск 10 (24). С. 331-348.

91. Семенченко А.І., Дрешпака В.М. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2017

92. Скочиляс-Павлів О.В. Сучасні загрози інформаційній безпеці України в умовах правового режиму воєнного стану // Юридичний науковий електронний журнал - №9/2023. – с. 263-266.

93. Слабкий Г. О., Жданова О. В. Європейські підходи до подолання *у* населення Інтернет-залежності. Здоров'я нації. 2019. № 2 (55). С. 198-201.

94. Солонина Є.О. Злив персональних даних українців: що сталося і як захиститися. *Радіо Свобода* : вебсайт. URL: https://www.radiosvoboda.org/a/zlyv-danyxi-diya/30610626.html

95. Сопільник Л., Ковалів М., Єсімов С. і інші. Розвиток цифрової економіки в контексті забезпечення інформаційної безпеки в Україні. Traektoriâ Nauki = Path of Science. 2020. Vol. 6. № 5. S. 2023-2032.

96. Тихомирова Є.Б., Смик Р.П. Інформаційна політика Польщі. Сучасні проблеми гуманітаристики: світоглядні пошуки, комунікативні та педагогічні стратегії : матеріали V Всеукраїнської науково-практичної конференції. Рівне, 2015. С. 113–115.

97. Н. В. Медіа, інформаційна і комп'ютерна грамотність як компоненти цифрової грамотності. Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична. 2021. Випуск 29. С. 46-56.

98. Ткачук П.П., Гула Р.В., Сивак О.І., Щурко О.М., Шемчук В.В. Інформаційна війна і національна безпека: монографія. Л.: НАСВ, 2015. 265 с.

99. Триняк В. Інформаційна безпека як соціокультурний феномен (соціальнофілософський аналіз): автореф. дис. канд. філос. н. (спеціальність: 09.00.03 -соціальна філософія та філософія історії). Дніпропетровськ. 2009. 24 с. – с.11.

100. Український Інтернет-банкінг – проблеми та перспективи [Електронний ресурс]. – Режим доступу: http://uastudent.com/ukrainskyj-internet-bankingproblemy-ta-perspektyvy/

101. У Польщі створили Центр із протидії російській пропаганді. URL: https://www.ukrinform.ua/rubric-world/2220050-u-polsi-stvorili-centriz-protidii-rosijskij-propagandi.html.

102. Уханова Н.С. Виклики і загрози правам та безпеці людини в інформаційній сфері/Н.С. Уханова// Інформація і право.- № 4(27)/2018 – с. 33-45.

103. Фань Ч. Правове забезпечення інформаційної безпеки в системі сучасної міжнародної співпраці // Наукові праці МАУП. 2012. Вип. 4 (35). С. 110–115.

104. Філіпенко А. С. Міждисциплінарна методологія: базові принципи. International relations, part «Economic sciences». 2018. № 13. С. 7-13.

105. Цимбалюк В.С., Бабінська А.В. (2014). Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики. Адміністративне право і процес. № 2 (8). 22—30

106. Черевко О.В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту// Ефективна економіка №5, 2014 – с.

107. Чернухін І. О. Досвід Федеративної Республіки Німеччини в побудові системи захисту інфраструктури від кібернетичних загроз. Інформаційна безпека людини, суспільства, держави. 2014. № 1. С. 28 – 43.

108. Чуб О. О. Розвиток Інтернет-банкінгу в глобальному середовищі [Текст] / О. О. Чуб // Вісник Української академії банківської справи. – 2009. – № 1 (26). – С. 62–67.

109. Шалига Т. С. Дистанційне банківське обслуговування роздрібних клієнтів: монографія / Т. С. Шалига. – Ніжин: Аспект-Поліграф, 2014. – 412 с.

110. Шемчук В. В. Інформаційна безпека та інформаційна оборона в контексті розвитку вітчизняної доктриний законодавчої основи / В. В. Шемчук // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Юридичні науки. - 2019. - Т. 30(69), № 4. - С. 31-37.

111. Щепанківський В. Г. Інформаційна безпека як складова образу країни. *Актуальні проблеми міжнародних відносин*. 2011.Вип. 102. Ч. 1. С. 219 – 228.

112. Що таке фішинг і як від нього захиститись? URL. https://www.fg.gov.ua/articles/50140-shcho-take-fishing-i-yak-vidnogozahistitis.html

113. Юденков Н. М. Інтернет-технології в банківському бізнесі: перспективи і ризики [Текст]: учбово-практичний посібник / Н. М. Юденков, И. С. Сандалов, С. Л. Ермаков. – М.: КНОРУС, 2010. – 320 с.

114. Юдін О. К., Богуш В. М. Інформаційна безпека держави: Навчальний посібник. - Харків: Консум. - 576с.

115. Яковлєв П.О. Досвід державного регулювання забезпечення інформаційної безпеки зарубіжних держав (на прикладі Сполучених Штатів Америки, Канади, Німеччини, Франції)// Вісник Харківського національного університету імені В. Н. Каразіна. Серія «ПРАВО». Випуск 30, 2020.

116. Abomhara M., Koien G. Cyber Security and the Internet Of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security. 2015. Vol. 4. P. 65-88.

117. Baker J. Process, Practice and Principle: Teaching National Security Law and the Knowledge that Matters Most. The Georgetown Journal of Legal Ethics. 2014. Vol. 27. P. 163-189.

118. Bilynska M. (2018). The Formation of the Paradigm of National Resilience in the State Administration of Ukraine. International Scientific Journal «Progress». vol. 1-2. pp. 41-45.

119. GDPR – нові виклики для обробників персональних даних / К. Тищенко / Юридична газета online. URL: http://yur-gazeta.com/ publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/gdpr--novi-vikliki-dlya-obrobnikiv-personalnih-danih-vukrayini.html.

120. Shaw T.J. Information security and privacy: A practical guide for global executives, law technologists. Chicago: American Bar Association. 2011. P. 17. URL: http://faculty.cbpa.drake.edu/dmr/0101/DMR010113B.pdf

121. Shohruh Rahmat. Organyi obespecheniya informatsionnoy bezopasnosti: zarubezhnyiy opyit. Internet-sayt «ictnews». URL: https://ictnews.uz/27/02/2018/infosec-agencies/

122. The Administration’s Priorities on Cybersecurity. White House. URL: https://www.whitehouse.gov/issues/foreign policy/cybersecurity#section-protect-critical-infrastructure

123. The Economist: З травня 2018-го у ЄС почне діяти новий закон про захист конфіденційних даних / Тиждень.UA. 5 січня 2018 року. URL: http://tyzhden.ua/News/207156.

124. Panama papers. URL: https://panamapapers.sueddeutsche.de/en/

125. Recommendation CM/Rec (2016)5 of the Committee of Ministers to member States on the Internet freedom. URL: https://
search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa.

126. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=ENм.

LE RÈSUMÈ

Le mémoire de maîtrise est consacré à l'étude du système de protection des données personnelles dans le cadre de la garantie de la sécurité de l'information d'une personne, de la société et de l'État. L'auteur a examiné l'essence, la signification et les approches méthodologiques de la sécurité de l'information de l'individu, de la société et de l'État, les menaces pouvant survenir dans le système de protection des données personnelles et les moyens de les éviter. L'ouvrage met également en évidence l'état actuel de la garantie de la sécurité des informations d'une personne, de la société et de l'État, y compris les principaux types de fraude sur Internet et les méthodes permettant de les prévenir. Dans ce travail, le chercheur s'est concentré sur les domaines d'amélioration du système de protection des données personnelles sur la base de l'expérience étrangère dans le domaine de la sécurité de l'information. Un aspect important pour assurer la sécurité de l'information est la formation d'une culture dans ce domaine dans les conditions de la transformation numérique mondiale.

Dans le premier chapitre, des informations ont été mises en évidence sur la signification et l'importance des technologies de l'information, l'essence des données personnelles, leur protection et l'histoire de leur formation à toutes les étapes de développement, le système de protection des données personnelles a été caractérisé, et l'essence de la sécurité de l'information, son interprétation de différents points de vue et sa composition ont été définis, les objectifs de mise en œuvre de la stratégie de sécurité de l'information et les tâches définies pour atteindre les objectifs, les fonctions de sécurité de l'information, les niveaux auxquels la sécurité de l'information peut être mis en œuvre sont caractérisés, l'essence et la signification des menaces informatiques ont été caractérisées, leurs types selon diverses caractéristiques de classification, les actions d'information dangereuses ont été mises en évidence, ainsi que les facteurs, les menaces pour la sécurité de l'information et leurs sources conformément aux intérêts de l'individu,

la société et l'État dans le domaine de la sécurité de l'information, les défis mondiaux et nationaux ont été présentés et les menaces dans la sphère de l'information, les approches méthodologiques pour la définition de la sécurité de l'information, les principes d'analyse de la sécurité de l'information ont été définis, divers objets de la sécurité de l'information ont été caractérisés, les facteurs d'assurer la sécurité de l'information de l'État, ainsi que la législation dans le domaine de la sécurité de l'information ont été soulignées.

La deuxième section est consacrée aux règles de sécurité du travail sur Internet, aux recommandations pour la protection de la sécurité de l'information dans les réseaux sociaux, dans le domaine de la collecte de données, dans la correspondance électronique, dans les pouvoirs publics lorsque les salariés exercent leurs fonctions fonctionnelles, et est également consacré au type de fraude le plus courant - l'ingénierie sociale, le système de sécurité de l'information a été décrit, ses objectifs, ses tâches, ses problèmes et ses solutions ont été précisés, les organismes publics impliqués dans le processus visant à assurer la sécurité de l'information de l'État ont été indiqués et les les aspects clés de la gestion étatique de la sécurité de l'information dans le système d'administration électronique ont été caractérisés, les services bancaires fournis à l'aide des technologies Internet ont été caractérisés, des modèles de services bancaires sur Internet, des statistiques de transactions frauduleuses avec des cartes de paiement ont été présentées, les plus les stratagèmes de fraude courants et les moyens de s'en protéger ont été présentés.

Le troisième chapitre a analysé l'expérience des pays de l'Union européenne et des pays hautement développés qui ne sont pas membres de l'Union européenne, l'interprétation de la question de la « sécurité internationale de l'information » de différents points de vue, a décrit les normes internationales liées à la sphère de l'information, les principes sur lesquels repose la protection des données personnelles, ainsi que les principales tendances de l'expérience internationale dans le domaine de la sécurité de l'information, ont souligné l'importance de la culture de l'information à l'ère de la transformation numérique mondiale, les facteurs de le développement de la culture de l'information de la société, des individus, leurs

fonctions ont été caractérisés, les tâches de la politique culturelle de l'État, les problèmes dans le domaine de l'information et les orientations du développement de la culture de l'information ont été décrits.