ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА ІМЕНІ ЛЕОНІДА ЮЗЬКОВА
ФАКУЛЬТЕТ ПУБЛІЧНОГО УПРАВЛІННЯ

Кафедра: публічного управління та адміністрування

МАГІСТЕРСЬКА РОБОТА

на здобуття освітнього ступеня магістра
на тему:

Публічне управління у сфері забезпечення інформаційної безпеки України

Виконала: студентка магістратури за спеціальністю 281 Публічне управління та адміністрування заочної форми навчання
Щансевич Карина Миколаївна
(прізвище та ініціали)

Керівник: **Шевчук Інна Володимирівна,** д.держ.упр., доцент, професорка кафедри
(прізвище та ініціали)

Рецензент: _____
(прізвище та ініціали)

Хмельницький – 2023 рік

Анотація

Щансевич К. М. Публічне управління у сфері забезпечення інформаційної безпеки України. Кваліфікаційна наукова праця на правах рукопису. Магістерська робота на здобуття освітнього ступеня магістра за спеціальністю 281 Публічне управління та адміністрування. Хмельницький університет управління та права імені Леоніда Юзькова, Хмельницький, 2022. 76 с.

Визначено сутність інформаційної безпека діяльності органів публічного управління. Проведено аналіз світового досвіду у сфері забезпечення інформаційної безпеки.

Здійсненоаналізі інституційного забезпечення захисту інформації в Україні. Досліджено роботу Державної служби спеціального зв'язку та захисту інформації України, що є центральним виконавчим органом зі спеціальним статусом, який діє під керівництвом Кабінету Міністрів України.

Запропоноано шляхи підвищення рівня інформаційної безпеки в органах публічного управління. Зазначено, що завдання адміністративного рівня боротьби з загрозами інформаційної безпеки повинно включати ключові кроки, такі як визначення керівних документів і стандартів, методів управління ризиками та проведення сертифікації відповідності стандартам інформаційної безпеки.

Описано організаційні принципи впровадження інформаційного аудиту з метою підвищення інформаційної безпеки в органах публічного управління. Запропоновано організаційну модель аудиту інформаційної безпеки в органах публічного управління.

Ключові слова: інформаційна безпека, публічне управління у сфері інформаційної безпеки, стандарти інформаційної безпеки органів публічного управління, аудит інформаційної безпеки органів публічного управління.

Abstract

Shchansevich K. M. Public management in the sphere of ensuring information security of Ukraine. Qualifying scientific paper on copywriting. Master's degree work for obtaining an open master's degree in the specialty 281 Public management and administration. Khmelnytskyi Leonid Yuzkov University of Management and Law, Khmelnytskyi, 2023. 76 p.

The essence of information security of activities of public administration bodies is defined. An analysis of world experience in the field of information security was carried out.

An analysis of the institutional provision of information protection in Ukraine was carried out. The work of the State Service for Special Communications and Information Protection of Ukraine, which is a central executive body with a special status that operates under the leadership of the Cabinet of Ministers of Ukraine, was studied.

Ways to increase the level of information security in public administration bodies are proposed. It is noted that the task of the administrative level to combat information security threats should include key steps, such as the definition of guiding documents and standards, risk management methods and certification of compliance with information security standards.

The organizational principles of information audit implementation in order to improve information security in public administration bodies are described. An organizational model of information security audit in public administration bodies is proposed.

Keywords: information security, public administration in the field of information security, information security standards of public administration bodies, audit of information security of public administration bodies.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Інформаційна безпека в системі національної безпеки України займає ключову позицію, оскільки в сучасному світі інформація, яка постійно зазнає якісних та кількісних змін, вважається найціннішим глобальним ресурсом. Інформаційні відносини стають необхідною складовою всіх процесів у державі та суспільстві. З урахуванням зростання вразливості інформаційного суспільства до недостовірної та деструктивної інформації, зокрема внаслідок злочинів в інформаційній сфері, надання інформаційної безпеки стає пріоритетним завданням державної політики. Стаття 17 Конституції України визначає захист суверенітету, територіальної цілісності та забезпечення економічної та інформаційної безпеки як найважливіші функції держави, яка покладається на всі органи влади, місцеве самоврядування, підприємства та громадян. Ці принципи відображені у Стратегії національної безпеки України та вимагають розробки ефективних правових актів, впровадження безпечних інформаційних технологій, створення національної інфраструктури та розвитку інформаційних відносин.

Глобальний розвиток дистанційних комунікацій, інформаційних технологій і продуктів призводить до появи нових суспільних відносин в інформаційній сфері, економіці та виробництві, що є ключовою рисою сучасної цивілізації. Ці процеси відзначаються глобалізацією, яка проникає в усі аспекти людського життя, сприяючи розвитку інформатизації та формуванню нових світоглядних та стереотипів серед населення.

Проведені зарубіжними та вітчизняними авторами дослідження в сфері забезпечення інформаційної безпеки (В.П. Бабак [2], В.М. Брижко[10], П.Д. Біленчук[7], С.П. Головань [17], В.О. Голубев [18], В.П. Горбулін [20], М.В. Карчевський [33], Б.А. Кормич [37-40], О.А. Олійник [51], В.М. Петрик [58], Н.А. Савінова [85], О.О. Смірнов [92], .О. Шепета [103], О.О. Шиверський [104], В.І. Ярочкин [107] та ін.) в основному стосуються

захисту прав громадян на інформацію та боротьби зі злочинністю в інформаційній сфері.

Проте, на сьогодні виникає надзвичайно актуальна наукова проблема, яка полягає у необхідності визначення політичних, правових і в цілому концептуальних засад удосконалення публічного управління у сфері забезпечення інформаційної безпеки в Україні.Це обумовлює актуальність обраної теми дослідження.

Мета і завдання дослідження. Метою магістерської роботи є виявлення і систематизація проблем захисту інформації як складової (підсистеми) інформаційної безпеки України, обґрунтування правових і організаційних засад, удосконалення цієї діяльності.

Визначена мета зумовила постановку наступних завдань дослідження:

– визначити сутність інформаційної безпеки в публічному управлінні;

– систематизувати досвід зарубіжних країн у сфері захисту інформації;

– проаналізувати інституційне забезпечення захисту інформації в Україні;

– охарактеризувати практику реалізації функцій Державної служби спеціального зв’язку у сфері забезпечення інформаційної безпеки;

– визначити пріоритетні напрями підвищення ефективності заходів інформаційної безпеки в органах публічного управління;

– запропонувати шляхи впровадження інформаційного аудиту з метою підвищення інформаційної безпеки органів публічного управління.

Об’єктом дослідження є суспільні відносини у сфері публічного управління у сфері забезпечення інформаційної безпеки України.

Предметом дослідження є напрями удосконалення публічного управління у сфері забезпечення інформаційної безпеки України.

Методи дослідження.Методологічну основу роботи складають загальновизнані методи пізнання і розкриття змісту соціально-правових явищ у сфері інформації.

В основу магістерського дослідження покладено метод системного аналізу і синтезу, що дозволило визначити захист інформації як складову загальної системи інформаційної безпеки, виявити їх співвідношення, взаємодію та взаємозалежність.Для розв'язання поставлених завдань використані також методи:діалектичний (засоби захисту інформації розглядаються у нерозривному зв'язку їх юридичного закріплення та соціального і політичного впливу на суспільні відносини);інформаційно-кібернетичний (система інформаційної безпеки розглядається через призму інформаційних складових основних сфер соціальної діяльності, які містять певну інформацію обмеженого доступу);порівняльно-правовий (використовувався при з'ясуванні співвідношень понять внутрішньої і зовнішньої інформаційної політики, а також для дослідження трансформації пострадянської системи захисту інформації та аналізу документальних джерел: норм міжнародного права, міждержавних угод України, вітчизняної законодавчої бази та нормативно-правових актів інших країн).

Інформаційна база дослідження є законодавчі та нормативні акти України з питань захисту інформації, розвитку державної інформаційної політики, офіційні матеріали Державної служби статистики України, нормативно-правові акти органів публічного управління, монографії і статті вітчизняних і зарубіжних авторів.

Практичне значення одержаних результатів полягає в тому, що дослідження дозволило сформулювати та висвітлити низку важливих положень, пов'язаних з удосконаленням правових основ та організаційних засад забезпечення інформаційної безпеки в Україні.

Структура та обсяг магістерської роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел, який налічує 104 найменування. Робота містить 5 рисунків та 2 таблиці. В цілому обсяг дослідження становить 76 сторінок.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ЗАБЕЗПЕЧЕНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Сутність інформаційної безпеки в публічному управлінні

Аналіз існуючої категоріальної бази слід почати з розгляду сутності терміну "безпека". Найчастіше безпеку розглядають як стан, коли відсутня небезпека, тобто "...факторів і умов, що можуть загрожувати існуванню безпосередньо індивіда або їх спільноти у формі сім'ї, населеного пункту або держави..." [20, с. 56].

Загальноприйняте визначення безпеки визначається як "стан, при якому немає загрози для кого-небудь або чого-небудь" [45, с. 67]. У свою чергу, поняття "небезпека" тлумачиться як можливість чогось небезпечного, здатного завдати шкоди [45, с. 147]. А "загроза" у літературі розкривається як "реальна небезпека, реальна можливість заподіяти шкоду, ймовірність настання описаного поєднання ситуації і стану взаємодії об'єктів, засобів і результатів, що створює реальну небезпеку" [10, с. 284].

Безпека часто визначається як здатність об'єкта зберігати свої найважливіші, системоутворюючі властивості, основні характеристики та параметри, навіть при наявності деструктивних та дезорганізуючих впливів (зовнішніх та/або внутрішніх). Втрата цих елементів може призвести до втрати об'єктом своєї сутності, тобто бути самим собою [90, с. 11]. Декілька дослідників визначають безпеку як систему гарантій, що забезпечують нормальний розвиток об'єкта.

Практично всі наведені вище визначення продовжують бути предметом критики як з боку фахівців-практиків, так і з боку вчених [20, с. 54].

Сутність безпеки не може існувати без її діалектичної протилежності – небезпеки. Комплекс небезпек завжди присутній. Поняття "небезпека" описує стан об'єкта, при якому загроза його існування, через розрив або спотворення

важливих зв'язків і відносин в системі, перевищує суб'єктивно встановлену гранично допустиму величину. Небезпека виникає, коли об'єкт піддається впливу (зсередини або ззовні) так, що його механізми життєзабезпечення не можуть підтримувати нормальний режим функціонування. Це може призвести до часткового або повного знищення об'єкта (деструкції) та/або припинення його основних функцій (дисфункції). Важливо відзначити, що не кожна загроза деструкції і дисфункції вважається небезпекою. Тільки та, яка може призвести до порушення структури об'єкта, при якому він втрачає свою цілісність або перестає виконувати свої основні функції, вважається реальною небезпекою. Отже, безпека виникає тільки при подоланні цієї ситуації.

Безпеку системи слід розуміти як стан, при якому забезпечується її стійке існування в межах встановлених параметрів, зберігається можливість і здатність постановки і досягнення вигідних для об'єкта цілей. При цьому об'єкт може змінюватися в межах допустимого (заходи або норми), ускладнюватися, змінювати структуру, властивості, але він повинен зберігати свої цілі, функції і власну ідентичність (зберігати структурну і функціональну цілісність).

Після визначення поняття "безпека" перейдемо до розгляду сутності та змісту терміну "інформація". Сучасний стан та розвиток інформаційного середовища визначають інформацію як один з ключових ресурсів для функціонування суспільства. Інформація широко застосовується у всіх сферах суспільного життя, оскільки вона відрізняється різноманітністю та різноплановою значимістю.

Згідно з висловленням Субіної Т.В., органи державної влади, включаючи Службу безпеки України, активно використовують інформацію [91, с. 22], що підкреслює її важливість у контексті дослідження.

Управління будь-якою державою базується на ухваленні управлінських рішень, для чого використовується значний обсяг інформації. Збір, обробка та систематизація цієї інформації дозволяють чітко визначити цілі та засоби

досягнення поставленої мети. Таким чином, робота з інформацією передбачає її збір, зберігання та захист від несанкціонованого втручання.

Відповідно до Закону України "Про інформацію", інформацією вважають будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [68]. У Законі України "Про телекомунікації" інформацію визначають як відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб [77].

Закон України "Про захист економічної конкуренції" пропонує інший підхід до змісту інформації, розглядаючи її як відомості в будь-якій формі та вигляді, збережені на будь-яких носіях (в тому числі книги, ілюстрації, звукові записи, фотографії, бази данних компютерних систем) та пояснення осіб, а також будь-які інші публічно оголошені чи документовані відомості [64].

Отже, правове визначення сутності інформації значно залежить від сфери її застосування, що призводить до різного роду трактувань. Сучасна управлінська діяльність об'єктів стає неможливою без використання інформації, яка, за словами В.Г. Афанасьєва, є основою для прямого й зворотного зв'язку в системі управління [7, с. 19]. Таким чином, інформація служить основою функціонування органів публічного управління, виступаючи предметом комунікаційного процесу всередині державних інституцій.

Сутність інформаційної безпеки, більшістю фахівців, асоціюється зі здатністю захистити об'єкт від шкідливого впливу, зберігаючи його властивості та ефективність [89, с. 54].

Оскільки інформація та інформаційні технології грають ключову роль у діяльності державних органів, терміни "інформаційна безпека", "інформаційний суверенітет" та "захист інформації" активно використовуються. Наприклад, коли йдеться про захист національного інформаційного простору, вказують на державний інформаційний суверенітет,

що передбачає контроль та розповсюдження національних інформаційних ресурсів усією спільнотою в державі [48, с. 103].

А. Бурьяк розглядає національну безпеку як показник стану нації, що вказує на те, що сукупність внутрішніх і зовнішніх негативних факторів не може суттєво погіршити якість життя і не створює загрози існуванню [14].

За визначенням І. Л. Прохоренка, національна безпека – це умови, при яких відсутні критичні загрози для держави, і в той же час зберігається здатність держави адекватно реагувати на такі загрози, якщо вони все-таки виникнуть [78, с. 70].

Ліпкан В.А. дефініцію національної безпеки розуміє як захист життєважливих інтересів людей, громадян, суспільства і держави. Згідно з його визначенням, національна безпека передбачає належний розвиток суспільства, своєчасне виявлення, запобігання та нейтралізацію реальних та потенційних загроз національним інтересам у всіх сферах життєдіяльності держави, що виникають внаслідок певних негативних тенденцій [37, с. 233].

У Законі України «Про національну безпеку», поняття «національна безпека» означає захищеність життєважливих інтересів людей, громадян, суспільства і держави. Це охоплює сталий розвиток суспільства, своєчасне виявлення, запобігання та нейтралізацію реальних та потенційних загроз національним інтересам у різних сферах державної діяльності, включаючи правоохоронну діяльність, боротьбу з корупцією, прикордонну діяльність та оборону, міграційну політику, охорону здоров'я, освіту та науку, науково-технічну та інноваційну політику, культурний розвиток, свободу слова, інформаційну безпеку, соціальну політику, пенсійне забезпечення, житлово-комунальне господарство, ринок фінансових послуг, права власності, фондові ринки, бюджетно-податкову політику та інші аспекти державного управління, які можуть стикатися з потенційними або реальними загрозами національним інтересам [73].

Після ретельного аналізу Закону України «Про національну безпеку України», стає очевидним, що в ньому відсутнє чітке визначення терміну

"інформаційна безпека". Термін розглядається лише як один з аспектів національної безпеки, що визначається конкретними загрозами національним інтересам [97, с. 26].

Згідно з висловленням Попової С.М., інформаційна безпека визнається обов'язковим елементом кожної сфери національної безпеки. Одночасно інформаційна безпека розглядається як самостійна сфера в системі гарантування національної безпеки держави. Забезпечення високого рівня інформаційної безпеки визначає подальший розвиток держави як суверенної, демократичної, правової та економічно стабільної [55, с. 273].

Серед країн Європейського Союзу поширене визначення "інформаційна безпека", яке характеризується як захист інформації від несанкціонованого доступу, захист особистої інформації відправників та одержувачів, створення надійного джерела постачання інформації, інформаційних послуг та необхідного обладнання, а також захист інформації, пов'язаної з усіма аспектами національної безпеки, включаючи військовий потенціал країни [107].

Під час дослідження, особливий інтерес викликає визначення інформаційної безпеки, яке пропонує О.І. Алексенцев: "інформаційна безпека - це стан інформаційного середовища, що забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, безпеку інформації та захист суб'єктів від негативного інформаційного впливу" [3, с. 56]. У цьому контексті, інформаційне середовище, розглядається як область діяльності суб'єктів, яка пов'язана зі створенням, трансформацією і споживанням інформації, виступаючи метою та об'єктом захисту.

Таким чином, згідно з поглядом О.І. Алексенцева, інформаційна безпека включає три ключові компоненти [3, с. 56]:

задоволення інформаційних потреб суб'єктів.

забезпечення безпеки інформації.

захист суб'єктів інформаційних відносин від негативного інформаційного впливу.

Відповідно до Доктрини інформаційної безпеки, структура та зміст поняття "інформаційна безпека", а також основні напрямки та принципи державної політики у сфері інформаційної безпеки представлені на рис. 1.1.

Рисунок 1.1. - Структура і склад інформаційної безпеки

Джерело: [26, с. 20].

Основні напрями державної політики в галузі інформаційної безпеки в Україні включають:

Інформаційно-психологічний напрям: забезпечення конституційних прав і свобод людини і громадянина, формування сприятливого психологічного клімату в національному інформаційному просторі для підтримки загальнолюдських і національних моральних цінностей.

Технологічний напрям: розвиток і інноваційне оновлення національних інформаційних ресурсів, впровадження передових технологій у створенні, обробці та поширенні інформації.

Захист інформації: забезпечення конфіденційності, цілісності і доступності інформації, включаючи технічний захист інформації в національних інформаційних ресурсах від кібернетичних атак.

Отже, інформаційна безпека визначається як стан об'єкта, при якому його інформаційне середовище дозволяє йому зберігати здатність і можливість приймати та реалізовувати рішення відповідно до своїх цілей, спрямованих на прогресивний розвиток.

Отримані дані з літературних джерел та систематизація наукових поглядів стосовно інформаційної безпеки дають підставу вважати, що інформаційна безпека в діяльності органів публічного управління включає в себе заходи захисту інформаційних баз даних, інформаційних систем, посадових осіб та інфраструктури, максимально обмежуючи негативні наслідки використання інформаційних продуктів та технологій і забезпечуючи їхню безпеку від наслідків несанкціонованого доступу та втручання.

1.2. Досвід зарубіжних країн у сфері забезпечення інформаційної безпеки

Швидкий розвиток інформаційних технологій, процеси інформатизації та комп'ютеризації, а також формування глобального інформаційного простору визначили появу зовсім нових реалій - інформаційного суспільства та інформаційних і кібернетичних просторів. Ці нові реалії мають величезний потенціал і відіграють ключову роль у економічному та соціальному розвитку світових країн. Однак створення інформаційного суспільства може призвести до виникнення численних інформаційних загроз. Таким чином, одним із основних завдань у сучасному інформаційному просторі є гарантування інформаційної та кібернетичної безпеки.

Аналіз міжнародного досвіду в галузі інформаційної безпеки вказує на те, що ключовими напрямами вирішення цих проблем у світовому співтоваристві є: захист прав особистості в інформаційній сфері: Захист визначено Загальною декларацією прав людини та Конвенцією Ради Європи з прав людини, які гарантують свободу виявлення переконань та безперешкодний доступ до інформації.

Захист державних інтересів: У світовому співтоваристві приділяється велика увага заходам захисту інтересів країн у контексті інформаційної безпеки.

Захист підприємницької та фінансової діяльності: забезпечення безпеки в сферах бізнесу та фінансів визнається однією з головних складових інформаційної безпеки.

Боротьба з комп'ютерними злочинами: у міжнародному досвіді акцентується увага на необхідності протидії комп'ютерним злочинам та кібертероризму.

Нормативне регулювання прав особистості в інформаційній сфері визначається Загальною декларацією прав людини та Конвенцією Ради Європи з прав людини. Стаття 19 Загальної декларації прав людини (1948 р.) закріплює право на свободу переконань та вільне їх виявлення, включаючи свободу дотримуватися переконань та вільно шукати, одержувати та

поширювати інформацію та ідеї будь-якими способами і незалежно від державних кордонів. Стаття 10 Конвенції "Про захист прав людини і основних свобод" (1950 р.) гарантує "запобігання розголошенню інформації, одержаної конфіденційно". Навіть при тому, що ці міжнародні документи були прийняті до активного використання ІКТ, вони залишаються актуальними і в наш час.

Згідно з повідомленням Генеральної Асамблеї ООН A/55/40, міжнародна інформаційна безпека визначається як "стан міжнародних відносин, який виключає порушення світової стабільності та створення загрози безпеці держав і світової спільноти в інформаційному просторі" [105].

У міжнародно-правовому регулюванні глобальних процесів інформаційної безпеки важливим етапом стало прийняття резолюції Генеральної Асамблеї ООН 54/90 "Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки". У цьому документі висловлено питання щодо доцільності розробки міжнародних принципів, спрямованих на зміцнення безпеки глобальних інформаційних та телекомунікаційних систем і сприяння боротьбі з тероризмом і криміналом. Світове співтовариство визнало міжнародну безпеку як глобальну проблему, яка вимагає негайного вирішення [3, с. 122].

Кіберпростір став невід’ємною частиною інформаційного простору та п'ятою сферою здійснення збройних конфліктів. Завдяки інформаційному чиннику, сама збройна боротьба стала високо керованою. Деякі країни, з метою захисту свого кіберпростору, розробляють проекти регулювання (правил поведінки) у кіберпросторі, або, за визначенням деяких відповідних документів, "сфері міжнародної інформаційної безпеки". У 2013 році свої стратегії кібербезпеки прийняли такі країни, як Нідерланди, Іспанія, Туреччина, Угорщина, Польща, Індія, а в 2016 році - Україна [26].

У напрямку міжнародної інформаційної безпеки прийнято чимало документів, що свідчить про формування міжнародного інформаційного законодавства. Крім міжнародних нормативних актів, багато країн мають власні внутрішні законодавчі акти, що регулюють відносини в даній сфері.

Основним юридичним актом, який регулює інформаційну безпеку у США, є "Закон про інформаційну безпеку". Цей закон передбачає виконання мінімально необхідних заходів для забезпечення безпеки в федеральних комп'ютерних системах, не обмежуючи при цьому всіх можливих заходів. Відповідно до цього закону, визначення стандартів та директив, спрямованих на захист інформації від знищення і несанкціонованого доступу, а також від крадіжок та підробок, здійснює Національний інститут стандартів і технологій.

За останні двадцять років у США були спрощені експортні обмеження на криптозасоби, створена інфраструктура з відкритими ключами, і розроблено численні стандарти, такі як стандарт ЕЦП (FIPS 186-2). Це все сприяло створенню національної інфраструктури електронної аутентифікації.

Програма безпеки інформаційних систем у США включає в себе наступне:

систематичну оцінку ризиків, що враховує як внутрішні, так і зовнішні загрози цілісності, конфіденційності та доступності систем та пов'язаних з ними даних;

визначення правил та процедур, які дозволяють економічно обґрунтовано зменшити ризики до прийнятного рівня, ґрунтуючись на проведеному аналізі ризиків;

навчання персоналу для інформування їх про існуючі ризики та обов'язки, пов'язані з їхньою нейтралізацією;

регулярну перевірку та переоцінку ефективності правил та процедур;

прийняття заходів при внесенні суттєвих змін в систему;

виконання процедур виявлення порушень інформаційної безпеки та реагування на них, з метою зменшення ризиків, уникнення серйозних втрат та співпраці з правоохоронними органами.

Крім того, в законодавстві США міститься достатня кількість положень, спрямованих на обмеження, а також директиви, які захищають інтереси відомих агентств, таких як Міністерство оборони, ФБР та ЦРУ [2, с. 54].

У сучасному світі Китай визначається як одна з країн Азіатсько-Тихоокеанського регіону, що найбільш активно розвивається, та є лідером в області інформаційної протидії та забезпечення сучасного захисту національних інформаційних ресурсів.

Законодавство у сфері ІКТ в Китаї розпочало свій розвиток паралельно з розбудовою сучасних інформаційних систем.

У 1994 році Державною радою країни були опубліковані положення "Про захист комп'ютерних та інформаційних систем". Законотворчий процес у галузі регулювання Інтернету розпочався в 1995 році, коли було прийнято ряд заходів, спрямованих на запобігання незаконній онлайн-діяльності в Інтернеті. У положенні "Про захист безпеки міжнародної мережі комп'ютерних та інформаційних систем", опублікованому Міністерством державної безпеки КНР, описані категорії інформації, розробка, збільшення, пошук і поширення якої заборонені, а також відповідні види діяльності, що становлять загрозу безпеці комп'ютерних та інформаційних систем. Прийняте в 2001 році положення "Про захист комп'ютерних програм" стало першим нормативним актом у галузі охорони безпеки комп'ютерних систем Китаю. У 2003 році був прийнятий Закон "Про авторські права", в якому комп'ютерні програмні продукти вперше були прирівняні до категорії об'єктів авторських прав.

Постанова "Про захист комп'ютерних мереж", що була прийнята в Китаї у 2004 році, встановлює кримінальну відповідальність за такі види порушень:

1. Мережева атака і пошкодження комп'ютерної системи, включаючи хакерські атаки з метою перехоплення, знищення, зміни і підробки інформації, яка зберігається в комп'ютері, а також порушення нормального функціонування комп'ютерної системи та мереж; розробка та поширення комп'ютерних вірусів; розкрадання інформації, що зберігається в комп'ютері.

2. Мережеве шахрайство.

3. Розкрадання грошових коштів з фінансових установ шляхом несанкціонованого доступу до комп'ютерних систем.

4. Азартні ігри в он-лайн середовищі та реклама послуг сексуального характеру в Інтернеті.

5. Посягання на авторські та суміжні права, а також злочини проти інтелектуальної власності.

6. Розкрадання інформації, яка є державною таємницею, та проникнення в інформаційні системи державних служб.

7. Розповсюдження порнографічної продукції, інформаційних продуктів, що викликають прояви расизму і розпалюють міжнаціональну ворожнечу, а також іншої інформації, що загрожує державній безпеці.

8. Посягання на приватне життя громадянина, включаючи:

- фальсифікація та поширення інформації, що порушує гідність та репутацію громадянина;

- наклеп, дезінформація та розповсюдження інформації від імені іншої особи;

- розголошення особистого життя людини без її дозволу.

Для підвищення контролю над Інтернетом та визначення виконавчого апарату в Китаї вживається значна кількість заходів. Орган громадської безпеки (міліція) в країні відповідає за забезпечення інформаційної безпеки. Закон Китаю "Про міліцію" та інші відповідні закони та нормативні акти визначають обов'язки міліції у сфері контролю за інформаційною безпекою в Інтернеті:

визначення рівнів безпеки інформаційних систем та розробка засобів їх захисту;

повідомлення цих відомостей користувачам Інтернету;

розслідування справ, пов'язаних з несанкціонованим використанням комп'ютерної інформації;

розробка систем для запобігання поширенню комп'ютерних вірусів та іншої небезпечної інформації;

визначення реальних методів державного регулювання продажу мережевих продуктів та інформаційних систем;

контроль за діяльністю по забезпеченню інформаційної безпеки в Інтернеті;

виявлення порушень в Інтернеті.

На сьогоднішній день виконавчий апарат безпеки мережі Інтернет в Китаї успішно здійснює контроль за інформаційним обміном та припиняє незаконну діяльність в китайському сегменті мережі Інтернет.

Стратегія кібербезпеки Канади визначає кібертероризм та ворожі дії в кіберпросторі (кібершпигунство та кібервійна) як основні загрози кібербезпеці держави. Координацію та контроль за реалізацією стратегії, реалізацію державної політики та координацію заходів у сфері кібербезпеки та протидії кіберзагрозам виконує Міністерство громадської безпеки Канади.

Відповідно до Закону ФРН "Про посилення безпеки інформаційних систем", відповідальність за попередження, реагування на кіберзагрози, управління та координацію захисту критичної інформаційної інфраструктури, зокрема у взаємодії з приватним сектором, покладено на Федеральне відомство безпеки інформаційних систем (BSI) ФРН.

У Великій Британії головним органом, відповідальним за захист критичної інфраструктури та мінімізацію загроз, зокрема терористичних, є Центр захисту національної інфраструктури (Centre for the Protection of National Infrastructure, CPNI). Крім того, Центр із протидії кібернетичним загрозам, створений наприкінці березня 2013 року, спрямований на запобігання та нейтралізацію кібератак на об'єкти критичної інфраструктури, а також швидке реагування на правопорушення у цій сфері.

В Австрії Центр боротьби з кіберзлочинністю Федерального міністерства внутрішніх справ визначений як національний координатор і центральний орган з кібербезпеки, виконуючи головні функції у сфері правоохоронної діяльності та боротьби з кіберзлочинністю.

Ключову роль у забезпеченні кібербезпеки Польщі відіграє Агентство внутрішньої безпеки (АВБ) – контррозвідувальний орган, який у 2013 році розробив Стратегію кібербезпеки Польщі та створив Центр криптології при

Міністерстві національної оборони Польщі, відповідальний за захист інформації та проведення кібероперацій.

У Румунії ключова роль у забезпеченні кібербезпеки відводиться Румунській службі інформації (РСІ), яка виконує спеціальні контррозвідувальні функції.

Аналізуючи системи кібербезпеки в провідних країнах світу, ми приходимо до висновку, що на сьогоднішній день не існує загальноприйнятої моделі для побудови національних систем кібербезпеки. Наприклад, в рамках комплексного нормативно-правового акта у сфері безпеки, який був прийнятий 25 листопада 2002 року в США, а саме закону «Про внутрішню безпеку» (Homeland Security Act of 2002), урядові структури, що відповідали за забезпечення комп'ютерної безпеки, були піддані контролю цього новоствореного відомства.

Цей закон також узяв на себе посилення відповідальності за комп'ютерні злочини, включаючи можливість накладання довічного ув'язнення, і зобов'язав інтернет-провайдерів надавати інформацію про клієнтів за вимогою правоохоронних органів. Він розширив їхні права щодо можливості перехоплення інформації, такої як прослуховування телефонних розмов та перегляд електронних повідомлень, без судового дозволу. Також були визначені основні напрями діяльності федеральних органів для підвищення ефективності захисту критичної інфраструктури США від кібератак, зокрема, об'єктів стратегічного значення, що перебувають у приватній власності.

У 1990-х роках, в контексті розвитку інформаційного суспільства в Європейському Союзі, виникали питання про ризики та загрози в області інформаційної безпеки. Для вирішення цих проблем було прийнято комплекс нормативно-правових актів в рамках системи правового регулювання телекомунікацій та захисту інформації.

Так, у 2001 році Європейською комісією було опубліковано повідомлення під назвою "Мережева та інформаційна безпека: пропозиції для підходу європейській політиці" [101]. У цьому документі проводився аналіз

ситуації та основних тенденцій у сфері забезпечення інформаційної безпеки, а також пропонувалися рішення для забезпечення цієї безпеки в Європейському союзі. Було введено поняття "мережева та інформаційна безпека", що характеризується як "здатність мережі або інформаційної системи надійно протистояти на заданому рівні випадковим загрозам або умисним шкідливим діям, які можуть наражати на ризик доступність, автентичність, цілісність і конфіденційність збережених або переданих служб, до яких здійснюється доступ за допомогою таких мереж або систем".

Запропонований Комісією підхід для європейської політики забезпечення мережевої та інформаційної безпеки базується на наступних складових:

- забезпечення прикладного характеру правових норм на основі загального розуміння основних питань безпеки та застосування спеціальних заходів для її забезпечення;
- постійне вдосконалення правового регулювання з урахуванням технічного прогресу та нових загроз;
- необхідність доповнення ринкових механізмів політичними заходами;
- створення європейського внутрішнього ринку інформаційно-комунікаційних послуг.

Взаємозв'язок основних сфер політики ЄС в інформаційній сфері включає дії у галузі мережевої та інформаційної безпеки, боротьби з кіберзлочинністю, захисту інформації та діяльності у сфері телекомунікацій. Усі ці сфери політики перетинаються, маючи як загальні питання, так і свої власні аспекти відносно кожної з них, і застосовують триступеневий підхід, який охоплює:

1. спеціальні заходи для забезпечення системи інформаційної безпеки.
2. правове регулювання електронних комунікацій, включаючи питання захисту інформації та приватного життя.
3. боротьбу з кіберзлочинністю.

В межах першого напряму були ухвалені Рішення від 28 січня 2002 р. (2002/C43/02) "Про загальні підходи і спеціальні заходи в сфері мережевої та інформаційної безпеки" і Рішення від 18 лютого 2003 р. (2003/C48/01) "Про європейський підхід щодо культури мережевої та інформаційної безпеки".

У рамках другого напряму, в 2002 році була прийнята Директива 2002/58/ЕС "Про приватне життя та електронні комунікації", яка визначила гарантії захисту особистих даних і приватного життя в електронних комунікаціях. Право на захист особистих даних також включено до Хартії Європейського Союзу про основні права з 2007 року [93].

Для розвитку європейської політики в галузі системи інформаційної безпеки у 2006 році була прийнята "Стратегія безпеки інформаційного суспільства: діалог, партнерство і розширення можливостей". В цьому документі проводиться огляд сучасних загроз безпеці інформаційного суспільства та визначаються додаткові заходи для забезпечення інформаційної безпеки. Зазначається, що незважаючи на активність на міжнародному, європейському та національному рівнях, виникають нові виклики безпеці, зокрема атаки на інформаційні системи та поширення шкідливого програмного забезпечення. Комісія акцентує увагу на зростанні використання мобільних пристроїв і мережевих мобільних послуг, яке може зробити їх головною мішенню комп'ютерних атак. Будь-які нові платформи для комунікації та інформаційних систем створюють нові можливості для шкідливих атак.

Однією з фундаментальних цілей ЄС є надання його громадянам простору свободи, безпеки та законності без внутрішніх кордонів. Для досягнення цієї мети в рамках політики ЄС в галузі інформаційної безпеки здійснюється діяльність інститутів ЄС і держав-учасників ЄС у боротьбі зі злочинністю, включаючи кіберзлочинність, яка охоплює нові види злочинів, характерних для Інтернет-середовища.

Крім того, традиційні злочини, такі як шахрайство та поширення нелегального контенту в Інтернеті (зокрема матеріали сексуального

насильства над дітьми або пропаганда насильства), все частіше вчиняються за допомогою комп'ютерів.

У зв'язку із зростанням кіберзлочинності, Європейська Комісія розробила політику по її боротьбі, яка була викладена в Повідомленні 2007 року "На шляху до спільної політики в боротьбі з кіберзлочинністю". Основна мета цього повідомлення полягає в розвитку співробітництва між правоохоронними органами, державно-приватним партнерством та міжнародним співробітництвом. У ньому пропонується реалізація комплексу заходів для протидії кіберзлочинності, включаючи запуск оперативного співробітництва між національними правоохоронними органами, збільшення фінансової підтримки ініціатив з підготовки національних правоохоронних органів до розслідування кіберзлочинів, підтримку досліджень у сфері боротьби з кіберзлочинністю, підвищення обізнаності про небезпеки кіберзлочинності в приватному секторі та реалізація заходів щодо запобігання та протидії масштабним атакам на інформаційну інфраструктуру.

В останні роки в ЄС також реалізовано кілька інноваційних проектів у сфері протидії кіберзлочинності, зокрема у червні 2010 року було прийнято рішення про створення Спеціальної групи з кіберзлочинності в ЄС (European Union Cybercrime Task Force), в яку увійшли представники Європолу, Євроюсту та Європейської Комісії, з метою сприяння транскордонній боротьбі з кіберзлочинністю.

Під патронатом Європолу було запущено виконання дослідницького проекту, визначеного як аналіз організованої злочинності, що використовує можливості Інтернету (Strategic analysis of Internet Facilitated Organised Crime, або iOCTA). Його мета полягає в оцінці поточних та майбутніх тенденцій розвитку кіберзлочинності та наданні інформації для операційної діяльності та формування політики ЄС у цій області. Аналіз iOCTA ґрунтується на обробці операційної інформації від правоохоронних органів ЄС та відкритих джерел. Забезпечення кібербезпеки в інформаційному просторі визначено як один із пріоритетів до 2020 року в ключових стратегічних документах ЄС.

Отже, аналіз вищезазначеного дає підставу зробити висновок, що система інформаційної безпеки ЄС дозволяє ефективно реагувати на основні загрози. Система публічного управління України, яка взаємодіє з глобальним кіберпростором, стикається з різноманітними загрозами та негативними впливами, пов'язаними з її функціонуванням, і це актуалізує проблеми кібербезпеки на національному рівні. Вирішення завдань щодо підвищення ефективності інформаційної безпеки та кібербезпеки в системі публічного управління вимагає вивчення нових реалій кібербезпеки, оновлення внутрішнього нормативно-правового середовища, чіткого визначення повноважень відомств і організацій, що залучені до забезпечення цих видів безпеки, і комплексного вирішення проблем, пов'язаних із їх інтеграцією в діяльність конкретних органів публічного управління.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ СУЧАСНОГО СТАНУ ЗАБЕЗПЕЧЕНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

2.1. Інституційне забезпечення захисту інформації в Україні

Державне управління та захист інформації представляють собою важливу складову державної інформаційної політики та інформаційної безпеки України. Ми вважаємо, що під системою управління та захисту інформації слід розглядати організовану структуру, яка включає органи публічного управління, їх спеціальні підрозділи, служби, посадових осіб, підприємства, установи, інші суб'єкти господарювання, громадські організації та окремих громадян, що об'єднані спільною метою та завданнями щодо формування, зберігання, поширення інформації, задоволення інформаційних потреб особистості, суспільства й держави, а також впровадження спеціальних заходів і засобів захисту інформаційних ресурсів та прав суб'єктів інформаційної діяльності в рамках чинного законодавства України.

Зараз чинне інформаційне законодавство не надає повного юридичного визначення поняття "національні інформаційні ресурси". Без вивчення та юридичного обґрунтування цього поняття стосовно інформаційних ресурсів утруднено формування системи національних інформаційних ресурсів та державного управління цією системою. Зокрема, у Законі України "Про національну програму інформатизації" термін "інформаційний ресурс" визначено як "сукупність документів в інформаційних системах (бібліотеках, архівах, банках даних тощо)".

Важливими характеристиками інформаційного ресурсу є його системотворний та керівний фактор, які позитивно впливають на соціально-економічний розвиток суспільства і держави, а також сприяють національній безпеці. Крім того, інформаційний ресурс може завдавати шкоди суспільному

життю при дефіциті, низькій якості чи негативній інформаційній експансії, бути об'єктом кримінальних зазіхань і вимагати спеціальних засобів захисту.

Отже, узагальнення ключових характеристик інформаційних ресурсів та об'єктивних законів, що діють у сфері інформації, служить підґрунтям для висновку, що формування, розвиток і ефективне використання національних інформаційних ресурсів, в умовах постіндустріального суспільства та ринкової економіки, повинні базуватися на споживчій вартості у всіх сферах діяльності особистості, суспільства і держави, а саме: політичній, економічній, науковій, освітній, соціокультурній, оборонній, ринковій інформації та інших.

Національні інформаційні ресурси виникають як результат інтелектуальної діяльності у всіх сферах життєдіяльності людини, суспільства і держави, і вони фіксуються на відповідних матеріальних носіях інформації, таких як документи, бази даних, архіви, бібліотеки тощо. Ці ресурси представляють собою об'єкти права власності суб'єкта України і мають споживчу цінність в різних сферах, таких як політичній, економічній, науковій, освітній, соціокультурній, оборонній, ринковій, історичній, інформаційній тощо.

Згідно з Законом України "Про інформацію", основні галузі інформації включають політичну, економічну, духовну, науково-технічну, соціальну, екологічну, міжнародну (ст. 17), а види інформації поділяються на статистичну, масову, діяльність державних та місцевих органів, правову, особисту, довідково-енциклопедичну, соціологічну (ст. 18). Визначення видів інформаційних ресурсів призначене для формування системи державного управління національними інформаційними ресурсами, хоча перелік не є вичерпним і не враховує всі різновиди інформаційних ресурсів та систем управління ними.

Крім того, визначені види інформації не розкривають суті галузей інформації. Наприклад, в Законі України "Про інформацію" визначена галузь "економічна" (ст. 17), проте зміст цієї галузі у вигляді видів інформації, які її складають, не визначено, що ускладнює формування системи національних

інформаційних ресурсів. За думкою авторів, доцільно було б включити до галузі економічної інформації види інформаційних ресурсів, що стосуються сфери матеріального виробництва, фінансів, зовнішньоекономічної діяльності, природних ресурсів і т. д.

На державному рівні в Україні було кілька спроб оптимізації регулювання інформаційної сфери. Засідання Ради національної безпеки і оборони України 17 червня 1997 р., 21 березня 2008 р., 17 листопада 2010 р. були присвячені цьому питанню. Наприклад, у рішенні РНБО України від 21 березня 2008 р. Кабінету Міністрів України було доручено "здійснити заходи щодо вдосконалення державного управління в інформаційній сфері, чіткого визначення повноважень та організації ефективної взаємодії органів державної влади із забезпечення національної безпеки в інформаційній сфері" [80]. Однак ці рішення не призвели до значних змін у системі державного управління інформаційною сферою.

Адміністративна реформа, впроваджена відповідно до Указу Президента України "Про оптимізацію системи центральних органів виконавчої влади" від 9 грудня 2010 р. № 1085/2010, мало вплинула на структуру державного управління в інформаційній сфері. Однак слід відзначити, що відповідні органи державної влади України, зокрема Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (далі – НКРЗІ) та Державне агентство з питань науки, інновацій та інформатизації України (далі – Держінформнауки України), вказують на розпорошеність, дублювання функцій та повноважень, низький рівень загальнодержавної координації та міжвідомчої взаємодії в цьому напрямі. Вони також пропонують провести реорганізацію системи органів державної влади в інформаційній сфері, посиливши координуючу роль з єдиного центру [105].

На сьогоднішній день в Україні управління інформаційною сферою здійснюється п'ятьма основними органами державної влади (рис. 2.1): два регуляторних органи – Національна рада України з питань телебачення і

радіомовлення (далі – Національна рада) та НКРЗІ, а також три органи виконавчої влади – Державний комітет з телебачення та радіомовлення України (далі – Держкомтелерадіо України), Державне агентство з питань електронного урядування України та Державна служба спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку України).

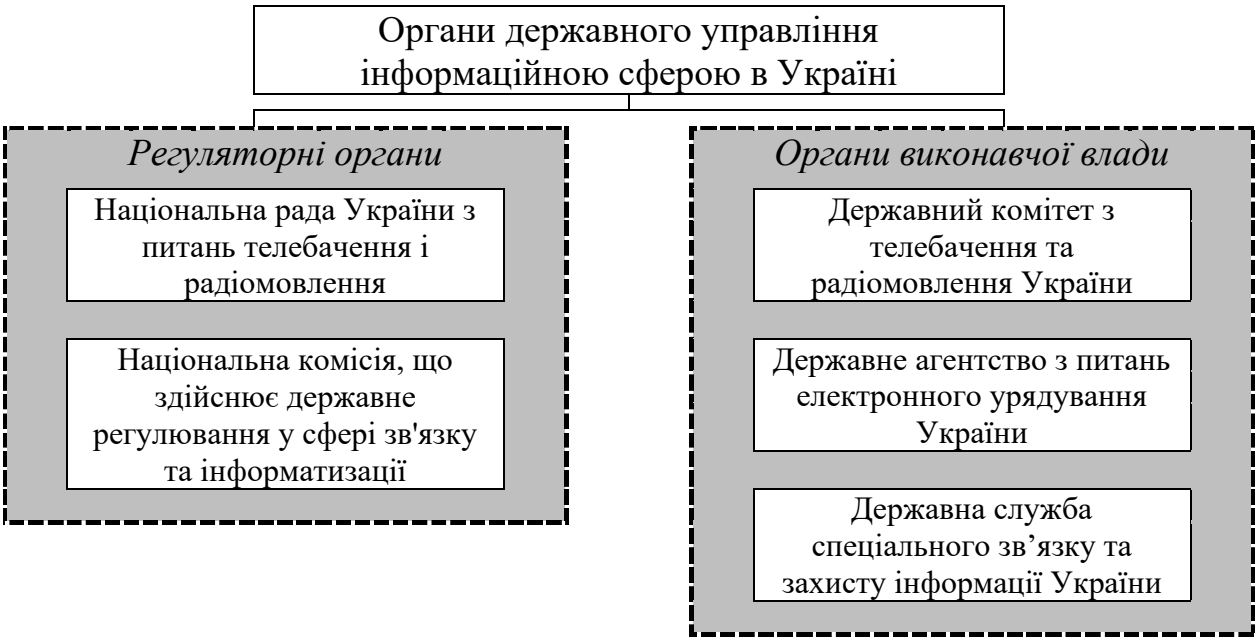

Рисунок 2.1 - Система органів публічного управління у сфері інформаційної безпеки України

Примітка. Складено автором

Крім того, виконання завдань та програм в інформаційній сфері залучає понад 20 допоміжних органів державної влади України, таких як Служба безпеки України, Генеральне управління розвідки Міністерства оборони України, Служба зовнішньої розвідки України, Міністерство зовнішніх справ України, Міністерство юстиції України, а також Комітет Верховної Ради України з питань свободи слова та інформатизації, Комітет Верховної Ради України з питань інформатизації та інформаційних технологій і інші.

Національна рада володіє наглядовими та регуляторними повноваженнями, що стосуються виконання телерадіоорганізаціями та провайдерами програмної послуги вимог законодавства у сфері телерадіомовлення, ліцензійних умов та умов ліцензій, стандартів та норм

технічної якості телерадіопрограм, а також дотримання вимог законодавства України щодо частки вітчизняного продукту у їх програмах та інших аспектів.

Національна рада виконує такі функції:

– здійснює нагляд за тим, як телерадіоорганізації та провайдери програмної послуги дотримуються вимог законодавства у галузі телерадіомовлення.

– контролює виконання ліцензіатами вимог щодо реклами та спонсорства в сфері телерадіомовлення.

– слідкує за тим, як ліцензіати дотримуються ліцензійних умов та умов ліцензій.

– наглядає за дотриманням ліцензіатами визначеного законодавством порядку мовлення під час проведення виборчих кампаній та референдумів.

– виконує контроль за дотриманням телерадіоорганізаціями стандартів та норм технічної якості телерадіопрограм.

– забезпечує виконання телерадіоорганізаціями законодавства України у сфері кінематографії.

– спостерігає за дотриманням телерадіоорганізаціями вимог законодавства України щодо частки національного аудіовізуального продукту.

– контролює виконання телерадіоорганізаціями, які здійснюють радіомовлення, вимог щодо часток пісень (словесно-музичних творів) державною мовою та офіційними мовами Європейського Союзу в обсязі пісень, поширених протягом доби та часових проміжків, визначених законом.

– відслідковує дотриманням телерадіоорганізаціями, які здійснюють радіомовлення, вимог законодавства України щодо обсягу ведення передач державною мовою.

– здійснює контроль за дотриманням телерадіоорганізаціями законодавства у сфері захисту суспільної моралі.

– контролює дотримання телерадіоорганізаціями вимог законодавства щодо складу їх засновників (власників) та частки іноземних інвестицій у їх статутному капіталі.

– застосовує санкції відповідно до закону в межах своїх повноважень.

– проводить офіційний моніторинг телерадіопрограм.

– забезпечує контроль та нагляд за дотриманням телерадіоорганізаціями та провайдерами програмної послуги вимог щодо розкриття інформації про кінцевих бенефіціарних власників (контролерів), а в їх відсутності - про всіх власників та учасників телерадіоорганізації або провайдера програмної послуги і всіх фізичних осіб та власників і учасників юридичних осіб на всіх рівнях ланцюга володіння корпоративними правами телерадіоорганізації або провайдера програмної послуги, а також про пов’язаних осіб та структуру власності телерадіоорганізації або провайдера програмної послуги.

Нагляд та контроль реалізуються Національною радою через подання запитів для отримання інформації від органів державної та місцевої влади, фізичних і юридичних осіб, запитів на видачу інформації з державних реєстрів, а також запитів до компетентних органів іноземних держав у відповідності до міжнародних нормативно-правових актів, які були ратифіковані Верховною Радою України. У сфері телерадіомовлення Національна рада виконує регуляторні функції відповідно до чинного законодавства України.

До сфери компетенції Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗІ), входить державне регулювання та нагляд у галузі телекомунікацій, інформатизації, використання радіочастотного ресурсу, а також надання поштових послуг [59].

Основними завданнями Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗІ), є:

– забезпечення реалізації єдиної державної політики у сфері телекомунікацій, інформатизації, розвитку інформаційного суспільства, користування радіочастотним ресурсом та послуг поштового зв'язку.

– здійснення державного регулювання та нагляду у галузі телекомунікацій, інформатизації, користування радіочастотним ресурсом та послуг поштового зв'язку з метою задоволення попиту споживачів на зв'язок та інформаційні послуги, створення сприятливих умов для залучення інвестицій, збільшення обсягів послуг та підвищення їх якості, а також розвитку та модернізації мереж з урахуванням національних інтересів у сфері безпеки.

– забезпечення ефективного використання радіочастотного ресурсу та функціонування ринку послуг у сферах телекомунікацій, інформаційно-телекомунікаційних та поштового зв'язку на основі балансування інтересів суспільства, суб'єктів господарювання та споживачів.

– підтримка розвитку конкуренції та підприємництва, створення рівних умов для суб'єктів господарювання різних форм власності, вдосконалення механізму регулювання ринкових відносин у галузях телекомунікацій, інформатизації, користування радіочастотним ресурсом та послуг поштового зв'язку.

– забезпечення системності, комплексності та узгодженості розвитку інформатизації та інформаційного суспільства в Україні.

На перший погляд, області компетенції та повноважень Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗІ) та Національної ради, виглядають досить визначено. Проте це ствердження може бути точним лише при умові наявності відокремлених інфраструктур для різних видів зв'язку, таких як телерадіомовлення, поштовий зв'язок, Інтернет тощо. Але на сучасному етапі розвитку цифрових інформаційних та мережевих технологій спостерігається подальша інтеграція інфраструктур різного призначення в універсальні інформаційно-комунікаційні мережі. Ці мережі можуть одночасно передавати голосові, текстові та відеодані, а також використовуватися як для послуг телефонного та факсимільного зв'язку, так і для телерадіопередач.

Це призводить до того, що національне регулювання в інформаційному просторі нині є недостатньо роздільним, зокрема щодо діяльності Інтернет-ЗМІ, мобільного телебачення тощо. В результаті виникає необхідність вирішення питання щодо створення єдиного конвергентного органу регулювання в інформаційній сфері в Україні, який може мати робочу назву "Національна рада України з питань комунікацій".

Щодо обов'язків в інформаційній сфері органів виконавчої влади в нашій країні, Держкомтелерадіо України включає в свою компетенцію такі завдання, як розробка заходів для запобігання внутрішньому і зовнішньому інформаційному впливу, який становить загрозу для інформаційної безпеки держави, суспільства і особи; участь у формуванні єдиного інформаційного простору та сприяння розвитку інформаційного суспільства; виконання завдань, спрямованих на забезпечення інформаційної безпеки спільно з іншими державними органами; розробка пропозицій для удосконалення системи державного управління у сфері телебачення і радіомовлення, інформаційних та видавничих сферах, поліграфії; визначення порядку функціонування веб-сайтів органів виконавчої влади та надання пропозицій щодо інформаційного наповнення Єдиного веб-порталу органів виконавчої влади і інше [78].

Щодо завдань Державного агентства з питань електронного урядування України, серед інших, вони включають в себе реалізацію державної політики в сфері інформатизації, електронного урядування, формування та використання національних електронних інформаційних ресурсів, розвиток інформаційного суспільства; а також вносити пропозиції на розгляд Кабінету Міністрів України щодо забезпечення формування державної політики у цій області.

Агентство відповідно до своїх обов'язків:

1. систематизує практику застосування законодавства у сферах, що належать до його компетенції, розробляє пропозиції з удосконалення законодавчих актів, актів Президента України та Кабінету Міністрів України

і, в установленому порядку, представляє їх на розгляд Кабінету Міністрів України;

2. організовує проведення прогнозово-аналітичних досліджень щодо розвитку інформаційного суспільства, електронного урядування та сфери інформатизації;

3. виконує обов'язки генерального державного замовника Національної програми інформатизації, включаючи:

здійснення моніторингу в галузі інформатизації;

погодження галузевих та регіональних програм та проектів інформатизації, а також програм та проектів інформатизації органів публічного управління, з координацією та поданням Кабінету Міністрів України пропозицій щодо зупинення виконання таких програм та проектів;

забезпечення методологічної, нормативно-правової, інформаційної та організаційної підтримки процесів формування і виконання Національної програми інформатизації;

щорічне звітування перед Кабінетом Міністрів України щодо стану інформатизації в Україні;

подання Кабінету Міністрів України завдань Національної програми інформатизації на наступні три роки і проекту програми завдань (робіт) на наступний бюджетний рік;

внесення пропозицій Кабінету Міністрів України щодо внесення змін до Національної програми інформатизації;

4. виконує інші повноваження, передбачені законодавством [66].

Державне агентство зв'язку України відповідає за забезпечення функціонування та розвитку системи урядового зв'язку, Національної системи конфіденційного зв'язку, а також захисту державних інформаційних ресурсів у різних системах. В цьому контексті, його функції, обов'язки та структуру ретельно розглянемо у наступних розділах.

Аналіз існуючого регулювання в інформаційній сфері дозволяє визначити розпорошеність повноважень державних органів та виявити певні

невідповідності в цьому напрямі. Наприклад, ми можемо зазначити про перетин повноважень між Держкомтелерадіо України та Національною радою у справах телерадіомовлення. Виникають питання щодо легітимності положення, визначеного в п. 24 ст. 4 Положенні про Держкомтелерадіо України, яке координує діяльність різних організацій, що належать до його сфери управління, що може суперечити закону про телебачення і радіомовлення.

Отже, зазначена норма у Положенні суперечить чинному законодавству. Інша невідповідність стосується широкого кола повноважень Держкомтелерадіо України, які виходять за межі сфери телебачення та радіомовлення. Це суперечить рішенню Конституційного Суду, яке визначає, що назва органів влади повинна відповідати їх цільовому призначенню. Отже, вимагається зміна назви та переведення його у статус Міністерства з комунікацій, інформації та інформатизації України (робоча назва).

На сьогоднішній день, одним з ключових завдань управління інформаційною сферою є оптимізація системи державних органів з метою підвищення ефективності загальнодержавної координації, відповідно до останніх тенденцій у розвитку інформаційно-телекомунікаційної сфери.

2.2.Практика реалізації функцій Державної служби спеціального зв’язку та захисту інформації у сфері забезпечення інформаційної безпеки

Державна служба спеціального зв'язку та захисту інформації України, що має спеціальний статус та діє під керівництвом Кабінету Міністрів України, відповідає за формування та реалізацію державної політики в областях організації спеціального зв'язку, захисту інформації, телекомунікацій та користування радіочастотним ресурсом в Україні (далі - Держспецзв'язок). Це є центральним органом виконавчої влади у сфері зв'язку, за винятком повноважень, пов'язаних із наданням послуг поштового зв'язку загального

користування, і також є спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

Основні завдання Державної служби спеціального зв'язку та захисту інформації України включають:

1. забезпечення формування та реалізації державної політики в галузях криптографічного і технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, спеціального поштового зв'язку, урядового фельд'єгерського зв'язку, захисту державних інформаційних ресурсів та інформації в інформаційно-телекомунікаційних системах та на об'єктах інформаційної діяльності, а також в галузі використання державних інформаційних ресурсів у частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв'язку та Національної системи конфіденційного зв'язку;

2. Участь у формуванні та реалізації державної політики у сфері електронного документообігу, включаючи захист інформації державних органів та органів публічного управління, а також у розробленні та впровадженні електронного цифрового підпису. Також бере участь у формуванні та реалізації державної тарифної політики у сферах телекомунікацій та користування радіочастотним ресурсом України.

Державна служба спеціального зв'язку та захисту інформації України, відповідно до своїх завдань:

1. Здійснює державне регулювання у сферах поштового зв'язку спеціального призначення та урядового фельд'єгерського зв'язку.

2. Забезпечує нормативно-правове регулювання у галузях криптографічного і технічного захисту інформації, організації спеціального зв'язку, урядового фельд'єгерського зв'язку, захисту державних інформаційних ресурсів та інформації, щодо захисту якої встановлені законом в інформаційно-телекомунікаційних системах і на об'єктах інформаційної

діяльності, протидії технічним розвідкам, телекомунікаціям та користуванням радіочастотним ресурсом України.

3. Здійснює технічне регулювання у сферах криптографічного і технічного захисту інформації, протидії технічним розвідкам, захисту державних інформаційних ресурсів та інформації, щодо захисту якої встановлені законом в інформаційно-телекомунікаційних системах і на об'єктах інформаційної діяльності. Організовує, координує та проводить роботи з підтвердження відповідності, розроблення стандартів, технічних регламентів і технічних умов.

4. Здійснює методичне керівництво та координацію діяльності державних органів, органів публічного управління, військових формувань, підприємств, установ і організацій у сферах криптографічного і технічного захисту інформації, протидії технічним розвідкам, запобігання порушенням безпеки інформації в інформаційно-телекомунікаційних системах та виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів та інформації, щодо захисту якої встановлені законом, в інформаційно-телекомунікаційних системах.

5. Організовує забезпечення урядовим фельд'єгерським зв'язком Президента України, Голови Верховної Ради України, Прем'єр-міністра України, державних органів, органів публічного управління, органів військового управління та інших юридичних осіб відповідно до законодавства.

6. Організовує забезпечення урядовим зв'язком Президента України, Голови Верховної Ради України, Прем'єр-міністра України, інших посадових осіб державних органів, органів публічного управління, органів військового управління, керівників підприємств, установ і організацій у мирний час, в умовах надзвичайного стану і в особливий період.

7. Здійснює інші повноваження,

Державна служба спеціального зв’язку та захисту інформації України в межах власних повноважень, які передбачені законодавством, виконує заходи для запобігання корупції та контролює їх впровадження в Адміністрації

Держспецзв’язку, її територіальних органах, територіальних підрозділах, а також в закладах, установах і організаціях, що входять до структури Держспецзв’язку, на підприємствах і в установах, які підпорядковані йому. Уповноважені посадові особи Держспецзв’язку мають право складати протоколи про адміністративні правопорушення. Уповноважені представники Адміністрації Держспецзв’язку та її територіальних органів мають право:

- мати доступ на об’єкти державних органів, органів публічного управління, військових формувань, підприємств, установ і організацій незалежно від форми власності, де розміщені засоби спеціального зв’язку Держспецзв’язку, а також на об’єкти, щодо яких здійснюється державний контроль за станом криптографічного і технічного захисту інформації, яка є у володінні держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, та протидії технічним розвідкам;

- ознайомлюватися з необхідними документами для проведення перевірок стану криптографічного і технічного захисту інформації, яка є у володінні держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, протидії технічним розвідкам, додержання умов проведення робіт з технічного захисту інформації для власних потреб, ліцензійних умов провадження господарської діяльності з надання послуг у галузі криптографічного та технічного захисту інформації, і вимог законодавства щодо надання послуг електронного цифрового підпису;

- мати доступ до інформаційно-телекомунікаційних систем та отримувати інформацію, необхідну для визначення стану захищеності інформаційно-телекомунікаційних систем, оцінки повноти та достатності вжитих заходів із захисту інформації.

Державна служба спеціального зв’язку та захисту інформації України виконує свої функції як безпосередньо, так і через територіальні органи, утворені відповідно до встановленого порядку. В рамках своєї діяльності служба здійснює комплекс заходів, спрямованих на виявлення загроз інформаційній безпеці, які можна класифікувати у три основні групи:

1. розкриття інформаційних ресурсів: це стан, коли дані та інформація стають доступними несанкціонованим особам. У контексті дослідження системи органів виконавчої влади загроза розкриття виникає при несанкціонованому доступі до інформаційних ресурсів, які належать Секретаріату Кабінету Міністрів України, центральним та місцевим органам виконавчої влади, як відкритих, так і тих, які мають обмежений доступ.

2. порушення цілісності інформаційних ресурсів: це взаємовплив на дані (модифікація, видалення тощо) в інформаційній системі органів виконавчої влади та під час їх передачі до інших систем. Система органів виконавчої влади має три рівні, і взаємодія між ними не завжди забезпечується належним чином, зокрема, щодо взаємодії місцевих державних адміністрацій, Секретаріату Кабінету Міністрів України та центральних органів влади.

3. Збій у роботі обладнання: ця загроза може виникнути при блокуванні доступу до одного чи декількох ресурсів інформаційної системи. Блокування може бути постійним або тимчасовим, призводячи до недоступності чи затримок у отриманні необхідної інформації.

Згідно звітів про діяльність Державної служби спеціального зв'язку та захисту інформації України, найпоширенішими та найнебезпечнішими є непередбачені помилки, які роблять користувачі, оператори, системні адміністратори та інші особи, що обслуговують інформаційні системи. Ці помилки можуть виявитися загрозами, такими як неправильно введені дані або помилки в програмах, які можуть призвести до збою системи. Час від часу такі помилки можуть створювати ситуації, якими можуть скористатися зловмисники. За даними фахівців, понад 65% шкоди, завданої інформаційним ресурсам, є результатом ненавмисних помилок [107, с. 78]. У порівнянні з природними та техногенними загрозами, такими як пожежі та землетруси, які трапляються рідше, імовірність реалізації цих загроз вважається низькою. Отже, запропоновано максимально автоматизувати інформаційні системи органів виконавчої влади та встановити чіткий контроль за правильністю виконання дій.

Другою за розміром шкоди загрозою є дії підлеглих працівників. У більшості випадків суб'єктами цих дій є штатні працівники структурних підрозділів органів виконавчої влади, які мають глибокі знання роботи інформаційних систем і принципів безпеки [107, с. 79]. Серед них особливо небезпечні співробітники, які відчувають невдоволення або не поділяють цінності своєї організації. Зазвичай такі працівники діють із наміром завдати шкоди організації, в якій вони працюють, і яка, на їхню думку, їх образила. Це може виявитися у руйнуванні обладнання, вбудовуванні логічної бомби, що з часом руйнує програми та дані, введенні невірних даних, знищенні чи модифікації даних, або наданні несанкціонованого доступу до обмежених даних. Зокрема, проблема інсайду – це основний тренд у сфері інформаційної безпеки, який продовжує наростати, і часто включає навмисні дії або дії, пов'язані з недбалістю та низькою кваліфікацією. (рис.2.2)

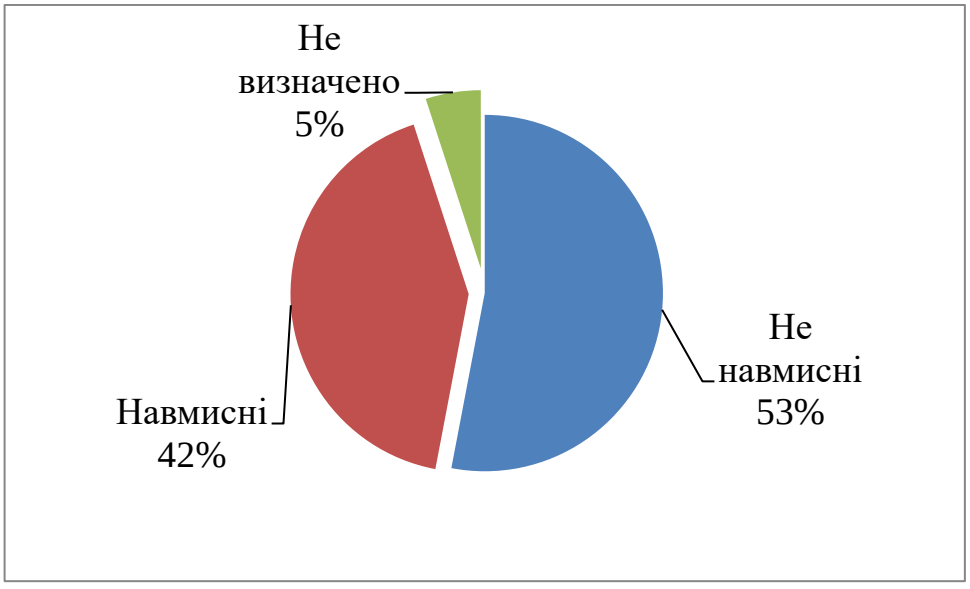

Рисунок2.2. -Відношення кількості навмисних та ненавмисних витоків конфіденційної інформації

Примітка. Складено автором на основі даних Державної служби спеціального зв'язку та захисту інформації України

Людські риси, такі як користь, ненависть (помста, злість), страх та некомпетентність, стають все більш проблематичними з підвищенням цінності

даних, що зберігаються в організації. Ці фактори змушують працівників скоїти крадіжки та неправомірно розголошувати конфіденційну інформацію, несанкціоновано змінювати чи знищувати дані, блокувати доступ до них, випускати троянів та хробаків в мережу, вчиняти інші дії, які іноді можуть призвести до катастрофічних наслідків [16].

Співробітники, які невдоволені своїм становищем, можуть ефективно завдати шкоди інтересам організації, в якій вони працюють. Важливо вдаватися до заходів, щоб при звільненні працівника повністю обмежити його права доступу до інформаційних ресурсів і змінити всі паролі доступу до внутрішньої мережі. Крім того, слід обмежити його комунікацію з особами, які мають доступ до важливої інформації.

Ці загрози мають особливу актуальність для системи державного управління, оскільки кіберзлочинці виявляють підвищений інтерес до неї. Зокрема, статистика Міністерства внутрішніх справ України свідчить, що крім особистого зиску, політичні мотиви є значущою частиною комп'ютерних злочинів (рис. 2.3) [16].

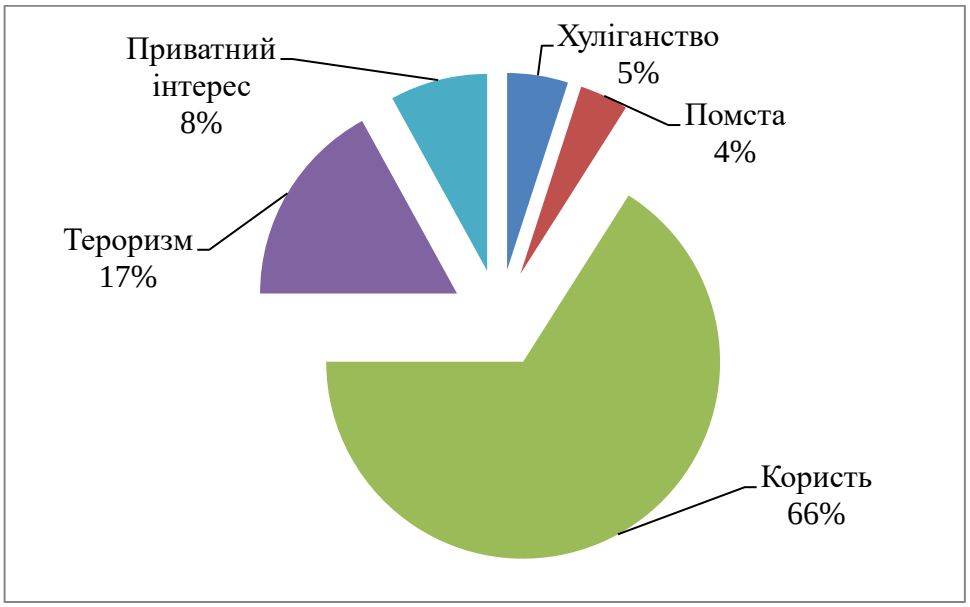

Рисунок2.3. -Статистика мотивів при здійсненні комп’ютерних злочинів

Примітка. Складено автором на основі даних Державної служби спеціального зв’язку та захисту інформації України

Щорічно аналітичний центр InfoWatch узагальнює та представляє глобальні дослідження щодо інцидентів в області внутрішньої інформаційної безпеки. У звіті за 2016 рік було проаналізовано всі випадки витоку конфіденційної інформації, які були висвітлені в ЗМІ по всьому світу та в усіх сферах діяльності. За отриманими даними виявлено, що частка державних установ серед різних видів організацій, що зазнали втрат, складає вже практично 16% (рис. 2.4) [16].

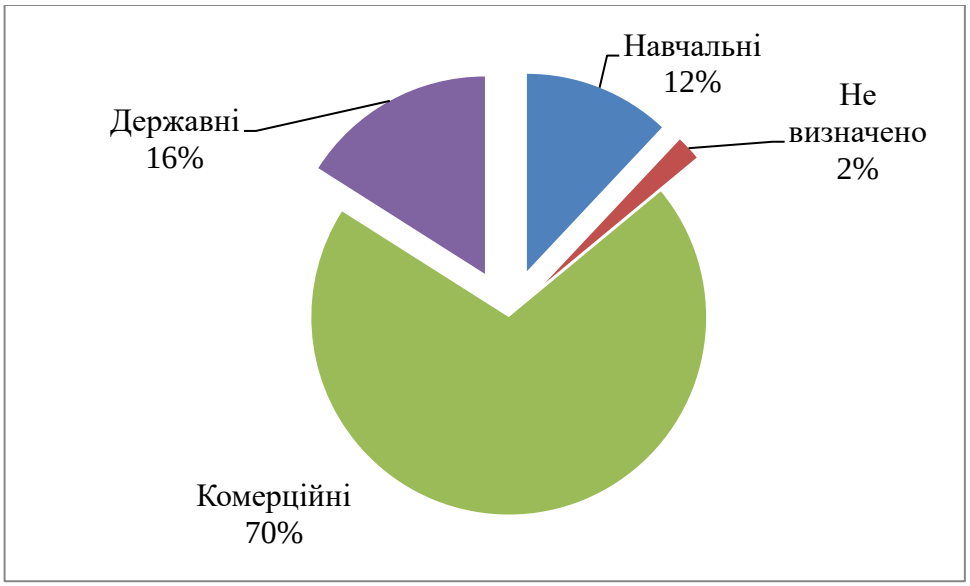

Рисунок 2.4. - Відношення кількості навмисних та ненавмисних витоків конфіденційної інформації в залежності від типу джерела

Примітка. Складено автором на основі даних Державної служби спеціального зв'язку та захисту інформації України

Діяльність Державної служби спеціального зв'язку та захисту інформації України включає в себе дві основні сфери заходів із захисту інформації: криптографічний та технічний захист.

Використання криптографічного захисту інформації може ефективно вирішити проблеми безпеки для високопродуктивних телекомунікаційних систем. Цей вид захисту забезпечує конфіденційність та цілісність даних, що передаються у відкритих мережах, а також забезпечує анонімність об'єкта та його причетність до дій, що здійснюються в телекомунікаційних системах. Криптографія – це комплекс методів перетворення даних з метою приховання

їх інформаційного змісту, а криптографічна система захисту інформації включає алгоритми, протоколи та процедури для формування, розподілу, передачі та використання криптографічних ключів.

Створення системи технічного захисту інформації (ТЗІ) в державі обумовлено необхідністю зниження рівня ймовірності реалізації загроз національній безпеці України в інформаційній сфері та уникнення їх негативних наслідків. Забезпечення технічного захисту інформації є складною задачею, що вимагає спеціалізованої підготовки, нормативного та методичного супроводження, а також технічного оснащення відповідних робіт. Правові та організаційні принципи технічного захисту визначені у "Положенні про технічний захист інформації в Україні" (Указ Президента України від 27 вересня 1999 року №1229/99).

Об'єктами захисту виступають:

1. конфіденційна інформація, яка знаходиться у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації";

2. відкрита інформація, що відноситься до державних інформаційних ресурсів;

3. інформація, отримана від іноземної держави чи міжнародної організації із застосуванням необхідного захисту, який передбачений у рамках міжнародних договорів, щодо яких Верховна Рада України надала згоду на обов'язковість;

4. внформація, яка є державною, банківською, професійною таємницею та таємницею досудового розслідування;

5. службова інформація;

6. інша інформація, вимога щодо захисту якої встановлена законом.

Об'єктами захисту інформації є:

– об'єкти інформаційної діяльності.

– інформаційні (автоматизовані), телекомунікаційні та інформаційно-телекомунікаційні системи (далі - ІТС).

– об'єкти протидії технічним розвідкам.

– об'єкти та системи спеціального зв'язку.

Серед суб'єктів у сфері захисту інформації визначаються:

– Державна служба спеціального зв’язку та захисту інформації України.

– виконавці робіт в галузі захисту інформації.

– власники, розпорядники, користувачі інформації, яка підлягає захисту згідно з цим законом.

– власники, розпорядники, користувачі об'єктів, де відбувається захист інформації.

– фізичні та юридичні особи, що проводять підготовку фахівців, займаються науковою, науково-технічною та виробничою діяльністю у галузі захисту інформації.

Відповідно до законодавства, суб'єктами у сфері захисту інформації також можуть бути міжнародні організації, іноземні держави, їх представництва, громадяни та юридичні особи нерезиденти, особи без громадянства.

Інформація, що містить державну таємницю, підлягає використанню атестованого комплексу технічного захисту інформації на об'єкті інформаційної діяльності. Порядок створення та атестації таких комплексів визначає Державна служба спеціального зв’язку та захисту інформації України. Інформація, що підлягає захисту, обробляється в інформаційно-телекомунікаційній системі за наявності комплексної системи захисту інформації, яка підтверджена відповідністю. Ця відповідність перевіряється підчас проведення державної експертизи в галузі захисту інформації.

Під час обробки інформації, що містить державну таємницю, у інформаційно-телекомунікаційній системі, її захист від технічних витоків забезпечується атестованим комплексом технічного захисту інформації, який у цьому випадку є складовою частиною комплексної системи захисту інформації. Порядок створення цієї комплексної системи та порядок

проведення державної експертизи встановлюються Державною службою спеціального зв’язку та захисту інформації України.

Для забезпечення технічного захисту інформації використовуються засоби технічного захисту, які мають відповідний документ, такий як сертифікат відповідності або позитивний експертний висновок з результатами державної експертизи у сфері технічного захисту інформації. Перелік таких засобів формується компетентним органом у галузі захисту інформації. Оцінка відповідності засобу, який виконує функції захисту інформації, може проводитися під час атестації комплексу технічного захисту інформації або державної експертизи комплексної системи захисту інформації. Зазначений засіб використовується тільки в тій системі захисту, де він був оцінений.

Засоби та алгоритми криптографічного захисту інформації, яка містить державну таємницю, та службової інформації повинні мати свідоцтво про допуск до експлуатації. Процедура допуску визначається Державною службою спеціального зв’язку та захисту інформації України. Планування, будівництво, реконструкція, розробка, створення, модернізація, впровадження та експлуатація об'єктів (систем, зразків, технологій) повинні враховувати вимоги щодо захисту інформації в залежності від рівня обмеження доступу та умов її оброблення чи розголошення. Ці вимоги повинні бути визначені в тендерній документації при закупівлі за бюджетні кошти товарів, робіт чи послуг для виконання цих цілей.

Фізичні та юридичні особи, винні у порушенні законодавства у сфері захисту інформації, несуть дисциплінарну, цивільну, адміністративну чи кримінальну відповідальність відповідно до закону. За стан захисту інформації відповідають керівники державних органів та інших юридичних осіб, а також об'єкти інформаційної діяльності та інформаційно-телекомунікаційні системи, де обробляється або розголошується інформація, що підлягає захисту.

Отже, Державна служба спеціального зв’язку та захисту інформації України впроваджує державну політику в галузі інформаційної безпеки та захисту інформації, забезпечує технічний та криптографічний захист

інформації, виявляє та моніторить інформаційні загрози, а також надає сертифікати фізичним та/або юридичним особам, які виражають бажання займатися діяльністю, пов'язаною із захистом інформації.

РОЗДІЛ 3
УДОСКОНАЛЕННЯ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ЗАБЕЗПЕЧЕНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

3.1. Пріоритетні напрями підвищення ефективності заходів інформаційної безпеки в органах публічного управління

Інформаційна безпека в органах публічного управління є невід'ємною частиною національної безпеки України, спрямованою на захист системи публічного управління від інформаційно-комунікаційних загроз та викликів. Одночасно ця система публічного управління відіграє важливу роль у забезпеченні суспільства, держави та громадян інформаційно-якісними послугами та якісною інформацією. Основними викликами для забезпечення інформаційної безпеки системи публічного управління, зокрема органів публічного управління, є:

1. недостатній рівень захисту системи електронного урядування від інформаційних загроз;

2. постійне виникнення інноваційних інформаційних небезпек, які потребують термінового та ефективного вирішення;

3. необхідність забезпечення високоякісної підготовки кадрового складу у сфері інформаційної безпеки в системі публічного управління.

4. повільний перехід органів публічного управління, зокрема публічного управління, на вітчизняне програмне забезпечення, використання неліцензійних програм, зокрема антивірусних.

З урахуванням вищезазначеного, враховуючи проведене теоретичне дослідження інформаційної безпеки діяльності органів публічного управління в умовах розвитку інформаційного суспільства та аналізу міжнародного досвіду, можна визначити пріоритетні напрями удосконалення управління системою забезпечення інформаційної безпеки органів публічного управління, зокрема Хмельницької обласної ради.

Таблиця 3.1. Напрями удосконалення управління системою забезпечення інформаційної безпеки в органах публічного управління

Складові	Напрями удосконалення	Результат
1	2	3
Інформаційно-аналітичне забезпечення	Впровадження сучасних інформаційних систем забезпечення інформаційної безпеки	Зменшення ризиків інформаційної та кібербезпеки в установі. Уникнення втрат внаслідок розголошення/ витоку і несанкціонованого доступу до джерел інформації
Систематичне здійснення інформаційного аудиту	Залучення зовнішніх аудиторів або навчання персоналу існуючих служб інформаційного забезпечення	Зменшення ризиків інформаційної та кібербезпеки в установі. Уникнення втрат внаслідок розголошення/ витоку і несанкціонованого доступу до джерел інформації
Методичне забезпечення вимірювання інформаційної безпеки та організації моніторингу	Розробка алгоритмів, прийомів, методів, способів і засобів механізму функціонування та механізму управління системою забезпечення інформаційною безпеки	Розроблення профілів та індикаторів ризику інформаційної та кібер небезпеки та визначення області їхнього застосування Контроль ефективності профілів ризику та внесення змін на підставі оновлених даних Визначення чинників ризику інформаційної та кібер небезпеки, надання пропозицій щодо розробки та формалізації конкретних профілів ризику
Забезпечення безпечного функціонування систем електронного урядування	Навчання та інструктаж персоналу щодо організаційно-технічних заходів захисту Придбання сертифікованих електронних ключів	Безпечне використання послуг в галузі електронних комунікацій, безпечне використання пристроїв Уникнення підробки електронних підписів Посилення програмно-технічного рівня протидії загрозам інформаційній безпеці та політиці безпеки в системах е-урядування.
Кадрове забезпечення	Забезпечення установи компетентними працівниками у сфері інформаційної та кібербезпеки. Введення посади спеціаліста з інформаційної та кібербезпеки	Належне виконання покладених обов'язків та забезпечення бажаного рівня інформаційної та кібербезпеки безпеки Концентрація безпекозабезпечувальної діяльності в одному центрі з широким повноваженнями. Можливість швидкого та прямого втручання в діяльність структурних підрозділів для нейтралізації загроз та ризиків в діяльності установи
Формування культури кібербезпеки	Проведення тренінгів/вебінарів з питань кібербезпеки	Забезпечення безпеки робочого середовища, попередження ризиків, пов'язаних із зовнішніми атаками. Зменшення загроз та наслідків кібератак

Примітка. Складено автором.

Ефективність заходів інформаційної безпеки можна підвищити через навчання та інструктаж персоналу щодо організаційно-технічних заходів захисту, що застосовуються на рівні конкретної організації чи системи публічного управління. Вирішення питання про межу між допустимими і неприпустимими ризиками вимагає фахового оцінювання, зокрема врахування специфіки систем е-урядування для конкретних органів публічного управління. Розробка адміністративного рівня служить основою для програми інформаційної безпеки, яка впроваджується на організаційно-процедурному та програмно-технічному рівнях.

Наприклад, в органах публічного управління наразі використовується встановлення Wi-Fi мереж для забезпечення доступу до Інтернету для громадян та персоналу. Проте потрібно враховувати, що загрози, пов'язані з проникненням у Wi-Fi мережу, часто виникають з метою зміни налаштувань DNS сервера у системах електронного урядування. Ця атака може призвести до зміни публічного DNS-сервера на сервер зловмисника, що дозволяє здійснювати різні види кібератак, таких як перехоплення особистих даних та маніпулювання мережевим трафіком.

Цей вид атаки може призвести до витоку конфіденційної інформації, включаючи логіни та паролі, і відкриття доступу для різних інших хакерських атак, таких як злам сайтів, DDOS-атаки та інші. Важливо враховувати, що зловмисник може використовувати ці атаки від імені зареєстрованих користувачів інформаційних систем та їх IP адрес.

Отже, важливим аспектом є дотримання правил безпеки на процедурному рівні у системах електронного урядування, коли використовується Wi-Fi мережа. Це включає в себе:

1. вибір відповідного типу шифрування протоколу для взаємодії з точкою доступу (роутером) Wi-Fi мережі;

2. фільтрацію пристроїв комп’ютерної мережі за їх MAC-адресами;

3. відключення віддаленого доступу до адміністрування роутера чи точки доступу з глобальної мережі Інтернет;

4. використання надійних паролів.

На програмно-технічному рівні заходи протидії загрозам передбачають механізми безпеки, такі як ідентифікація та аутентифікація користувачів, управління доступом, протоколювання та аудит, криптографія, екранування каналів зв'язку, забезпечення високої доступності і так далі. Важливо ефективно керувати інформаційною системою в цілому, зосереджуючись на механізмах безпеки. Зазначені заходи безпеки мають відповідати загальноприйнятим стандартам, бути стійкими до мережевих загроз і враховувати специфіку окремих сервісів.

Додатково, важливим є ефективне управління доступом до комп'ютерів, де доступ до інформаційних систем повинен надаватися лише зареєстрованим користувачам. Комп'ютерні системи, які обслуговують багатьох користувачів, повинні виконувати такі вимоги:

– ідентифікація та перевірка відповідності особистості користувачів, включаючи можливість визначення терміналу чи місця перебування зареєстрованого користувача;

– реєстрація випадків успішного та неуспішного доступу до інформаційної системи;

– надання системи управління паролями, яка забезпечує вибір надійних паролів;

– обмеження часу підключення користувачів до інформаційної системи.

Необхідно забезпечувати доступ до інформаційної системи через надійну процедуру входу. Процедура входу (login) повинна мінімізувати ризик несанкціонованого доступу. Вона повинна:

– утримувати виведення ідентифікаторів системи або додатків на екран до завершення процесу входу;

– виводити загальне попередження про те, що доступ до комп'ютера мають лише зареєстровані користувачі;

– не надавати додаткову інформацію під час процедури входу;

– перевіряти точність реєстраційної інформації лише після завершення введення всіх даних;

– в разі виникнення ситуації збою не вказувати, яка частина введених даних правильна чи неправильна;

– обмежувати кількість невдалих спроб входу в систему (зазвичай рекомендується три спроби), перед тим як розірвати зв’язок з користувачем.

Також важливо слідкувати за доступом до інформаційної системи та використанням Інтернет-ресурсів. Для відповідності стандартам управління доступом, необхідно слідкувати за роботою інформаційної системи та використання ІР. Це необхідно для оцінки ефективності заходів безпеки і забезпечення відповідності політиці безпеки. Всі події та випадки, пов'язані з порушенням режиму безпеки, слід реєструвати в контрольному журналі. Записи в цьому журналі слід зберігати протягом певного періоду для подальших розслідувань та контролю за доступом до інформаційної системи.

Крім того, слід реєструвати випадки успішного доступу до системи, а контрольний журнал повинен містити ідентифікатори користувачів, дату і час входу та виходу, ідентифікаційний код робочої станції та її власника. Важливо встановити процедури спостереження за використанням системи, щоб користувачі виконували тільки дозволені дії. Рівень контролю повинен визначатися на основі незалежної оцінки ризиків для конкретних систем.

Усі дії, пов'язані із спостереженням за системами, повинні мати письмовий дозвіл від керівництва. Для точності контрольних журналів, які можуть бути необхідні під час розслідувань або судових процесів, важливо правильно налаштувати системний годинник комп'ютерів. Неточні записи можуть ускладнити розслідування і підірвати довіру до цих записів.

Важливо регулярно проводити аудит інформаційних систем для мінімізації ризику виникнення збоїв у роботі ІР. Вимоги щодо аудиту та пов'язаних із ним робіт, таких як перевірка робочих станцій, повинні бути попередньо заплановані та узгоджені.

Електронний цифровий підпис (ЕЦП) є одним з найпоширеніших засобів ідентифікації та аутентифікації користувачів у системах електронного урядування. ЕЦП отримується через криптографічне перетворення набору електронних даних, і його використання дозволяє підтверджувати цілісність та ідентифікувати підписувача.

Ефективне зберігання особистого (закритого, секретного) ключа власником робить його підробку неможливою. Електронний документ також стає інтегрованою непідробною одиницею: будь-які несанкціоновані зміни в тексті документу виявляються під час перевірки. Особистий ключ ЕЦП формується генератором випадкових чисел і використовується тільки у парі з відкритим ключем.

ЕЦП підписується лише особистим ключем, який належить його власникові, і залишається унікальною послідовністю символів завдовжки 264 біта, генерація якої є неможливою з відкритого ключа. Особистий ключ повинен бути добре захищений від сторонніх доступів, оскільки його підробка дозволяє підробити ЕЦП.

Також існує концепція Сертифіката, що містить відкритий ключ та підтверджує приналежність цього ключа конкретній особі. Сертифікат містить персональну інформацію про власника, його унікальний реєстраційний номер та термін дії.

З метою гарантування недоторканності інформації, представленої у Сертифікаті, цей документ додатково підписується особистим ключем Центру сертифікації ключів (ЦСК). Сертифікат відкритого ключа може бути оприлюднений на веб-сайті відповідного Центру сертифікації ключів (ЦСК) згідно з умовами Договору про надання послуг ЕЦП.

В Україні існує Національна система електронного цифрового підпису, яка включає в себе:

Центральний засвідчувальний орган;

Акредитовані центри сертифікації ключів;

Центри сертифікації ключів;

Контролюючий орган.

Послуги з надання ЕЦП в Україні реалізуються акредитованими центрами сертифікації ключів. Акредитований центр сертифікації ключів — це центр, де ключі проходять сертифікацію відповідно до визначених державою процедур.

Центральний засвідчувальний орган в Україні відповідає за акредитацію таких сертифікаційних центрів. Поточний перелік усіх акредитованих центрів сертифікації ключів доступний на веб-сайті Центрального засвідчувального органу. Важливо відзначити, що акредитований центр має право обслуговувати виключно посилені сертифікати ключів, відмінно від звичайних центрів сертифікації ключів.

Акредитований центр сертифікації ключів (АЦСК) повинен виконувати всі обов'язки і вимоги, що встановлені законодавством для центру сертифікації ключів, та додатково зобов'язаний використовувати надійні засоби електронного цифрового підпису для надання послуг ЕЦП. АЦСК має право:

- надавати послуги електронного цифрового підпису та обслуговувати виключно сертифікати відкритих ключів (відповідно до статті 9 Закону України "Про електронний цифровий підпис");

- отримувати та перевіряти інформацію, необхідну для реєстрації підписувача та формування посиленого сертифіката ключа, безпосередньо в юридичної або фізичної особи чи її представника.

Перелік міжнародних та європейських стандартів, інших актів технічного регулювання для гармонізації системи електронного цифрового підпису визначено наказом Міністерства юстиції України та Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 05.12.2013 р. № 2563/5/645 (у редакції наказу від 25.12.2014 р. № 2170/5/703).

Отже, електронний цифровий підпис (ЕЦП) вдало використовується для ідентифікації підписувача електронного документа і надає можливість чітко визначити джерело інформації у цифрових файлах користувачів.

Однак, говорячи про безпеку використання ЕЦП, слід акцентувати увагу на захисті особистих (таємних) ключів користувачів. Зловмисник, який отримає доступ до чужого ключа, має можливість використання електронного цифрового підпису, а саме, накладання підпису на документах, здійснення дій в інформаційних системах, зміни записів у базах даних, проведення нелегітимних фінансових транзакцій, розшифрування зашифрованої інформації та інше.

Міжнародний досвід використання засобів ЕЦП підтверджує застосування широкого спектру нормативних і технічних заходів для захисту особистих ключів від несанкціонованого використання. Один з найбільш надійних заходів — це використання захищеного носія особистих ключів. Цей носій має вбудовані апаратно-програмні засоби для захисту даних від несанкціонованого доступу, включаючи запобігання ознайомленню з параметрами особистих ключів та їх копіюванню.

Іншими словами, захищений носій є своєрідним "маленьким комп'ютером", де створюються (генеруються), зберігаються та використовуються ключі. Він працює на засаді "чорного ящика", де відомо, що подається на вхід і що видається на виході, але внутрішні процеси невідомі та захищені від зовнішнього доступу. У відміну від інших носіїв, ключ не створюється, не зберігається і не використовується на робочому комп'ютері в оперативній пам'яті, що робить його неможливим для викрадення.

Замість того, щоб генерувати ключі на незахищених носіях, які можуть бути вкрадені шляхом копіювання або за допомогою шкідливого програмного забезпечення, застосовується захищений носій. Важливо відзначити, що вкрасти ключ можливо тільки разом із носієм, і власник ключа буде про це відомий. У випадку втрати носія, власник має негайно повідомити центр сертифікації ключів і заблокувати сертифікат ключа.

Застосування захищеного носія ключів не є лише модою, але і необхідним засобом захисту інтересів його власника при використанні електронного цифрового підпису. З точки зору користувача, перевагою

захищеного носія є неможливість копіювання ключа, що перешкоджає зловмисникам вчиняти дії від імені його власника.

Захищений носій особистих ключів є засобом кваліфікованого електронного підпису або печатки, який створено для зберігання особистого ключа та має вбудовані апаратно-програмні засоби для захисту записів на ньому від несанкціонованого доступу, включаючи запобігання ознайомленню з параметрами особистих ключів та їх копіюванню.

Статтею 17 Закону України "Про електронні довірчі послуги" передбачено, що суб'єкти, уповноважені державою на здійснення функцій державного реєстратора, для засвідчення чинності відкритого ключа використовують лише кваліфікований сертифікат відкритого ключа. При реалізації повноважень, спрямованих на набуття, зміну чи припинення прав та/або обов'язків фізичної або юридичної особи, вони застосовують виключно засоби кваліфікованого електронного підпису чи печатки, які мають вбудовані апаратно-програмні засоби для захисту записів на них від несанкціонованого доступу та забезпечують безпосереднє запобігання ознайомленню з параметрами особистих ключів та їх копіюванню.[63].

Пунктом 1 статті 4 "Порядку використання електронних довірчих послуг в органах публічного управління, підприємствах, установах та організаціях державної форми власності", прийнятого Постановою № 749 Кабінету Міністрів України від 19 вересня 2018 року, встановлено, що державні установи використовують виключно кваліфіковані сертифікати відкритих ключів для засвідчення чинності відкритого ключа та застосовують захищені носії особистих ключів для виконання повноважень, пов'язаних із набуттям, зміною або припиненням прав та/або обов'язків фізичної або юридичної особи згідно із законодавством, а також для здійснення інформаційного обміну з іншими юридичними особами.

З метою забезпечення гарантованої підтримки доступу до Єдиних та Державних реєстрів, які належать Міністерству юстиції України, АЦСК органів юстиції України, відповідно до встановленого Порядку, постачає

захищені носії особистих ключів таких видів: "Алмаз-1К" (виробництво ПрАТ "Інститут інформаційних технологій"), "Кристал-1" (виробництво ПрАТ "Інститут інформаційних технологій"), "SecureToken-337К" (виробництво ТОВ "Автор"), "SecureToken-337М" (виробництво ТОВ "Автор"), "CryptoCard-337" (виробництво ТОВ "Автор").

Таким чином, протистояння загрозам безпеки в інформаційних системах органів публічного управління, включаючи місцеве самоврядування, вимагає комплексного підходу для забезпечення інформаційної безпеки, який включає заходи на різних рівнях, таких як законодавчий, адміністративний, процедурний та програмно-технічний.

3.2. Впровадження інформаційного аудиту з метою підвищення інформаційної безпеки органів публічного управління

Використання інформаційних систем в органах публічного управління сприяє забезпеченню інформаційної прозорості управління, розширюючи можливості громадян та їх об’єднань в контролюванні за діяльністю органів. У сучасних умовах вирішення проблем аудиту інформаційного забезпечення та інформаційних технологій в органах публічного управління може виконуватися фахівцями відділів внутрішнього аудиту даного органу або за допомогою зовнішніх аудиторів, які спеціалізуються на питаннях інформаційного аудиту.

Основним завданням інформаційного аудиту в органах публічного управління є оцінка фактичного стану інформаційних ресурсів та комп’ютерних технологій, а також визначення їх відповідності вимогам, які висуваються до них з боку органу публічного управління. Інформаційний аудит слід розглядати як важливий компонент системи внутрішнього аудиту в органах публічного управління. В рамках інформаційного аудиту можна створити "інформаційну карту" системи електронного уряду, яка може

слугувати основою для підписання рішень та обґрунтування інформаційної стратегії організації. Цей процес дозволяє аналізувати типи та обсяг інформації в масштабах всієї організації. Застосування інформаційного аудиту в органах публічного управління дозволяє підвищити рівень інформованості посадових осіб та населення щодо їх діяльності.

Інформаційний аудит володіє також наступними можливостями:

1. визначення інформаційних потреб органів публічного управління, їх структурних підрозділів та конкретних потреб окремих посадових осіб.

2. аналіз складу інформації, що створюється та оцінка її цінності для організації.

3. оцінка інтелектуальних активів органів публічного управління та виявити в інформаційному забезпеченні.

4. вивчення стану та оцінка використання внутрішніх і зовнішніх інформаційних ресурсів та визначення шляхів їх ефективного використання.

5. складання карти інформаційних потоків та виявлення вузьких місць в цих потоках.

6. обґрунтування напрямків вдосконалення інформаційного забезпечення, інформаційної інфраструктури та захисту інформації в органах публічного управління.

Практичне впровадження аудиту інформаційних технологій має наступні переваги: системний підхід до управління IT-середовищем; розробка технології проведення аудиту інформаційних технологій; ефективний вибір і поєднання методів функціональних видів IT-аудиту для комплексного та максимально ефективного дослідження IT-середовища, уникнення фрагментарності, невизначеності та інших проблем.

Аудитор повинен провести детальний аналіз та скласти висновок з усіх суттєвих аспектів комп'ютерно-інформаційної системи, зокрема [6]:

розгляд функціонування системи, включаючи організацію, введення, настроювання та відновлення даних;

забезпечення архівування та зберігання даних;

наявність спеціальних контрольних процедур для моніторингу функціонування середовища обробки даних;

аналіз програмного забезпечення та визначення наявності ліцензій;

відповідність застосованих алгоритмів вимогам нормативної документації щодо обліку та звітності;

гнучкість у реагуванні на зміни законодавства з погляду настроювання та відновлення програмного забезпечення;

можливості розширення функціональності наявних комп'ютерно-інформаційних систем;

питання інформаційної безпеки, зокрема обмеження несанкціонованого доступу;

аналіз загальної інформаційної політики та планів розвитку системи інформаційних технологій суб'єкта, який перевіряється.

Велика увага під час перевірки приділяється питанням надійності та безпеки системи. Дефекти в організації контролю доступу виявляються через спеціалізовані аудиторські процедури, такі як періодичний аналіз прав користувачів, системний підхід до поділу повноважень та обмеження доступу до бізнес-функцій. Невиконання цих вимог може призвести до серйозних наслідків, таких як несанкціонований доступ до даних та виконання неавторизованих операцій у системі, а також невизначеність відповідальності за внесені зміни. Аудитор може рекомендувати створення матриці розмежування повноважень для забезпечення дотримання принципів мінімальних прав доступу, документування всіх змін у системі контролю доступу та їх відповідність посадовим обов'язкам.

Організаційна структура аудиту інформаційної безпеки в органах публічного управління представлена у таблиці 3.2.

Аудиторський висновок щодо реалізації проекту надає повну картину процесу, дозволяючи оцінити поточний стан, виявити недоліки, визначити невідповідності та можливі ризики, пов'язані з ними, і надати рекомендації щодо їх усунення. Це надає керівникам можливість оцінити якість

впровадження, аналізувати потенційні можливості системи, визначати пріоритетність запланованих завдань і робити вибір щодо подальшої стратегії розвитку.

Таблиця 3.2. Організаційна модель аудиту інформаційної безпеки Хмельницької обласної ради

Аудит ІТ-безпеки
Мета: надання обґрунтованого аудиторського висновку щодо поточного стану, сильних і слабких сторін інформаційної безпеки організації, а також рекомендацій щодо її удосконалення для задоволення потреб
Цілі: 1) оцінити і проаналізувати ефективність, економічність, надійність ІТ-безпеки тощо для задоволення потреб, вирішення задач і досягнення цілей організації, а також виявити можливі шляхи покращення; 2) встановити відповідність інформаційної безпеки затвердженим політикам, сценаріям, нормам, правилам та ІТ-стратегії, а також, за необхідності, певним еталонам (стандартам, кращим практикам, критеріям зрілості тощо); 3) виявити "вузькі місця" (недоліки, невідповідності, інциденти тощо) в ІТ-безпеці; 4) отримати аудиторський висновок і рекомендацій за визначеними цілями аудиту та ін. У кожному конкретному випадку аудиту зазначені вище цілі можуть бути конкретизовані і деталізовані відповідно до потреб його замовника, наприклад: 1) виявити і усунути причини певного виду інцидентів інформаційної безпеки; 2) оцінити ефективність впроваджених заходів ризик-менеджменту ІТ-середовища тощо.
Ініціація:1) плановий аудит; 2) позаплановий аудит; 3) в рамках іншого аудиту (наприклад, фінансового, комплексного ІТ-аудиту тощо); 4) сертифікація; 5) зміна моделі бізнесу або окремих бізнес-процесів (реінжиніринг); 6) зміна затверджених політик, сценаріїв, стандартів, норм, правил інформаційної безпеки тощо; 7) високий рівень ризику ІТ-середовища; 8) розслідування інцидентів, пов'язаних з порушенням інформаційної безпеки; 9) впровадження нових програмно-технічних засобів ІТ-безпеки тощо.
Об'єкти: 1) політики, сценарії, стандарти, норми, правила тощо інформаційної безпеки; 2) організаційна структура і функціональні обов'язки персоналу з ІТ-безпеки; 3) система управління інформаційною безпекою; 4) програмно-технічні засоби інформаційної безпеки; 5) середовище ІТ-ризику/система ІТ-контролів та ін. У кожному конкретному випадку аудиту зазначені вище об'єкти можуть бути конкретизовані і деталізовані відповідно до потреб його замовника, наприклад: 1) антивірусні та антиспамові заходи інформаційної безпеки; 2) засоби шифрування конфіденційних даних; 3) політика паролів і авторизації тощо.
Заходи: 1) оцінка й аналіз середовища ІТ-ризиків і відповідних контрзаходів; 2) оцінка й аналіз сукупної вартості володіння ІТ-безпекою; 3) оцінка й аналіз ефективності, надійності і достатності організаційних заходів, програмно-технічних та фізичних засобів інформаційної безпеки; 4) оцінка й аналіз рівня конфіденційності, цілісності і доступності інформаційних ресурсів; 5) аналіз інцидентів ІТ-безпеки та ін.
Методи: 1) *інспекційні* (інтерв'ю, анкетування, аудиторська вибірка та ін.); 2) *аналітичні* (оцінка ІТ-ризику та ін.); 3) *еталонні*.
Результати: 1) аудиторський висновок стосовно поточного стану ІТ-безпеки організації, відповідно до визначених цілей, задач і обмежень аудиту, забезпечений аудиторськими доказами і свідоцтвами; 2) рекомендації аудитора стосовно заходів, які необхідно виконати для усунення виявлених в інформаційній безпеці недоліків, а також невідповідностей потребам організації чи вимогам еталону, обраного для порівняння.

Примітка. Запропоновано автором.

Під час проведення аудиту інформаційної безпеки в органах публічного управління та перевірки готовності установи до роботи з інформаційними системами, аудиторам слід звертати увагу, зокрема, на підготовку персоналу, відповідального за інформаційну безпеку, організацію доступу до елементів інформаційної системи та обмеження програмно-апаратного доступу. Одним із способів підвищення безпеки органів публічного управління є систематичне і постійне підвищення кваліфікації працівників, зокрема, участь у конференціях, симпозіумах та виставках, присвячених інформаційній безпеці. Рекомендується також оцінити витрати на участь у навчальних заходах, зокрема, з питань захисту та протидії кіберзагрозам тощо.

При аналізі заходів, спрямованих на захист інформації, аудиторам слід звернути увагу на наявність та якість документів, що регламентують використання інформаційної системи, зокрема, систем електронного урядування. Важливо розробити докладні інструкції для користувачів щодо роботи з інформаційними системами, включаючи рекомендації щодо обмеження довжини, складності та часу життя паролів, унікальності власника паролю, заборони використання функцій автоматичного запам'ятовування паролів та інші аспекти безпеки. Також важливо врахувати питання, пов'язані із забороною використання приватної електронної пошти для службових цілей, моніторингом та документуванням подій, що стосуються інформаційної безпеки.

Під час проведення аудиту інформаційної безпеки в органах публічного управління, важливо звертати увагу не лише на традиційні організаційні й технічні заходи, а й на психологічну готовність працівників до методів соціальної інженерії. Такий підхід до проведення аудиту в органах публічного управління дозволяє забезпечити інформаційну безпеку на високому рівні, враховуючи стрімкий розвиток технологій та комплексний підхід до інформаційних систем, що вимагає спеціальної підготовки аудиторів та залучення експертів.

Слід також наголосити, що аудит інформаційної безпеки не є засобом контролю чи перевірки, а скоріше є інструментом, що надає впевненість користувачам у тому, що їхня система є надійною, безпечною та не стане джерелом фінансових чи соціальних ризиків у суспільстві.

Важливо також пам'ятати, що зловмисники не використовують лише технічні засоби, коли намагаються отримати цінну інформацію. Часто вони застосовують психологічні методи, щоб обдурити користувачів та здобути необхідну інформацію. Наука, що вивчає отримання інформації через соціальні методи, а саме, використання людських слабкостей та недостатніх заходів безпеки, відома як соціальна інженерія. Це також є засобом переконання користувачів надавати важливу інформацію.

У сучасних умовах для організації та проведення атак широко використовуються різноманітні інструменти (канали), такі як електронна пошта (e-mail), телефонний зв'язок, аналіз сміття, особистісні підходи, реверсивна соціальна інженерія. Завдяки відносній анонімності інтернету соціоінженерам вдається отримувати доступ до об'єкта атаки та використовувати його системні ресурси.

Враховуючи вищевикладене, аудиторам слід зосередити свою увагу на готовності працівників органів публічного управління протистояти методам соціальної інженерії. Цю готовність можна забезпечити як за допомогою підвищення кваліфікації працівників на спеціалізованих курсах, так і через проведення навчальних заходів всередині установи.

Інформаційний аудит виявляється вкрай важливим елементом посилення контролю за використанням інформаційного забезпечення та інформаційних технологій в органах публічного управління, оскільки він надає можливість отримати об'єктивні, якісні та кількісні оцінки поточного стану їхньої діяльності у цьому сегменті.

ВИСНОВКИ

В рамках магістерської роботи було проведено теоретичний аналіз та запропоновано вирішення наукової проблеми щодо удосконалення публічного управління в сфері забезпечення інформаційної безпеки України. Отримані результати дослідження дозволили сформулювати висновки та пропозиції, які мають як теоретичне, так і практичне значення.

1. Проведений критичний аналіз літературних джерел встановив, що інформаційна безпека діяльності органів публічного управління визначається рівнем захисту інформаційних баз даних, систем та посадових осіб органів публічного управління. Цей рівень захисту спрямований на мінімізацію негативних наслідків використання інформаційних продуктів та технологій, забезпечення їх захисту від несанкціонованого доступу та втручання. З інформаційної точки зору, інформаційна безпека включає три складові: задоволення інформаційних потреб суб'єктів; забезпечення безпеки інформації; забезпечення захисту суб'єктів інформаційних відносин від негативного інформаційного впливу.

2. Аналіз світового досвіду у сфері інформаційної безпеки свідчить про те, що основними напрямами вирішення цієї проблеми є: захист прав особистості в інформаційній сфері, захист державних інтересів, захист підприємницької та фінансової діяльності, захист інформації від комп'ютерних злочинів. Доведено, що розвинені країни вже сформулювали та успішно застосовують більш досконале законодавство з питань інформаційної безпеки. З урахуванням цього визначено важливість використання позитивного зарубіжного досвіду для вдосконалення механізмів захисту інформації та адаптації їх до світових стандартів регулювання, які визначаються глобалізаційними процесами в усьому світі.

3. При аналізі інституційного забезпечення захисту інформації в Україні стало відомо, що існує п'ять основних державних органів, які відповідають за управління інформаційною сферою, а саме: два регуляторних - Національна рада України з питань телебачення і радіомовлення (Національна рада) та

Національна комісія з питань регулювання зв'язку та інформатизації (НКРЗІ), а також три виконавчі - Державний комітет з телебачення та радіомовлення України (Держкомтелерадіо України), Державне агентство з питань електронного урядування України та Державна служба спеціального зв’язку та захисту інформації України (Держспецзв’язку України). Крім того, більше 20 допоміжних органів державної влади також взяли участь у вирішенні завдань та програм в інформаційній сфері, таких як Служба безпеки України, Генеральне управління розвідки Міністерства оборони України, Служба зовнішньої розвідки України, Міністерство зовнішніх справ України, Міністерство юстиції України, Комітет Верховної Ради України з питань свободи слова та інформатизації, Комітет Верховної Ради України з питань інформатизації та інформаційних технологій та інші.

4. Визначено, що Державна служба спеціального зв’язку та захисту інформації України є центральним виконавчим органом зі спеціальним статусом, який діє під керівництвом Кабінету Міністрів України. Ця служба відповідає за формування та реалізацію державної політики у сферах організації спеціального зв'язку, захисту інформації, телекомунікацій та користування радіочастотним ресурсом України. Основними завданнями є забезпечення формування та реалізація державної політики у сферах криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом, захисту державних інформаційних ресурсів та інформації в інформаційно-телекомунікаційних системах та об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів з приводу захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв’язку, Національної системи конфіденційного зв’язку.

5. Пропонуються шляхи підвищення рівня інформаційної безпеки в органах публічного управління. Зазначено, що завдання адміністративного рівня боротьби з загрозами інформаційної безпеки повинно включати ключові кроки, такі як визначення керівних документів і стандартів, методів

управління ризиками та проведення сертифікації відповідності стандартам інформаційної безпеки. Розробка програми інформаційної безпеки ґрунтується на адміністративному рівні та реалізується на організаційно-процедурному та програмно-технічному рівнях. Організаційні заходи інформаційної безпеки входять до процедурного рівня протидії загрозам, а програмно-технічний рівень включає механізми безпеки, такі як ідентифікація користувачів, управління доступом, протоколювання та аудит, криптографія, екранування каналів зв’язку, забезпечення високої доступності і т. д. Пропонується впровадження обов'язкового дотримання правил безпеки процедурного рівня в системах електронного урядування для роботи з Wi-Fi мережею, включаючи вибір правильного типу шифрування протоколу взаємодії з точкою доступу, фільтрацію пристроїв за MAC-адресою, відключення віддаленого доступу до адміністрування роутера чи точки доступу з Інтернету та використання стійких паролів. Також визначено передумови для використання захисту особистих електронних ключів від несанкціонованого використання, зокрема за допомогою захищеного носія особистих ключів із вбудованими апаратно-програмними засобами для захисту даних від несанкціонованого доступу та копіювання.

6. Описано організаційні принципи впровадження інформаційного аудиту з метою підвищення інформаційної безпеки в органах публічного управління. Визначено, що його завданням є оцінка реального рівня захисту інформації та кіберзахисту, оцінка здатності протистояти зовнішнім і внутрішнім загрозам та розробка рекомендацій щодо впровадження організаційних та програмно-технічних заходів для забезпечення захисту інформаційних та інших ресурсів в інформаційно-телекомунікаційних системах. Запропоновано організаційну модель аудиту інформаційної безпеки в органах публічного управління. В рамках навчання персоналу основам інформаційної безпеки пропонується розробити процедурні документи, такі як пам’ятки користувача Інтернет для виявлення та реагування на атаки, спрямовані на отримання інформації чи інші незаконні дії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аудит інформаційних систем URL: http: www.itsway.kiev.ua/index.phplanguage=ua&main_managemen=services& managemen=audit.
2. Бабак В. П. Теоретические основы защиты информации: НАН Украины, Ин-т проблем безопасности АЭС. Чернобыль, 2012. С. 721.
3. Баранов О. А. Інформаційне право України : стан, проблеми, перспективи. К. : Видавничий дім «СофтПрес», 2005. 316 с.
4. Баровська А. В. Механізми реалізації державної інформаційної політики у сфері європейської інтеграції. К.: Міністерство регіонального розвитку та будівництва України, Академія муніципального управління, 2010. С. 5.
5. Бєляков К.І. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення. Монографія К.: КВІЦ, 2008. 576 с.: іл..
6. Біленчук П. Д. Комп'ютерний тероризм: суперхакери, кібер-терористи, кібер-криміналісти. К.: Наука і життя, 2018. С. 5 – 86.
7. Богуш В. М. Інформаційна безпека держави. К.: «МК-Прес», 2005. С. 39.
8. Братель О. Поняття та зміст доктрини інформаційної безпеки. *Право України.* 2006. № 5. С. 36–41
9. Брижко В.М. Основи систематизації інформаційного законодавства : теоретичні та правові засади : монографія. К.: ТОВ ПанТоті, 2012 р. 304 с.
10. Бурило Ю.П. Організаційно-правові питання державного управління в інформаційній сфері.: Дис. канд. наук: 12.00.07. 2008. URL: http: adminpravo.com.ua/index.php/2010-04-13-14-05-13/145-2010-09-28-13-27-30/1942-22.
11. Бурячок В. Л. Соціальна інженерія як метод розвідки інформаційно-телекомунікаційних систем. *Захист інформації*. 2012. № 4. С. 5 – 12.

12. Використання інформаційних технологій в судах: Навчальний посібник. Ємельянов С.Л., Логінова Н.І., Тодощак О.В., Якутко В.Ф. Одеса: Фенікс, 2014. 157 с.
13. Всеобщая декларация прав человека. URL: http: zakon4.rada.gov.ua/laws/show/995_015.
14. Головань С. Про термінологію в області безпеки інформації. *Збірник наукових праць Інституту проблем моделювання в енергетиці імені Г.Є. Пухова.* 2013. Вип. 66. С. 31–35.
15. Голубев В.О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: монографія. За заг. ред. докт. юрид. наук Р.А. Калюжного. Запоріжжя: Просвіта, 2011. 252 с.
16. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть. *Вісник Київського університету імені Т.Шевченка*. 2009. Вип. 14: Міжнародні відносини. С. 46-48
17. Горбулін В. П. Проблеми захисту інформаційного простору України : монографія. Інтситут проблем національної безпеки. К. : Інтертехнологія. 2009. 136 с.
18. Горовий В. Соціальні інформаційні комунікації, їх наповнення і ресурс. К., 2010. С. 135.
19. Горовий В. Соціальні інформаційні комунікації, їх наповнення і ресурс. Наук. ред. Л. А. Дубровіна; НАН України, Нац. б-ка України ім. В. І. Вернадського. К., 2010. С. 141–146.
20. Давидюк А. В. Протидія автоматизованим засобам використання соціальної інженерії». Матеріали IX Всеукраїнської науково-практичної конференції «Актуальні проблеми управління інформаційною безпекою держави» (30 березня 2018 р., Київ). 2018 С. 346-347.
21. Данільян О. Національна безпека України: сутність, структура та напрями реалізації. Х. : «ФОЛІО», 2002. 296 с.
22. Довгань О. Д. Окремі аспекти методології вивчення проблем інформаційної безпеки. *Інформаційна безпека людини, суспільства,*

держави. 2015. № 1 (17). С. 17–28.

23. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. К.: ООО «ТИД «ДС», 2001. С. 650.
24. Ємельянов С. Л. Основи інформаційної безпеки: Навчальний посібник. Одеса: «Фенікс», 2014. С. 19–29.
25. Арістова І. В., Сулацький Д. В. Інформаційна безпека людини як споживача телекомунікаційних послуг. К. : *Ред. журн. «Право України»*; Х. : Право, 2013. 184 с.
26. Скулиш Є. Д., Остроухов В. В., Романов І. В. Інформаційна безпека України: теорія, практика, система захисту.та ін. К.: НАСБ України, 2012. 462 с.
27. Онищенко О. С., Горовий В. М., Попик В. І. Інформаційна складова соціокультурної трансформації українського суспільства. та ін.; НАН України, Нац. б-ка України ім. В. І. Вернадського. К., 2012. С. 5–35.
28. Цимбалюк В.С. Інформаційне право: концептуальні положення до кодифікації інформаційного законодавства. К.: Освіта України, 2011. 426 с.
29. Капица Ю. Проблемы правовой охраны конфиденциальной информации в Украине (часть 2) *Інтелектуальна власність* № 3, Київ, 2014, с. 27 – 33.
30. Карчевський М.В. Кримінально-правова охорона інформаційної безпеки України : дис. на здобуття наук. ступеня док. юрид. наук : спец. 12.00.08 «кримінальне право та кримінологія; кримінально-виконавче право». М.В.Карчевський. К., 2013. 536 с.
31. Кісілевич-Чорнойван О. М. Міжнародне інформаційне право: навч. посіб. К. : ДП «Вид. дім «Персонал», 2011. 160 с.
32. Климчук О.О. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. *Інформаційна безпека людини, суспільства*, держави. 2015. № 3. С. 75–83.

33. Коваль З.В. Динаміка світової управлінської реакції на кіберзагрози: уроки для України. *Демократичне врядування*. 2014. Вип. 14. URL: http: nbuv.gov.ua/UJRN/DeVr_2014_14_5.
34. Конвенция «О защите прав человека и основных свобод». URL: http: www.hand-help.ru/documents/evrop_konv.html.
35. Конституція України. Прийнята Верховною Радою України 28 червня 1996 року. *Відомості Верховної Ради України*. 1996. №30 Ст. 141. Офіційний сайт Верховної Ради України. URL: http: zakon3.rada.gov.ua/laws/show/1401-19.
36. Кормич Б. А. Інформаційне право. Підручник. Харків: БУРУН і К, 2011. 334с.
37. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України. Одеса: Юрид. література, 2007. 471 с.
38. Кормич Б. Інформаційна безпека: організаційно-правові основи: Навчальний посібник. К.: Кондор, 2015. 382 с.
39. Кормич Б.А. Інформація як категорія інформаційного права. *Актуальні проблеми держави і права: Зб. наук. праць.* Одеса: Юридична література, 2012. Вип. 16. С. 367 - 374.
40. Костицька І. Політико-правова природа народного представництва. *Право України*. 2006. № 10. С. 9–14.
41. Курас І. Інформаційні ресурси України: стратегія розвитку. *Бібл. вісн.* 2001. № 1. С. 2–6.
42. Литвиненко О. В. Інформаційний істеблішмент України у контексті національної безпеки. *Стратегічна панорама*. 2002. № 2. С. 172–176.
43. Литвиненко О. Спеціальні інформаційні операції та пропагандистські кампанії. К.: ВКФ Сатсанга, 2000. 222 с.
44. Ліпкан В.А. Національна безпека України : навч. посіб. 2-ге вид. К. : КНТ, 2009. 576 с.
45. Максименко Ю. Є. Сучасні проблеми криміналізації інформаційної сфери. *Актуальні проблеми політики : Зб. наук. праць.* Голов. ред. С. В.

Ківалов; відп. за вип. Л. І. Кормич. Одеса : ПП “Фенікс”. 2005. Вип. 26. С. 294-299.

46. Марутян Р. Національні інформаційні ресурси як першооснова інформаційного суверенітету України. Актуальні проблеми міжнародної безпеки: український вимір. К.: Стилос, 2010. С. 496.
47. Марущак А. До питання про забезпечення безпеки інформаційного простору та інформаційних ресурсів. *Юридичний радник.* Х., 2009. № 4. С. 64–67.
48. Носов В. В. Метод проектирования оптимальной системы защиты информации. *Науково-технічний збірник "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні"*, Київ, 2004, вип. 9, с. 94 – 102
49. Олійник О.А. Захист інформації в умовах інформаційного суспільства. *Право України*. 2015. № 10. С. 100-103.
50. Олійник О.В. Методологічні засади забезпечення системи інформаційної безпеки та її складової – захисту інформаційних ресурсів. *Право і безпека*. 2014. № 1 (52). С. 103–109.
51. Олійник О.В. Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної держави. *Держава і право: зб. наук. пр.* 2001. Вип. 13. С. 534–541.
52. Романюка Б. В., Скулиша Є. Д. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій. К.: НАСБ України. С. 351;
53. Бутузов В. М., Гавловський В. Д., Довгань О. Д. Словник термінів з кібербезпеки. К.: ВБ «Аванпост-Прим», 2012. С. 70.
54. Цимбалюк В., Гавловський В., Гриценко В. Основи інформаційного права України. К: “Знання”, 2014. 274 с.
55. Остроухов В. В. Інформаційна війна як форма ведення інформаційного протиборства. Актуальні проблеми забезпечення інформаційної безпеки держави. К.: Наук.-вид. відділ НА СБ України, 2009. С. 24 – 26.

56. Остроухов В.В. Інформаційна безпека (соціально-правові аспекти) Підручник ; за заг. ред. Є.Д.Скулиша. К. : КНТ, 2010. 776 с.
57. Офіційний веб-сайт Ради національної безпеки і оборони URL: http: www.rnbo.gov.ua
58. Петрик В. М. Соціально-правові основи інформаційної безпеки; за ред. Остроухова В. В. К.: Росава, 2007. С.10.
59. Положення про Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації: указ Президента України від 23.11.2011. № 1067/2011. URL: http: zakon1.rada.gov.ua/laws/show/1067/2011
60. Попова С.М. Інформаційне забезпечення діяльності органів податкової служби. *Право і безпека*. Харків: ХНУВС, 2011. № 2 (39). С. 273–277.
61. Почепцов Г. Г. Інформаційна політика: навч. посіб. 2-ге вид. стер. К.: Знання, 2008. 663 с.
62. Про використання захищених носіїв особистих ключів в інформаційних системах. URL. http: ca.informjust.ua/partnership_znok
63. Про внесення змін до Закону України «Про інформацію»: Закон України від 13.01.2011 р. *Офіційнийвісник України*. 2011. № 10. Ст. 445.
64. Про Державну службу спеціального зв'язку та захисту інформації України: закон України,№ 3475-IV від 23.02.2006. URL: http: zakon4.rada.gov.ua/laws/show/3475-15
65. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII. Офіційний сайт Верховної Ради України. URL: http:zakon3.rada.gov.ua/laws/show/3855-12.
66. Про Доктрину інформаційної безпеки України: проект указу Президента України URL: http: comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025.
67. Про електронний цифровий підпис: Закон України від 22.05.2003 № 852-IV. URL: http: zakon5.rada.gov.ua/laws/show/852-15

68. Про електронні довірчі послуги: Закон України від 5 жовтня 2017 року № 2155-VIII URL. http: zakon.rada.gov.ua/laws/show/2155-19
69. Про затвердження Порядку надання ідентифікаторів доступу до Єдиних та Державних реєстрів, держателем яких є Міністерство юстиції України,: Наказ Міністерства юстиції України 15.12.2015 № 2586/5, зареєстрованого в Міністерстві юстиції України 15 грудня 2015 р. за № 1568/28013 (зі змінами). URL: http: zakon5.rada.gov.ua/laws/show/z1568-15#n21
70. Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності: Постанова КМУ від 19 вересня 2018 року № 749. URL: http: zakon.rada.gov.ua/laws/show/749-2018-%D0%BF
71. Про захист економічної конкуренції: Закон України від 11.01.2001 р. № 2210-III URL: http: zakon.rada.gov.ua.
72. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Офіційний сайт Верховної Ради України. URL: http: zakon3.rada.gov.ua/laws/show/80/94-вр.
73. Про захист суспільної моралі: Закон України від 20.11.2003 № 1296-IV. Офіційний сайт Верховної Ради України. URL: http: zakon3.rada.gov.ua/laws/show/1296-15.
74. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні: Указ Президента України від 31.07.2000 № 928/2000. Офіційний сайт Верховної Ради України. URL: http: zakon2.rada.gov.ua/laws/show/928/2000.
75. Про інформацію: Закон України від 02.10.1992 № 2657-XII. Офіційний сайт Верховної Ради України. URL: http: zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12.

76. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 № 75/98-ВР. Офіційний сайт Верховної Ради України. URL: http: zakon0.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80/page.
77. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL: http: zakon.rada.gov.ua/laws/show/2469-19#Text
78. Про Національну раду України з питань телебачення і радіомовлення: закон України, ст. 13 – 14. - № 538/97-вр від 23.09.1997. URL: http: zakon2.rada.gov.ua/laws/show/538/97-вр URL: http: www.niss.gov.ua/articles/1156/ © Національний інститут стратегічних досліджень
79. Про організацію оборонного планування: Закон України від 18.11.2004 № 2198-IV. Офіційний сайт Верховної Ради України. URL: http: zakon3.rada.gov.ua/laws/show/2198-15.
80. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 № 537-V. Офіційний сайт Верховної Ради України. URL: http: zakon3.rada.gov.ua/laws/show/537-16.
81. Про телебачення і радіомовлення: закон України від 21.12.1993 р. № 3760-XII. URL: http: zakon1.rada.gov.ua/laws/show/3759-12
82. Про телекомунікації: Закон України від 18.11.2003 р. *Відомості Верховної Ради*. 2004. № 12. Ст. 155.
83. Про телекомунікації: Закон України від 18.11.2003 р. № 1280-IV URL: http: zakon.rada.gov.ua.
84. Голубєв В.О., Павловський В.Д. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: Навч. посіб.; За заг. ред. Р.А. Калюжного. Запоріжжя: ГУ "ЗІДМУ", 2012. 292 с.
85. Брижко ВЦимбалюк., В., Проблеми інформаційного права та правової інформатики; за ред. М.Я. Швеця і Р.А. Калюжного. К.: НДЦПІ АПрН України, 2014 р. 263 с.
86. Савінова Н.А. Кримінально-правове забезпечення розвитку

інформаційного суспільства в Україні : теоретичні та практичні аспекти: монографія. Київ: ТОВ«ДКС», 2012. 342 с.

87. Самойленко О.А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Х., 2007. 20 с.
88. Самчук З. Ф.Світоглядніосновисоціально-філософського дослідження ідеології: проблема критеріїв та пріоритетів вибору. Т. 1. 2009. 920 с.
89. Бутузов В. М., Гавловський В. Д., Довгань О. Д. Словник термінів з кібербезпеки. К.: ВБ «Аванпост-Прим», 2012. 214с.
90. Соснін О. В. Проблеми державного управління системою національних інформаційних ресурсів з наукового потенціалу України. К.: Ін-т держави і права ім. В. М. Корецького НАН України, 2003. 572 с.
91. Петрик В. М., Кузьменко А. М., Остроухов В. В. Соціально-правові основи інформаційної безпеки. за ред. Остроухова В. В. К.: Росава, 2007. С. 10.
92. Рубан І. А., Семенченко А. І., Троян П. І.Стан та перспективи розвитку інформаційної сфери України: збірник матеріалів з питань становлення інформаційного суспільства в Україні. К. : ТОВ «Пан Тот», 2009. 116 с. (Додаток до наукового журналу «Правова інформатика»).
93. Субіна Т.В. Адміністративно-правове забезпечення інформаційної безпеки в органах державної податкової служби України: дис. ... канд. юрид. наук : 12.00.07. Ірпінь, 2010. 219 с.
94. Тардаскіна Т. М. Менеджмент інформаційної безпеки в галузі зв'язку: навч. посіб. Одеса: ОНАЗ ім. О. С. Попова, 2011. 272 с.
95. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. К. : Держстандарт України, 1997. 15 с.

96. Базилюк Я. Б. Україна у системі міжнародної безпеки. Рада національної безпеки і оборони України, Національний ін-т проблем міжнародної безпеки. К.: Фоліант: Стилос, 2009. 572 с.
97. Ус Р.Л. Аудит інформаційних технологій – новий вид аудиту організацій. Текст Р.Л.Ус. *Формування ринкових відносин в Україні*. 2013. № 1. С. 81-86
98. Хартия Европейского Союза об основных правах (2007/C303/01). Европейский Союз: Основополагающие акты в редакции Лиссабонского договора с комментариями. X, 2010. С. 554-570.
99. Центральний засвідчувальний орган: Головна сторінка. URL: http: www.czo.gov.ua.
100. Шепета О. Адміністративно-правові засади технічного захисту інформації : дис. ... канд. юрид. наук : спец. 12.00.07 «Теорія управління; адміністративне право і процес; фінансове право; інформаційне право»; Нац. академія Служби безпеки України. К., 2011. 215 с.
101. Щодо надання інформації: Державне агентство з питань науки, інновацій та інформатизації України. 02.04.2013 за № 1/06-2-398. URL: http: www.niss.gov.ua/articles/1156
102. Ярочкин В.И. Информационная безопасность: Учеб. для студ. вузов, обуч. по гуманит. и соц.-экон. спец. М.: Фонд «Мир», 2009. 640 с.
103. Communication from the Commission to the Council, the European parliament, the European Economic and Social Committee and the Committee of the Regions «Network and Information Security: Proposal for A European Policy Approach». Brussels, 6.6.2001. COM (2001)298 final. URL: http: www.etsi.org/WebSite/document/aboutETSI/EC_Communications/COM_298.pdf.
104. Report of the Human Rights Committee. URL: http: www.un.org/documents/ga/docs/55/a5540vol2.pdf.

105. Sherr J. Particularities and priorities of the national security strategy of UK.URL: http: assets.publishing.service.gov.uk/media/5a7c68abed915d696ccfc92a/7291.pdf

106. The European Network and Information Security Agency (ENISA). URL: http: www.enisa.europa.eu/

Виконала: студентка магістратури за спеціальністю 281 Публічне управління та адміністрування заочної форми навчання

_____ К.М. Щасневич

Науковий керівник:

Професорка кафедри публічного управління та адміністрування, д.держ.упр., доцентка

_____ І.В. Шевчук

Робота допущена до захисту:

завідувач кафедри публічного управління та адміністрування, д.держ.упр., професор

_____Е.В. Щепанський