ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА ІМЕНІ ЛЕОНІДА ЮЗЬКОВА
ФАКУЛЬТЕТ ПУБЛІЧНОГО УПРАВЛІННЯ

Кафедра: публічного управління та адміністрування

БАКАЛАВРСЬКА РОБОТА

на здобуття освітнього ступеня бакалавра
на тему:

«Інформаційна безпека в системі органів публічного управління в умовах воєнного стану (на матеріалах Хмельницької обласної ради)»

Виконала: студентка магістратури за спеціальністю 281 Публічне управління та адміністрування заочної форми навчання
Рогожа Аріна
(прізвище та ініціали)

Керівник: доктор філософії, доцент кафедри
Вжешнєвська О.М.
(прізвище та ініціали)

Рецензент: _____
(прізвище та ініціали)

Хмельницький – 2026 рік

Анотація

Рогожа А. Інформаційна безпека в системі органів публічного управління в умовах воєнного стану (на матеріалах Хмельницької обласної ради). Кваліфікаційна наукова праця на правах рукопису. Бакалаврська робота на здобуття освітнього ступеня бакалавра за спеціальністю 281 Публічне управління та адміністрування. Хмельницький університет управління та права імені Леоніда Юзькова, Хмельницький, 2026. 99 с.

У бакалаврській роботі досліджено теоретичні та практичні аспекти забезпечення інформаційної безпеки в системі органів публічного управління в умовах воєнного стану. Розкрито сутність інформаційної безпеки, систематизовано основні загрози інформаційній безпеці органів публічного управління та проведено аналіз системи забезпечення інформаційної безпеки Хмельницької обласної ради. Здійснено оцінювання загроз, ризиків і проблем забезпечення інформаційної безпеки в діяльності обласної ради. Обґрунтовано напрями удосконалення організаційно-управлінських механізмів забезпечення інформаційної безпеки, зокрема запропоновано створення координаційної групи з питань інформаційної безпеки та розроблення Комплексної політики інформаційної безпеки. Розроблено рекомендації щодо підвищення стійкості інформаційно-комунікаційної інфраструктури та електронного документообігу Хмельницької обласної ради шляхом впровадження системи забезпечення безперервності діяльності, удосконалення управління ризиками та підвищення цифрової стійкості електронного документообігу.

Ключові слова: інформаційна безпека, органи публічного управління, органи місцевого самоврядування, кібербезпека, управління ризиками, інформаційно-комунікаційна інфраструктура, електронний документообіг, цифрова стійкість, воєнний стан.

Abstract

Rohozha A. Information Security in the System of Public Administration Bodies under Martial Law (Based on the Materials of the Khmelnytskyi Regional Council). Qualification Research Paper Manuscript. Bachelor's Thesis for obtaining the Bachelor's Degree in Specialty 281 Public Administration and Management. Leonid Yuzkov Khmelnytskyi University of Management and Law, Khmelnytskyi, 2026. 99 p.

The bachelor's thesis examines the theoretical and practical aspects of ensuring information security in the system of public administration bodies under martial law. The essence of information security is revealed, the main threats to the information security of public administration bodies are systematized, and the information security system of the Khmelnytskyi Regional Council is analyzed. An assessment of threats, risks, and problems related to information security in the activities of the Regional Council has been carried out. Directions for improving the organizational and managerial mechanisms of information security provision are substantiated, including the establishment of a permanent Information Security Coordination Group and the development of a Comprehensive Information Security Policy. Recommendations have been developed for enhancing the resilience of the

information and communication infrastructure and electronic document management system of the Khmelnytskyi Regional Council through the implementation of a business continuity management system, improvement of information security risk management, and strengthening the digital resilience of electronic document management.

Keywords: information security, public administration bodies, local self-government bodies, cybersecurity, risk management, information and communication infrastructure, electronic document management, digital resilience, martial law.

ЗМІСТ

ВСТУП

Актуальність теми. Сучасний етап розвитку публічного управління характеризується активним впровадженням цифрових технологій, розширенням використання інформаційно-комунікаційних систем та переходом до електронних форм взаємодії між органами влади, громадянами і суб'єктами господарювання. Цифровізація управлінських процесів сприяє підвищенню оперативності прийняття рішень, прозорості діяльності органів публічної влади та доступності адміністративних послуг, водночас зумовлюючи зростання залежності від інформаційних ресурсів та інформаційно-комунікаційної інфраструктури. В умовах воєнного стану питання забезпечення інформаційної безпеки набувають особливої актуальності, оскільки інформаційні системи органів державної влади та органів місцевого самоврядування стають об'єктами постійних кібератак, спроб несанкціонованого доступу до інформації, інформаційно-психологічного впливу та інших загроз. Порушення функціонування інформаційних систем може негативно впливати на безперервність управлінських процесів, ефективність виконання владних повноважень та рівень довіри громадян до органів влади. Особливого значення зазначені виклики набувають для органів місцевого самоврядування, які забезпечують реалізацію значної кількості управлінських функцій, взаємодію з територіальними громадами, органами державної влади та іншими суб'єктами публічного управління. В умовах широкого використання систем електронного документообігу, офіційних вебресурсів, електронної пошти та цифрових сервісів виникає необхідність формування ефективних механізмів захисту інформаційних ресурсів, управління інформаційними ризиками та забезпечення стійкості інформаційно-комунікаційної інфраструктури.

Вагомий внесок у дослідження теоретичних і практичних аспектів інформаційної безпеки, кібербезпеки та управління інформаційними ризиками зробили такі вітчизняні науковці, як Бондар І.Р. , Гурковський В.І., Золотар О.

О., Трубін І. О., Ліпкан В.А., Харченко Л.С., Логінов О.В., Миколюк А. В., Ніколайчук О. В., Шелепало Г. В., Панькова О. В., Харченко С. О. та інші. Питання забезпечення інформаційної безпеки в системі публічного управління, функціонування інформаційно-комунікаційних систем органів влади та формування механізмів протидії сучасним інформаційним загрозам висвітлено також у працях зарубіжних дослідників, зокрема Єнч Н., Міхалец О., Полліні А., Росадо Д. Г. та інших. Водночас, незважаючи на значну кількість наукових досліджень у сфері інформаційної безпеки, окремі питання забезпечення інформаційної безпеки органів місцевого самоврядування в умовах воєнного стану залишаються недостатньо дослідженими. Зокрема, потребують подальшого наукового обґрунтування механізми управління інформаційними ризиками, забезпечення цифрової стійкості інформаційно-комунікаційної інфраструктури, безперервності діяльності та організації захисту інформаційних ресурсів на місцевому рівні.

Зазначене обумовлює актуальність теми дослідження, її теоретичне та практичне значення для вдосконалення механізмів забезпечення інформаційної безпеки в діяльності Хмельницької обласної ради в умовах воєнного стану.

Мета і завдання дослідження. Метою бакалаврської роботи є теоретичне обґрунтування та розробка практичних рекомендацій щодо удосконалення механізмів забезпечення інформаційної безпеки Хмельницької обласної ради в умовах воєнного стану. Для досягнення поставленої мети в роботі були поставлені та вирішені такі завдання:

- визначити сутність інформаційної безпеки в системі органів публічного управління в умовах воєнного стану;
- узагальнити та систематизувати класифікації загроз інформаційній безпеці органів публічного управління в умовах воєнного стану;
- провести аналіз системи забезпечення інформаційної безпеки Хмельницької обласної ради в умовах воєнного стану;
- здійснити оцінювання загроз, ризиків та проблем забезпечення інформаційної безпеки в діяльності Хмельницької обласної ради;

- обґрунтувати напрями удосконалення організаційно-управлінських механізмів забезпечення інформаційної безпеки Хмельницької обласної ради;
- розробити рекомендації щодо підвищення стійкості інформаційно-комунікаційної інфраструктури та електронного документообігу Хмельницької обласної ради.

Об'єкт дослідження – процес забезпечення інформаційної безпеки в системі органів публічного управління в умовах воєнного стану.

Предмет дослідження – теоретичні засади, організаційно-управлінські механізми та практичні інструменти забезпечення інформаційної безпеки Хмельницької обласної ради, спрямовані на підвищення стійкості інформаційно-комунікаційної інфраструктури та електронного документообігу в умовах воєнного стану.

Методи дослідження. Теоретичною та методологічною основою дослідження стали наукові праці вітчизняних і зарубіжних учених з питань інформаційної безпеки, кібербезпеки, публічного управління та цифрової трансформації органів влади, а також нормативно-правові акти України, що регулюють сферу інформаційної безпеки.

У процесі дослідження використано комплекс загальнонаукових і спеціальних методів. Метод аналізу та синтезу застосовано для розкриття сутності інформаційної безпеки в системі органів публічного управління та узагальнення наукових підходів до її забезпечення. Метод класифікації використано для систематизації загроз інформаційній безпеці органів публічного управління в умовах воєнного стану. Системний підхід дав змогу розглядати інформаційну безпеку як складову системи публічного управління та дослідити взаємозв'язки між її елементами. Метод порівняльного аналізу застосовано для вивчення нормативно-правового забезпечення та сучасних підходів до управління інформаційною безпекою. Методи оцінювання та узагальнення використано під час аналізу системи забезпечення інформаційної безпеки Хмельницької обласної ради, ідентифікації ризиків і проблем її функціонування. Табличний та графічний методи застосовано для наочного

представлення результатів дослідження. На основі методу моделювання розроблено практичні рекомендації щодо удосконалення організаційно-управлінських механізмів забезпечення інформаційної безпеки, підвищення стійкості інформаційно-комунікаційної інфраструктури та електронного документообігу Хмельницької обласної ради.

Інформаційну базу дослідження становлять Конституція України, закони України, нормативно-правові акти Президента України, Кабінету Міністрів України, Державної служби спеціального зв'язку та захисту інформації України, Стратегія кібербезпеки України, державні стандарти та нормативні документи у сфері технічного захисту інформації, офіційні матеріали Хмельницької обласної ради, статистичні та аналітичні матеріали державних органів, наукові праці вітчизняних і зарубіжних учених з питань інформаційної безпеки, кібербезпеки та публічного управління, а також інформаційні ресурси мережі Інтернет.

Практичне значення одержаних результатів. Практичне значення одержаних результатів полягає у можливості використання розроблених рекомендацій для вдосконалення системи забезпечення інформаційної безпеки Хмельницької обласної ради та інших органів місцевого самоврядування в умовах воєнного стану. Запропоновані заходи щодо створення постійно діючої координаційної групи з питань інформаційної безпеки, розроблення Комплексної політики інформаційної безпеки, впровадження системи управління ризиками інформаційної безпеки, забезпечення безперервності діяльності та підвищення цифрової стійкості електронного документообігу можуть бути використані під час удосконалення внутрішніх процедур управління інформаційними ресурсами та організації захисту інформації в діяльності органів публічного управління. Окремі положення та результати дослідження можуть застосовуватися у навчальному процесі закладів вищої освіти під час викладання дисциплін, пов'язаних із публічним управлінням, інформаційною безпекою та цифровою трансформацією.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ ОРГАНІВ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ВОЄННОГО СТАНУ

1.1. Сутність інформаційної безпеки в системі органів публічного управління умовах воєнного стану

В умовах воєнного стану інформаційна безпека органів публічного управління набуває особливого значення, оскільки саме через інформаційні ресурси, цифрові платформи, державні реєстри та комунікаційні канали забезпечується безперервність управлінських процесів. Повномасштабна війна суттєво посилила залежність органів влади від захищеності інформаційно-комунікаційної інфраструктури, адже будь-яке порушення її функціонування може негативно вплинути на прийняття управлінських рішень, координацію дій між суб’єктами влади та надання публічних послуг. Інформаційний простір у період воєнного стану стає не лише середовищем обміну даними, а й полем цілеспрямованого впливу, у межах якого здійснюються дезінформаційні кампанії, кібератаки, психологічні операції та спроби дестабілізації суспільної довіри до державних інституцій. За таких умов інформаційна безпека органів публічного управління має розглядатися як комплексна управлінська категорія, що охоплює захист інформації, забезпечення стійкості цифрових систем, організацію безпечної комунікації та формування культури відповідального поводження з даними. Особливого значення набуває захист службової, персональної, стратегічної та критично важливої інформації, витік або спотворення якої може створити ризики для обороноздатності держави, громадської безпеки та стабільності публічного управління. Водночас воєнний стан виявляє наявні інституційні проблеми у сфері інформаційної безпеки, зокрема фрагментарність міжвідомчої взаємодії, нерівномірний рівень цифрової захищеності органів влади, недостатню підготовленість персоналу та

обмеженість ресурсів для швидкого реагування на інформаційні інциденти. Система органів публічного управління в таких умовах потребує не лише технічних засобів кіберзахисту, а й чітко визначених процедур управління ризиками, алгоритмів реагування, механізмів моніторингу загроз і відповідальності посадових осіб за дотримання вимог інформаційної безпеки. Важливим завданням є також забезпечення балансу між захистом державних інформаційних ресурсів і дотриманням прав громадян на доступ до достовірної, своєчасної та суспільно значущої інформації. Недостатній рівень інформаційної безпеки може призводити до порушення функціональної спроможності органів влади, зниження ефективності управлінських рішень, поширення панічних настроїв, втрати довіри до офіційних джерел інформації та послаблення стійкості держави перед гібридними загрозами. Саме тому дослідження сутності інформаційної безпеки в системі органів публічного управління в умовах воєнного стану є необхідною передумовою для формування цілісного наукового підходу до захисту інформаційного простору, підвищення інституційної спроможності влади та забезпечення стабільного функціонування держави в кризових умовах.

Дослідження сутності інформаційної безпеки в системі органів публічного управління в умовах воєнного стану потребує звернення не лише до сучасних нормативно-правових і управлінських підходів, а й до історико-філософських витоків осмислення інформації як чинника влади, управління, впливу та безпеки. Ще в давніх воєнно-стратегічних концепціях інформація розглядалася як ресурс, що здатний забезпечити перевагу над противником не лише у відкритому зіткненні, а й на етапі підготовки, прогнозування та прийняття рішень. У цьому контексті особливе значення має спадщина китайського мислителя і військового стратега Сунь-Цзи, який у праці «Мистецтво війни» наголошував на важливості попереднього знання про наміри, стан і можливості противника. Його ідея полягала в тому, що перемога значною мірою досягається не фізичним знищенням ворога, а завдяки володінню випереджувальною інформацією, здатності ввести противника в

оману, послабити його волю до опору, дезорганізувати та виснажити ще до початку безпосередньої атаки [41, с. 90]. Для сучасного публічного управління в умовах війни цей підхід є важливим, оскільки підтверджує, що інформаційна перевага, своєчасність даних, захищеність каналів комунікації та спроможність протидіяти дезінформації є не допоміжними, а системоутворюючими елементами державної стійкості.

Подальший розвиток уявлень про безпеку пов'язаний із гуманістичною традицією епохи Відродження, у межах якої в центрі науково-філософської уваги опинилася людина, її духовна свобода, соціальна захищеність і можливість гармонійного розвитку. Саме в цей період поступово формується розуміння того, що безпека не може зводитися лише до фізичного захисту, оскільки вона охоплює також сферу свідомості, переконань, інформаційного впливу та соціальної справедливості. Гуманістична думка, осмислюючи війну як одну з найбільших загроз для людини й суспільства, поставила питання про необхідність таких умов суспільного розвитку, за яких насильство, примус і руйнування не визначали б логіку державного життя. У сучасних умовах воєнного стану ця ідея набуває нового значення, адже органи публічного управління мають забезпечувати не лише оборонну та адміністративну спроможність держави, а й захист інформаційного простору, суспільної свідомості, довіри громадян до офіційних джерел інформації та легітимності управлінських рішень.

У політико-управлінській площині особливе місце посідають ідеї Нікколо Макіавеллі, який фактично одним із перших показав значення інформаційно-психологічного впливу у процесі здійснення державної влади. Його підходи дають змогу простежити раннє розуміння того, що влада спирається не лише на силу, право чи інститути, а й на здатність формувати уявлення, переконання, страхи, очікування та поведінкові моделі підлеглих і супротивників. У подальшій історії державного управління неодноразово спостерігалися масштабні інформаційно-пропагандистські кампанії, маніпулятивні технології та практики масової дезінформації, які впливали на суспільну стабільність,

політичні процеси та хід воєнних конфліктів. Для органів публічного управління в умовах воєнного стану це означає, що інформаційна безпека повинна охоплювати не лише захист технічних систем, а й протидію інформаційно-психологічним операціям, маніпуляціям, ворожій пропаганді та спробам руйнування суспільної єдності.

Важливим етапом у становленні безпекової думки стали спроби правового впорядкування міждержавних відносин, що особливо виразно проявилися у працях Гуго Гроція. Його трактат «Про право війни і миру» заклав підґрунтя для розуміння того, що навіть у період збройного протистояння дії держав мають бути обмежені правом, а війна не може бути простором абсолютної сваволі [41]. Ідеї про необхідність дотримання міжнародних зобов'язань, захисту мирного населення, недопущення надмірної жорстокості та обмеження руйнівних наслідків воєнних дій мають безпосередній зв'язок із сучасним розумінням інформаційної безпеки. В умовах воєнного стану органи публічного управління повинні діяти в межах права, забезпечуючи баланс між захистом державних інтересів, режимом обмеженого доступу до окремих відомостей і правом громадян на достовірну, своєчасну та суспільно необхідну інформацію.

У сучасному науковому розумінні проблема безпеки особистості, суспільства й держави була суттєво поглиблена у філософських концепціях Томаса Гоббса та Іммануїла Канта. Виходячи з уявлення про небезпеки природного стану, вони обґрунтовували необхідність створення такого громадянського устрою, який здатний гарантувати захищеність людини та впорядкованість суспільного життя. У цьому контексті держава постає як інституційний механізм забезпечення безпеки, а публічне управління — як система організованого впливу, спрямованого на підтримання порядку, стабільності й передбачуваності суспільних процесів. Для умов воєнного стану це має особливе значення, оскільки саме органи публічного управління повинні гарантувати безперервність державних функцій, координацію дій суб'єктів

сектору безпеки й оборони, захист критично важливих інформаційних ресурсів та недопущення управлінського хаосу внаслідок інформаційних атак.

Філософські підходи Джона Локка, Вольтера, Дені Дідро, Жан-Жака Руссо, Йоганна Фіхте та Йоганна Гердера також поглибили розуміння безпеки як умови існування правового, політично організованого та морально відповідального суспільства. У їхніх працях безпека пов'язувалася з ідеями свободи, миру, суверенітету, прав людини, справедливості та відповідальності держави перед суспільством. У сучасній системі публічного управління ці положення набувають нового змісту, оскільки інформаційна безпека має забезпечувати не лише захищеність державних інформаційних ресурсів, а й збереження довіри до органів влади, правомірність використання даних, прозорість комунікації та недопущення зловживань інформаційною владою. Отже, сутність інформаційної безпеки в органах публічного управління не може бути зведена до технічного захисту інформації, оскільки вона безпосередньо пов'язана з демократичними принципами, правами громадян і легітимністю управлінських рішень.

Окремої уваги заслуговують ідеї Анрі Бергсона, який розглядав проблеми безпеки крізь призму протиставлення відкритих і закритих суспільств. На його думку, насильство, ізоляція, конфліктність і війна значною мірою є наслідками закритості суспільних систем, які втрачають здатність до морального оновлення, солідарності та взаємного розуміння. Подолання таких проявів він пов'язував із духовним спрощенням, відмовою від надмірно штучних потреб і пошуком більш гармонійних форм людського співіснування [41, с. 93]. У контексті інформаційної безпеки органів публічного управління ця позиція може бути інтерпретована як необхідність запобігання інформаційній ізоляції, закритості владних комунікацій, монополізації інформаційних потоків та втрати зворотного зв'язку між державою і суспільством. Навіть в умовах воєнного стану, коли частина інформації об'єктивно потребує захисту, публічна влада має зберігати здатність до відкритої, відповідальної й достовірної комунікації з громадянами.

У науковому дискурсі особливе місце посідає поняття «інформаційна війна», яке безпосередньо пов’язане з проблематикою інформаційної безпеки держави та органів публічного управління. Одним із перших цей термін використав Томас Рона у доповіді «Системи озброєння та інформаційної війни», підготовленій у 1976 р. для компанії «Боїнг». У ній було обґрунтовано, що інформаційна інфраструктура, перетворюючись на ключовий елемент економічного й оборонного потенціалу держави, стає вразливою ціллю як у воєнний, так і в мирний час. Надалі термін «інформаційна війна» увійшов в офіційний обіг у США після прийняття відповідної директиви Міністерства оборони у 1992 р., а практичне використання новітніх інформаційних технологій під час війни в Перській затоці засвідчило зміну характеру сучасних воєн. Відтоді інформаційний простір почав розглядатися як самостійна сфера протиборства, у якій стратегічного значення набувають дані, комунікації, технології, психологічний вплив і контроль над інформаційними потоками.

Для України проблема інформаційної безпеки набула особливої гостроти в умовах протидії гібридній, а згодом і повномасштабній збройній агресії російської федерації. Воєнний стан виявив, що захист державного суверенітету, територіальної цілісності, демократичного ладу, прав людини, суспільної єдності та функціональної спроможності сектору безпеки й оборони неможливий без належного захисту інформаційного простору. Йдеться не лише про технологічне посилення інформаційного обміну, модернізацію цифрової інфраструктури чи впровадження засобів кіберзахисту, а й про усвідомлення всіма суб’єктами інформаційних відносин необхідності системного захисту інформаційних ресурсів, державних реєстрів, службової інформації, персональних даних, офіційних каналів комунікації та управлінських процесів [17, с. 46]. Саме тому органи публічного управління в умовах воєнного стану повинні виступати не лише користувачами інформації, а й активними суб’єктами її захисту, верифікації, поширення, збереження та стратегічного використання.

Попри значну кількість наукових підходів до тлумачення інформаційної безпеки, у сучасній доктрині відсутнє єдине й остаточно усталене розуміння її сутності. В. Ліпкан, систематизуючи наявні підходи, звертає увагу на багатовимірність цього феномену. Інформаційна безпека може розглядатися як стан захищеності інформаційного простору, як процес протидії загрозам і небезпекам, як умова забезпечення інформаційного суверенітету України, як захищеність національних інтересів в інформаційній сфері, як дотримання законодавчо визначених правил інформаційної діяльності, як функція держави, як система суспільних відносин щодо захисту найважливіших інтересів людини, суспільства й держави, а також як складова політичної, економічної, оборонної та інших елементів національної безпеки [17, с. 25–30]. Така багатозначність свідчить про те, що інформаційна безпека в системі органів публічного управління має комплексний характер і не може бути пояснена лише через одну ознаку або один управлінський інструмент.

О. Данильян, О. Дзьобан та М. Панов визначають інформаційну безпеку через захищеність об’єкта від інформаційних загроз або негативних впливів, пов’язаних з інформацією, а також через необхідність збереження в таємниці відомостей, які мають особливий правовий режим, зокрема становлять державну таємницю [7, с. 165]. Такий підхід є важливим для органів публічного управління в умовах воєнного стану, оскільки значна частина управлінської інформації безпосередньо пов’язана з оборонними, мобілізаційними, безпековими, інфраструктурними та гуманітарними процесами. Її розголошення, спотворення або використання ворожими суб’єктами може спричинити не лише адміністративні чи репутаційні наслідки, а й реальні загрози життю людей, безпеці громад, функціонуванню критичної інфраструктури та обороноздатності держави.

В. Гурковський пропонує розглядати інформаційну безпеку як систему суспільних відносин, спрямованих на захист життєво важливих інтересів людини і громадянина, суспільства та держави від реальних і потенційних загроз в інформаційному просторі. Водночас дослідник підкреслює, що така

безпека є необхідною умовою збереження й розвитку духовних і матеріальних цінностей державотворчої нації, самозбереження та прогресивного розвитку України як суверенної держави [6, с. 74]. У площині публічного управління це дає підстави розглядати інформаційну безпеку не лише як інструмент захисту даних, а як один із чинників національної консолідації, державної суб'єктності та здатності влади діяти в інтересах суспільства в умовах воєнної небезпеки.

О. Баранов, використовуючи категорію національних інтересів, визначає інформаційну безпеку як стан їх захищеності в інформаційному середовищі, за якого унеможливлюється або мінімізується завдання шкоди особі, суспільству й державі через неповноту, несвоєчасність, недостовірність інформації, несанкціоноване поширення чи використання даних, негативний інформаційний вплив і небажані наслідки функціонування інформаційних технологій [2, с. 60–62]. Близьку позицію висловлюють В. Шатун та О. Гладун, які також пов'язують інформаційну безпеку із захищеністю національних інтересів України в інформаційній сфері від загроз, що виникають унаслідок недостовірності, несвоєчасності або неповноти інформації, неправомірного її поширення, негативного інформаційного впливу та ризиків, породжених інформаційними технологіями [44, с. 175]. Для органів публічного управління ці підходи є особливо значущими, оскільки в умовах воєнного стану управлінське рішення прямо залежить від повноти, достовірності, оперативності й захищеності інформації.

У працях В. Шатуна та О. Гладун інформаційна безпека також розглядається як процес управління загрозами та небезпеками, що здійснюється державними й недержавними інституціями, а також окремими громадянами з метою забезпечення інформаційного суверенітету України [44, с. 175]. Такий підхід дає змогу перенести акцент із пасивного розуміння безпеки як певного стану на її динамічний, процесний характер. У системі органів публічного управління це означає необхідність постійного моніторингу інформаційних ризиків, прогнозування загроз, координації міжвідомчої взаємодії, реагування

на інформаційні інциденти, відновлення порушених інформаційних процесів і формування стійкої управлінської культури поводження з інформацією.

І. Бондар, розглядаючи інформаційну безпеку через функціонування системи засобів захисту інформаційних систем, акцентує увагу на впорядкованій сукупності інформаційних ресурсів, інформаційних технологій і програмно-технічних засобів, що забезпечують реалізацію інформаційних процесів у людино-машинному або автоматизованому режимі. Метою створення і функціонування такої системи є забезпечення прав людини, інтересів суспільства та держави в інформаційній сфері [3, с. 72]. Для органів публічного управління в умовах воєнного стану це визначення є цінним, оскільки воно дозволяє пов’язати інформаційну безпеку з практичним функціонуванням державних реєстрів, електронних сервісів, систем документообігу, цифрових платформ, каналів службової комунікації та технологічної інфраструктури публічної влади.

Нормативне розуміння інформаційної безпеки в Україні характеризується тим, що чинне законодавство не завжди містить її вичерпне й універсальне визначення, проте послідовно розглядає цю категорію у взаємозв’язку з національною безпекою. Такий підхід є обґрунтованим, оскільки в умовах інформатизації суспільства достовірні, своєчасні й захищені дані про економічні, політичні, соціальні, воєнно-стратегічні, науково-освітні, культурні та екологічні процеси визначають спроможність держави ухвалювати ефективні управлінські рішення. Інформація та інформаційні комунікації дедалі більше перетворюються на чинники, від яких залежить стійкість суспільства, функціональність державних інститутів і здатність публічної влади діяти в кризових умовах. Чим інтенсивніше розвивається інформаційна сфера як системоутворюючий елемент суспільного життя, тим більшою стає залежність політичної, економічної, оборонної, соціальної та інших складових національної безпеки від стану інформаційної безпеки [27, с. 45].

Отже, інформаційна безпека в системі органів публічного управління в умовах воєнного стану є не лише складовою національної безпеки, а й умовою

забезпечення безперервності державного управління, захисту національних інтересів, підтримання суспільної довіри та збереження інформаційного суверенітету України. Вона охоплює особистісний, суспільний, комерційний і державний виміри, оскільки всі суб'єкти інформаційного суспільства залучені до процесів створення, обміну, використання, зберігання та захисту інформації. У цьому сенсі інформаційна безпека органів публічного управління може бути визначена як комплексний стан і водночас управлінський процес, спрямований на захист інформаційних ресурсів, цифрової інфраструктури, службової та персональної інформації, офіційних комунікацій і управлінських рішень від реальних і потенційних загроз, які в умовах воєнного стану можуть порушити стабільність функціонування держави, її обороноздатність, правопорядок, суспільну єдність і довіру громадян до публічної влади.

Інформаційну безпеку в системі органів публічного управління в умовах воєнного стану доцільно визначати як комплексний стан захищеності та водночас динамічний управлінський процес, спрямований на забезпечення цілісності, достовірності, конфіденційності, доступності й безперервності функціонування інформаційних ресурсів, цифрової інфраструктури, офіційних комунікацій, управлінських даних і рішень органів влади від реальних і потенційних загроз, які можуть порушити стабільність державного управління, обороноздатність, суспільну довіру, правопорядок і національну стійкість. У такому розумінні інформаційна безпека не обмежується технічним захистом інформації або кіберзахистом інформаційно-комунікаційних систем, а охоплює ширший комплекс правових, організаційних, інституційних, кадрових, технологічних, комунікаційних і аналітичних заходів, що забезпечують спроможність публічної влади діяти ефективно, правомірно та безперервно в умовах підвищеної загрозової динаміки.

Особливість інформаційної безпеки органів публічного управління в умовах воєнного стану полягає в тому, що вона формується в середовищі постійної загрози не лише кібернетичного, а й інформаційно-психологічного, політичного, організаційного та управлінського характеру. За таких умов

інформація перетворюється на стратегічний ресурс держави, а її втрата, спотворення, несвоєчасне надходження або несанкціоноване поширення може мати наслідки не лише для окремого органу влади, а й для функціонування всієї системи публічного управління. Воєнний стан посилює значення оперативності управлінських рішень, достовірності офіційних повідомлень, захищеності державних реєстрів, безпеки міжвідомчого обміну даними, збереження службової та персональної інформації, а також стійкості каналів комунікації між державою, громадянами, територіальними громадами, військовими структурами та міжнародними партнерами.

Однією з ключових особливостей інформаційної безпеки в досліджуваній сфері є її міжсекторальний характер, оскільки вона поєднує інтереси національної безпеки, оборони, цифрового розвитку, адміністративного управління, захисту персональних даних, публічних комунікацій і забезпечення прав громадян. Вона не може бути реалізована лише силами одного органу або одного структурного підрозділу, оскільки потребує скоординованої взаємодії центральних органів виконавчої влади, органів місцевого самоврядування, військових адміністрацій, суб’єктів сектору безпеки й оборони, спеціалізованих органів кіберзахисту, розпорядників державних реєстрів та посадових осіб, відповідальних за інформаційні процеси. Саме тому інформаційна безпека в умовах воєнного стану має розглядатися як спільна управлінська відповідальність, що передбачає чіткий розподіл повноважень, встановлення процедур реагування, регулярний моніторинг ризиків, контроль за дотриманням режимів доступу до інформації та формування культури інформаційної дисципліни в органах влади.

Важливою характеристикою інформаційної безпеки органів публічного управління є її превентивна спрямованість. Вона передбачає не лише реагування на вже реалізовані загрози, а й завчасне виявлення вразливостей, прогнозування можливих інформаційних інцидентів, оцінювання ризиків, підготовку персоналу, резервування критичних даних, захист каналів комунікації та створення механізмів швидкого відновлення управлінських

функцій. У період воєнного стану превентивність набуває особливого значення, оскільки часовий проміжок між виникненням загрози та її негативними наслідками може бути мінімальним, а затримка в реагуванні здатна спричинити дезорганізацію управлінських процесів, поширення недостовірної інформації або втрату контролю над важливими інформаційними ресурсами.

Ще однією суттєвою ознакою є поєднання відкритості й обмеженості інформаційних процесів. З одного боку, органи публічного управління зобов'язані забезпечувати громадянам доступ до достовірної, своєчасної та суспільно значущої інформації, підтримувати офіційну комунікацію, пояснювати управлінські рішення та протидіяти дезінформації. З іншого боку, в умовах воєнного стану значна частина інформації потребує спеціального режиму захисту, оскільки її розголошення може завдати шкоди обороноздатності, безпеці громадян, функціонуванню критичної інфраструктури або проведенню управлінських і військово-організаційних заходів. Тому інформаційна безпека передбачає постійне дотримання балансу між принципом публічності влади та необхідністю обмеження доступу до інформації, яка має стратегічне, службове або безпекове значення.

Загальні характеристики інформаційної безпеки в системі органів публічного управління в умовах воєнного стану проявляються у її системності, безперервності, адаптивності, ризик-орієнтованості, нормативній визначеності та практичній спрямованості. Системність означає, що інформаційна безпека охоплює всі рівні публічного управління — від центральних органів влади до місцевого рівня — і стосується всіх етапів роботи з інформацією: її створення, збирання, оброблення, зберігання, передачі, використання, оприлюднення та архівування. Безперервність полягає в тому, що захист інформаційних процесів не може здійснюватися епізодично, а має бути постійною функцією управління, інтегрованою в щоденну діяльність органів влади. Адаптивність передбачає здатність системи інформаційної безпеки швидко реагувати на зміну характеру загроз, оновлення технологій, трансформацію воєнної ситуації та появу нових способів інформаційного впливу. Ризик-орієнтованість виявляється у

необхідності визначення найбільш уразливих інформаційних ресурсів і процесів, оцінювання ймовірності загроз та встановлення пріоритетів захисту залежно від можливих наслідків для держави й суспільства.

Нормативна визначеність інформаційної безпеки означає, що її забезпечення має здійснюватися на основі законодавчо встановлених правил, процедур, режимів доступу, вимог до захисту інформації та відповідальності за їх порушення. Водночас практична спрямованість цієї категорії полягає в тому, що вона повинна мати не декларативний, а прикладний характер, тобто втілюватися у конкретних управлінських рішеннях, інструкціях, алгоритмах реагування, цифрових інструментах, навчанні персоналу, міжвідомчих протоколах і механізмах контролю. У цьому контексті інформаційна безпека виступає не лише умовою захисту інформаційних ресурсів, а й чинником ефективності публічного управління, оскільки від якості інформації, захищеності каналів її передання та довіри до офіційних джерел безпосередньо залежить здатність органів влади виконувати свої функції.

Отже, інформаційна безпека в системі органів публічного управління в умовах воєнного стану є складною багатоаспектною категорією, що поєднує стан захищеності, управлінський процес, інституційну спроможність і стратегічну функцію держави. Її зміст розкривається через забезпечення захисту інформаційних ресурсів, стійкості цифрової інфраструктури, достовірності офіційної інформації, безпеки комунікацій, правомірного використання даних, протидії інформаційно-психологічним впливам і збереження довіри громадян до органів влади. В умовах воєнного стану така безпека набуває особливого значення, оскільки від неї залежить не лише ефективність адміністративної діяльності, а й здатність держави зберігати керованість, обороноздатність, суспільну єдність і національний суверенітет.

1.2. Класифікації загроз інформаційній безпеці органів публічного управління умовах воєнного стану

Сучасне безпекове середовище характеризується поєднанням кібератак, дезінформаційних кампаній, інформаційно-психологічних операцій, несанкціонованого доступу до державних інформаційних ресурсів, витоку персональних даних і спроб дестабілізації офіційних комунікацій. Для органів публічної влади такі загрози є небезпечними не лише через можливі технічні порушення функціонування інформаційних систем, а й через їхній вплив на якість управлінських рішень, довіру громадян, міжвідомчу координацію та здатність держави оперативно реагувати на кризові ситуації. Наукове осмислення класифікації загроз дозволяє перейти від фрагментарного реагування на окремі інформаційні інциденти до формування цілісної системи їх попередження, виявлення, оцінювання, нейтралізації та подальшого відновлення порушених інформаційних процесів. Саме тому дослідження класифікаційних ознак загроз інформаційній безпеці органів публічного управління в умовах воєнного стану є необхідною передумовою для розроблення ефективних управлінських механізмів захисту інформаційних ресурсів, забезпечення стійкості публічної влади та збереження інформаційного суверенітету держави.

Аналіз вітчизняних наукових праць свідчить, що проблема класифікації загроз інформаційній безпеці розглядається українськими дослідниками як необхідна передумова формування дієвої системи моніторингу, попередження, нейтралізації та управління ризиками в інформаційній сфері. О. О. Золотар та І. О. Трубін у статті «Класифікація загроз інформаційній безпеці» зазначають, що наукове осмислення класифікаційних підходів має не лише теоретичне, а й прикладне значення, оскільки дає змогу удосконалити нормативно-правову базу та сформувати більш ефективну систему управління інформаційною безпекою [10]. Автори звертають увагу на те, що різноманітність наявних класифікацій зумовлена відмінністю критеріїв, цілями систематизації та недостатнім теоретичним обґрунтуванням самої сутності загроз інформаційній

безпеці. У цьому контексті вони аналізують підхід В. А. Ліпкана, який пропонує класифікувати загрози за джерелами походження, ступенем можливої шкоди, повторюваністю, сферою походження, імовірністю реалізації, рівнем детермінізму, значенням, структурою впливу, характером реалізації, ставленням до них та об'єктом впливу, тобто щодо особи, суспільства і держави [17]. Такий підхід має комплексний характер, оскільки дозволяє розглядати загрози не лише як технічні або кібернетичні явища, а як багатовимірні процеси, що можуть мати природне, техногенне, антропогенне, внутрішнє або зовнішнє походження та різний рівень впливу на функціонування держави й суспільства.

У межах техніко-правового підходу значного поширення набула класифікація загроз за базовими властивостями інформації. О. О. Золотар та І. О. Трубін, аналізуючи нормативні й наукові джерела, вказують на поділ загроз на загрози витоку інформації, порушення її цілісності та блокування доступу до інформації [10]. Близький підхід простежується у працях Б. Кузьменка та О. Чайковської, які пропонують класифікувати загрози за ознакою порушення конфіденційності, цілісності та доступності інформації [16]. Така класифікація є особливо важливою для органів публічного управління, оскільки їхня діяльність безпосередньо залежить від збереження службової, персональної, управлінської та стратегічної інформації, а в умовах воєнного стану будь-яке порушення доступності державних інформаційних ресурсів або спотворення управлінських даних може спричинити дезорганізацію адміністративних процесів. Водночас обмеженість цього підходу полягає в тому, що він переважно зосереджується на інформації як об'єкті технічного захисту і не повною мірою враховує інформаційно-психологічні, комунікаційні, управлінські та соціальні виміри загроз.

С. О. Харченко, досліджуючи наукові підходи до класифікації загроз інформаційній безпеці органів Служби безпеки України, підкреслює необхідність визначення не лише джерел походження загроз, а й причин їх виникнення, способів впливу, ступеня контрольованості та передбачуваності [42]. У запропонованому автором узагальненні виокремлюються загрози за

джерелами виникнення, зокрема антропогенні, техногенні та стихійні, а також за способом впливу на інформацію — через технічні канали, канали спеціального впливу та несанкціонований доступ. Окремо виділяються загрози за способом викривлення інформації, до яких належать витік, порушення цілісності, спотворення та блокування інформації; за ступенем умисності — умисні й ненавмисні; за інтенсивністю — активні та пасивні; за контрольованістю — контрольовані, неконтрольовані й частково контрольовані. Значущість цієї класифікації для дослідження інформаційної безпеки органів публічного управління полягає в тому, що вона дозволяє перейти від загального переліку загроз до їх управлінської оцінки за параметрами походження, механізму реалізації та можливості контролю.

У дослідженнях С. Гуцу та О. Литвиненка, узагальнених у працях О. О. Золотар, І. О. Трубіна [10] та С. О. Харченка [42], загрози інформаційній безпеці пропонується розглядати ширше, ніж лише через технічне порушення інформаційних ресурсів. Автори виділяють загрози впливу неякісної інформації, зокрема недостовірної, фальшивої або дезінформаційної, на особистість, суспільство й державу; загрози несанкціонованого та неправомірного впливу сторонніх осіб на інформацію й інформаційні ресурси; а також загрози інформаційним правам і свободам особи. Такий підхід є особливо продуктивним для аналізу воєнного стану, оскільки інформаційна небезпека в цей період проявляється не лише у зламі інформаційних систем або витоку даних, а й у поширенні неправдивої інформації, маніпулятивному впливі на громадську думку, дискредитації органів влади, формуванні панічних настроїв і підриві суспільної довіри. Саме тому для органів публічного управління важливо враховувати не тільки технологічні, а й когнітивні, психологічні та комунікаційні загрози.

Окремий напрям становлять дослідження, у яких загрози інформаційній безпеці розглядаються в контексті публічного управління, цифровізації та інформаційної війни. Я. І. Чмир у статті «Проблеми забезпечення інформаційної безпеки в системі публічного управління» визначає

інформаційну безпеку публічного управління як складову національної безпеки, що забезпечує захист системи управління від інформаційно-комунікаційних загроз і викликів [43]. Автор наголошує, що інформація може бути не лише ресурсом розвитку, а й засобом впливу на світогляд людини, населення, ставлення до держави та суспільних процесів. Серед проблем, що посилюють вразливість системи публічного управління, Я. І. Чмир називає відсутність усталеного поняття інформаційної безпеки, недостатню дієвість електронного врядування, появу інноваційних інформаційних небезпек, кадрові проблеми, брак ефективних механізмів захисту та відсутність інституцій, здатних комплексно забезпечувати інформаційну безпеку в публічному управлінні. Такий підхід є важливим, оскільки класифікація загроз доповнюється управлінським виміром: загрози розглядаються не лише як зовнішні деструктивні впливи, а й як наслідок внутрішньої інституційної слабкості системи публічного управління.

А. В. Миколюк акцентує увагу на тому, що активне переведення публічного управління в цифровий вимір, з одного боку, розширює можливості держави, а з іншого — формує нові вразливості, пов’язані з відкритістю даних, цифровими сервісами, електронною взаємодією та залежністю органів влади від інформаційної інфраструктури [18]. Дослідниця звертає увагу на внутрішню суперечність між демократичною відкритістю інформації та потребою захисту критично важливих відомостей, що особливо загострюється в умовах серйозних загроз національній безпеці. Для класифікації загроз це означає необхідність окремого виокремлення загроз, пов’язаних із надмірною відкритістю чутливої інформації, порушенням режиму доступу, неконтрольованим поширенням даних, а також із недостатньою керованістю інформаційних потоків у кризових умовах. У площині воєнного стану такий підхід дозволяє обґрунтувати поділ загроз на ті, що виникають унаслідок зовнішньої агресії, і ті, що породжуються внутрішніми управлінськими дисбалансами між прозорістю, безпекою та режимом обмеженого доступу.

Г. Кириченко розглядає загрози інформаційній безпеці крізь призму сучасної цифровізації, кіберзлочинності, інформаційних війн, дезінформації, маніпулятивного впливу на громадську свідомість і вразливості критичної інформаційної інфраструктури [12]. Автор підкреслює, що ефективне публічне управління в цій сфері потребує координації між інституціями, розвитку інноваційних управлінських підходів, підвищення цифрової грамотності населення та гармонізації національного законодавства з міжнародними стандартами. У межах цього підходу загрози можна групувати за функціональними компонентами інформаційної безпеки: технологічні, пов'язані з кіберзахистом інформаційно-комунікаційних систем і критичної інфраструктури; соціально-комунікаційні, пов'язані з маніпуляціями, дезінформацією та низькою медіаграмотністю; інституційні, пов'язані з недостатньою координацією суб'єктів управління; міжнародні, зумовлені транснаціональним характером інформаційних впливів. Така класифікаційна логіка є найбільш наближеною до сучасних умов воєнного стану, оскільки поєднує кібернетичний, управлінський, комунікаційний і геополітичний аспекти інформаційної безпеки.

М. О. Шевчук, досліджуючи генезу поняття інформаційної безпеки як складової національної безпеки, звертає увагу на те, що чинне законодавство України не містить вичерпного універсального визначення інформаційної безпеки, однак послідовно розглядає її у зв'язку з національною безпекою [45]. Автор пропонує розуміти інформаційну безпеку як стан, за якого в умовах реальних і потенційних загроз забезпечуються самозбереження, сталий розвиток інформаційної сфери, захищеність інформаційної інфраструктури, інформаційного простору, ресурсів, процесів і суб'єктів, а також реалізація національних інтересів. Водночас інформаційна безпека трактується не лише як стан, а й як постійний процес діяльності компетентних органів щодо попередження та протидії загрозам в інформаційній сфері. З огляду на це класифікація загроз має враховувати не лише об'єкти впливу, а й функціональні

завдання органів влади: попередження, виявлення, протидію, локалізацію, відновлення та забезпечення довготривалої стійкості інформаційної сфери.

Узагальнення вітчизняних наукових підходів дає підстави стверджувати, що класифікації загроз інформаційній безпеці можна об’єднати в кілька основних груп. Перша група охоплює загрози за джерелом походження, серед яких виділяються природні, техногенні, антропогенні, внутрішні та зовнішні загрози. Друга група ґрунтується на властивостях інформації та включає загрози конфіденційності, цілісності, доступності, достовірності й своєчасності інформації. Третя група пов’язана зі способом реалізації загроз і охоплює несанкціонований доступ, технічні канали витоку, спеціальний інформаційний вплив, блокування, спотворення, фальсифікацію, дезінформацію та маніпулятивні комунікації. Четверта група відображає характер впливу на суб’єктів інформаційної безпеки — особу, суспільство, державу, органи публічного управління, критичну інформаційну інфраструктуру та інформаційні права громадян. П’ята група має управлінський характер і охоплює загрози, зумовлені інституційною неузгодженістю, кадровою недостатністю, низькою цифровою культурою, слабкістю механізмів реагування, недосконалістю нормативного регулювання та порушенням балансу між відкритістю інформації й режимом її захисту.

Отже, у вітчизняній науковій літературі простежується перехід від вузького технічного розуміння загроз інформаційній безпеці до комплексного, міждисциплінарного й управлінсько орієнтованого підходу. Якщо ранні класифікації переважно зосереджувалися на витоку, спотворенні, блокуванні інформації, порушенні конфіденційності, цілісності й доступності, то сучасні дослідження дедалі більше враховують кібератаки, інформаційні війни, дезінформацію, маніпулятивний вплив, вразливість критичної інфраструктури, проблеми електронного врядування, інституційну розпорошеність і кадрову неспроможність. Для органів публічного управління в умовах воєнного стану найбільш доцільною є інтегрована класифікація загроз, яка поєднує технічні, правові, організаційні, комунікаційні, кадрові, інституційні та інформаційно-

психологічні критерії. Саме така класифікація дозволяє розглядати інформаційну безпеку не лише як захист даних або цифрових систем, а як умову безперервності державного управління, стійкості публічної влади, збереження довіри громадян і забезпечення інформаційного суверенітету України в умовах війни.

В умовах воєнного стану загрози інформаційній безпеці органів публічного управління мають складний, багаторівневий і динамічний характер, оскільки вони виникають на перетині воєнних, політичних, технологічних, організаційних, соціально-психологічних та комунікаційних процесів. На відміну від мирного періоду, коли основна увага переважно зосереджується на захисті інформаційних систем, персональних даних і режимів доступу до інформації, у воєнний час інформаційні загрози безпосередньо впливають на безперервність управління, обороноздатність держави, стійкість територіальних громад, довіру громадян до влади та здатність державних інституцій швидко реагувати на кризові ситуації. Тому для потреб наукового аналізу доцільно запропонувати класифікацію загроз інформаційній безпеці органів публічного управління, яка враховує не лише їх походження, а й характер впливу, об’єкт спрямування, рівень керованості, масштаб наслідків і специфіку реалізації в умовах збройної агресії (табл. 1.1).

Запропонована класифікація дає змогу розглядати загрози інформаційній безпеці органів публічного управління в умовах воєнного стану як багатовимірне явище, що не зводиться лише до кібератак або технічного захисту інформації. Її практична цінність полягає в поєднанні традиційних критеріїв, пов’язаних із джерелом походження, способом реалізації, об’єктом впливу та масштабом наслідків, із критеріями, що мають безпосереднє значення для публічного управління: впливом на безперервність управління, довіру громадян, інформаційний суверенітет, права людини, міжвідомчу координацію та стійкість державних інституцій.

Таблиця 1.1. Класифікація загроз інформаційній безпеці органів публічного управління

Критерій класи-фікації	Види загроз	Змістова характеристика	Приклади прояву в умовах воєнного стану	Можливі наслідки для органів публічного управління
1	2	3	4	5
За джерелом походження	Зовнішні	Виникають поза межами національної системи публічного управління та спрямовані на послаблення державної стійкості, дестабілізацію інформаційного простору й порушення функціонування органів влади	Кібератаки з боку держави-агресора, інформаційні операції іноземних спецслужб, зовнішні дезінформаційні кампанії, втручання у державні цифрові сервіси	Порушення роботи інформаційних систем, зниження довіри до влади, ускладнення міжвідомчої координації, загроза інформаційному суверенітету
	Внутрішні	Формуються всередині органів влади або національного інформаційного середовища внаслідок організаційних недоліків, кадрових помилок, недбалості чи порушення процедур	Недотримання режиму доступу до службової інформації, слабка кібергігієна персоналу, неузгодженість між структурними підрозділами, помилки адміністрування інформаційних систем	Витік даних, управлінська дезорганізація, втрата службової інформації, зниження ефективності прийняття рішень
	Комбіновані	Поєднують зовнішній ворожий вплив із внутрішніми вразливостями органів публічного управління	Використання фішингових атак проти державних службовців, експлуатація слабких паролів, поширення ворожої дезінформації через внутрішню комунікаційну неузгодженість	Посилення ефекту зовнішніх атак, швидке поширення інформаційних інцидентів, ускладнення локалізації загроз
За об’єктом впливу	Загрози інформаційним ресурсам	Спрямовані на державні реєстри, бази даних, службову документацію, персональні дані, архівні та аналітичні матеріали	Несанкціонований доступ до реєстрів, викрадення персональних даних, знищення або підміна електронних документів	Втрата або спотворення даних, порушення прав громадян, неможливість надання публічних послуг
	Загрози інформаційно-комунікаційній інфраструктурі	Пов’язані з порушенням роботи серверів, мереж, цифрових платформ, систем електронного документообігу та каналів зв’язку	DDoS-атаки, шкідливе програмне забезпечення, блокування офіційних сайтів, атаки на хмарні сервіси	Зупинка електронних сервісів, порушення документообігу, обмеження доступу громадян до адміністративних послуг
	Загрози управлінським рішенням	Впливають на якість, своєчасність, обґрунтованість і законність управлінських рішень через спотворення або неповноту інформації	Надання недостовірних аналітичних даних, затримка критичної інформації, маніпулювання статистикою, інформаційні помилки в кризових штабах	Прийняття неефективних або помилкових рішень, втрата часу, нераціональне використання ресурсів
	Загрози офіційним комунікаціям	Спрямовані на підрив довіри до офіційних повідомлень, дискредитацію органів влади та спотворення державної інформаційної політики	Фейкові повідомлення від імені органів влади, злам офіційних сторінок, поширення неправдивих заяв посадових осіб	Панічні настрої, недовіра до державних інституцій, інформаційна дезорієнтація населення
За характером впливу	Кібернетичні	Реалізуються через цифрові технології та спрямовані на порушення роботи інформаційних систем, мереж і даних	Хакерські атаки, віруси, шифрувальники, фішинг, атаки на державні портали	Технічна дестабілізація, втрата доступу до систем, витік або знищення інформації
	Інформаційно-психологічні	Спрямовані на вплив на свідомість, емоції, поведінку громадян, посадових осіб і соціальних груп	Поширення панічних повідомлень, дискредитація влади, маніпулювання темою мобілізації, провокування соціальної напруги	Зниження суспільної довіри, дезорієнтація населення, погіршення комунікації між владою і громадянами
	Організаційно-управлінські	Пов’язані з недоліками внутрішньої організації роботи органів влади у сфері інформаційної безпеки	Відсутність алгоритмів реагування, нечіткий розподіл відповідальності, недостатня координація між органами влади	Повільне реагування на інциденти, дублювання функцій, втрата контролю над інформаційними процесами
	Правові	Виникають через прогалини, суперечності або недосконалість нормативного регулювання інформаційної безпеки	Невизначеність режимів доступу, недостатня регламентація обміну даними, нечіткість відповідальності за порушення інформаційної безпеки	Правова невизначеність, складність притягнення до відповідальності, нерівномірність практики захисту інформації
	Кадрові	Зумовлені недостатнім рівнем цифрових компетентностей, інформаційної культури та відповідальності персоналу	Невміння розпізнавати фішинг, використання незахищених каналів зв’язку, порушення правил роботи з документами	Внутрішні витоки інформації, помилки в роботі з даними, підвищення вразливості органу влади
За способом реалізації	Активні	Передбачають пряме втручання в інформаційні системи, процеси або комунікації	Злам державних сайтів, видалення баз даних, блокування сервісів, підміна офіційної інформації	Швидке порушення роботи органів влади, потреба в негайному реагуванні, високий рівень збитків
	Пасивні	Пов’язані зі збором, спостереженням, перехопленням або накопиченням інформації без негайного втручання	Моніторинг службових комунікацій, збір відкритих даних про посадових осіб, перехоплення трафіку	Підготовка майбутніх атак, створення профілів вразливостей, загроза прихованого використання інформації

Продовження табл. 1.1

1	2	3	4	5
За ступенем умисності	Умисні	Реалізуються цілеспрямовано суб'єктами, які мають намір завдати шкоди органам влади або державі	Диверсійні кібератаки, інсайдерські витоки, ворожі інформаційні операції	Значна шкода інформаційним ресурсам, підрив стійкості управління, загроза національній безпеці
	Неумисні	Виникають унаслідок помилок, недбалості, низької кваліфікації або неправильного використання інформаційних систем	Випадкове надсилання службових документів стороннім особам, помилки налаштування доступу, використання незахищених пристроїв	Ненавмисний витік даних, порушення службових процедур, зростання операційних ризиків
За масштабом наслідків	Локальні	Обмежуються одним структурним підрозділом, інформаційною системою або органом влади	Збій у роботі окремої бази даних, втрата доступу до локального сервера	Тимчасове ускладнення роботи окремого органу або підрозділу
	Регіональні	Впливають на роботу органів влади в межах області, громади або окремої території	Блокування інформаційних ресурсів військової адміністрації, злам сайту органу місцевого самоврядування, поширення фейків у громаді	Дезорганізація управління на територіальному рівні, зниження довіри населення, ускладнення кризової комунікації
	Загальнодержавні	Стосуються функціонування центральних органів влади, національних реєстрів, державних сервісів або інформаційного простору держави загалом	Атака на державні реєстри, масштабна дезінформаційна кампанія, порушення роботи національних цифрових платформ	Загроза інформаційному суверенітету, порушення державного управління, суспільна дестабілізація
За рівнем передбачуваності	Прогнозовані	Можуть бути виявлені завчасно на основі моніторингу, аналітики, попереднього досвіду або типових сценаріїв ворожих дій	Очікуване посилення кібератак у період державних рішень, масові фейки під час мобілізаційних заходів	Можливість підготовки захисних заходів, резервування ресурсів, попередження негативних наслідків
	Непрогнозовані	Виникають раптово, мають нестандартний характер або використовують нові технології та способи впливу	Нова форма шкідливого програмного забезпечення, неочікуваний витік через невідомий канал, раптовий інформаційний вкид	Потреба в кризовому реагуванні, високий рівень невизначеності, ризик несвоєчасних управлінських рішень
За рівнем керованості	Контрольовані	Можуть бути локалізовані наявними організаційними, технічними або правовими засобами	Виявлений фішинговий лист, локальна спроба несанкціонованого доступу, помилка користувача	Обмежені наслідки за умови своєчасного реагування
	Частково контрольовані	Піддаються управлінському впливу лише частково через складність, масштабність або зовнішній характер загрози	Координована дезінформаційна кампанія, масові атаки на публічні сервіси, витік інформації з кількох джерел	Потреба у міжвідомчій координації, залученні спеціалізованих органів і кризових комунікацій
	Неконтрольовані	Не можуть бути повністю усунені органом влади самостійно та потребують системної державної або міжнародної протидії	Транснаціональні кібератаки, масштабні інформаційні операції держави-агресора, атаки на глобальні цифрові платформи	Високий рівень загрози для державної стійкості, необхідність комплексної національної відповіді
За часовою тривалістю	Короткострокові	Мають разовий або обмежений у часі характер, але можуть спричинити швидкі негативні наслідки	Одноразовий злам сайту, короткочасна DDoS-атака, інформаційний вкид	Тимчасове порушення роботи, потреба в оперативному спростуванні або технічному відновленні
	Довгострокові	Діють протягом тривалого часу та поступово послаблюють інформаційну стійкість органів влади	Системна дискредитація державних інституцій, тривале проникнення в інформаційну систему, постійне поширення наративів держави-агресора	Втрата довіри до влади, накопичення вразливостей, стратегічне послаблення управлінської системи
За функціональним спрямуванням	Загрози безперервності управління	Порушують здатність органів влади виконувати свої функції в кризових умовах	Зупинка електронного документообігу, втрата доступу до критичних реєстрів, блокування внутрішньої комунікації	Порушення управлінського циклу, затримка рішень, зниження ефективності державної реакції
	Загрози довірі до публічної влади	Спрямовані на формування недовіри до офіційних джерел, посадових осіб і державних інституцій	Фальшиві заяви від імені органів влади, інформаційні кампанії про «некомпетентність» держави, маніпуляції навколо чутливих тем	Поширення паніки, зниження легітимності управлінських рішень, суспільна напруга
	Загрози інформаційному суверенітету	Спрямовані на підпорядкування національного інформаційного простору зовнішнім ворожим впливам	Нав'язування ворожих наративів, масовані пропагандистські кампанії, підміна джерел інформації	Послаблення національної ідентичності, дезорієнтація суспільства, підрив державної незалежності в інформаційній сфері
	Загрози правам громадян в інформаційній сфері	Порушують право на доступ до достовірної інформації, захист персональних даних і безпечне користування публічними сервісами	Витік персональних даних, обмеження доступу до важливої інформації без належних підстав, поширення недостовірних повідомлень	Порушення прав людини, зниження якості публічних послуг, недовіра до електронного врядування

Примітка. Систематизовано автором

У практичному вимірі така класифікація може бути використана для розроблення системи моніторингу інформаційних ризиків, визначення пріоритетів захисту державних інформаційних ресурсів, формування алгоритмів реагування на інформаційні інциденти та підвищення готовності органів публічного управління до функціонування в умовах воєнних і гібридних загроз.

Отже, загрози інформаційній безпеці органів публічного управління в умовах воєнного стану мають комплексний характер і поєднують кібернетичні, інформаційно-психологічні, організаційно-управлінські, правові, кадрові та комунікаційні ризики. Їх небезпека полягає не лише у можливому порушенні роботи інформаційних систем, а й у впливі на безперервність державного управління, якість управлінських рішень, суспільну довіру та інформаційний суверенітет держави. Аналіз вітчизняних наукових підходів свідчить про необхідність переходу від вузького технічного розуміння загроз до їх комплексної класифікації за джерелами походження, об’єктами впливу, способами реалізації, масштабом наслідків, рівнем керованості та функціональним спрямуванням. Особливого значення в умовах війни набувають загрози, пов’язані з дезінформацією, кібератаками, інформаційно-психологічними операціями, витоком службової та персональної інформації, а також недостатньою цифровою культурою посадових осіб. Запропонована класифікація дозволяє систематизувати різні види загроз і розглядати інформаційну безпеку як важливу складову стійкості публічного управління. У практичному вимірі вона може бути використана для формування системи моніторингу інформаційних ризиків, визначення пріоритетів захисту інформаційних ресурсів, розроблення алгоритмів реагування на інциденти та вдосконалення міжвідомчої взаємодії.

РОЗДІЛ 2. СУЧАСНИЙ СТАН ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ ОРГАНІВ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ВОЄННОГО СТАНУ (НА МАТЕРІАЛАХ ХМЕЛЬНИЦЬКОЇ ОБЛАСНОЇ РАДИ)

2.1. Аналіз системи забезпечення інформаційної безпеки Хмельницької обласної ради в умовах воєнного стану

В умовах цифрової трансформації публічного управління та зростання кількості кіберзагроз питання забезпечення інформаційної безпеки набувають особливого значення для органів державної влади та органів місцевого самоврядування. Повномасштабна військова агресія російської федерації проти України суттєво посилила ризики інформаційного та кібернетичного характеру, що обумовило необхідність перегляду існуючих підходів до захисту інформаційних ресурсів, інформаційно-комунікаційних систем і каналів обміну даними в діяльності суб’єктів публічного управління.

Хмельницька обласна рада є представницьким органом місцевого самоврядування, який здійснює свої повноваження в межах Конституції та законів України, забезпечуючи реалізацію інтересів територіальних громад області. Для виконання покладених функцій обласна рада використовує значний обсяг інформаційних ресурсів, електронних документів, баз даних, інформаційно-аналітичних систем та засобів електронної взаємодії з громадянами, органами державної влади, підприємствами, установами та організаціями.

Використання сучасних цифрових технологій забезпечує оперативність прийняття управлінських рішень, підвищує відкритість діяльності органу влади та сприяє розвитку електронного врядування. Водночас цифровізація супроводжується зростанням вразливості до кіберінцидентів, несанкціонованого доступу до інформації, витоку службових даних, поширення дезінформації та інших загроз інформаційній безпеці.

Система забезпечення інформаційної безпеки Хмельницької обласної ради формується під впливом загальнодержавних нормативно-правових вимог та внутрішніх організаційних механізмів управління інформаційними ресурсами. Основу правового забезпечення становлять Конституція України [15], закони України «Про інформацію» [33], «Про захист інформації в інформаційно-комунікаційних системах» [32], «Про основні засади забезпечення кібербезпеки України» [35], «Про доступ до публічної інформації» [28], а також Стратегія кібербезпеки України [36] та інші нормативно-правові акти у сфері інформаційної безпеки.

В умовах воєнного стану суттєво зростає значення забезпечення належного рівня захисту інформаційних ресурсів органів публічного управління, оскільки інформаційний простір став одним із ключових напрямів протиборства в умовах гібридної війни. Особливої уваги потребує захист службової інформації, персональних даних працівників та громадян, електронних документів, офіційних вебресурсів і каналів електронної взаємодії між органами влади та громадськістю.

Правові засади такого захисту визначаються низкою нормативно-правових актів. Зокрема, відповідно до Закону України «Про інформацію», інформація визнається об’єктом права власності, а держава гарантує її захист від неправомірного доступу, використання та поширення. У статті 17 зазначеного закону визначено, що охорона права на інформацію забезпечується шляхом створення системи захисту інформації та встановлення відповідальності за порушення інформаційного законодавства [33]. Це положення набуває особливої актуальності для органів місцевого самоврядування, діяльність яких пов'язана з обробкою значних масивів управлінської інформації та персональних даних.

Важливим нормативним підґрунтям є Закон України «Про захист інформації в інформаційно-комунікаційних системах», відповідно до якого захист інформації розглядається як комплекс організаційних, інженерно-технічних, криптографічних та інших заходів, спрямованих на запобігання

несанкціонованим діям щодо інформації [32]. Закон передбачає необхідність створення комплексних систем захисту інформації в державних інформаційно-комунікаційних системах, що є особливо важливим в умовах постійних кібератак на державний сектор України.

Після початку повномасштабної агресії російської федерації значно зросла кількість спроб несанкціонованого доступу до державних інформаційних ресурсів, поширення шкідливого програмного забезпечення та здійснення атак на офіційні вебресурси органів влади. У зв'язку з цим особливого значення набули положення Закону України «Про основні засади забезпечення кібербезпеки України» [35], яким визначено, що кібербезпека є складовою національної безпеки держави та забезпечується шляхом реалізації комплексу правових, організаційних і технічних заходів. Закон також встановлює обов'язок суб'єктів забезпечення кібербезпеки здійснювати своєчасне виявлення, попередження та нейтралізацію кіберзагроз.

Стратегія кібербезпеки України, затверджена Указом Президента України від 01.02.2022 № 37/2022, визначає сучасне кіберсередовище як один із ключових вимірів національної безпеки та наголошує на необхідності формування стійкості державних інформаційних ресурсів до кіберзагроз [36]. Серед пріоритетних напрямів визначено розвиток систем моніторингу кіберінцидентів, удосконалення механізмів реагування на кіберзагрози, підвищення рівня кібергігієни користувачів та впровадження ризик-орієнтованого підходу до управління інформаційною безпекою.

Для Хмельницької обласної ради особливого значення набуває захист системи електронного документообігу, оскільки саме через неї здійснюється підготовка проєктів рішень ради, розпорядчих документів, службового листування, інформаційний обмін між структурними підрозділами виконавчого апарату, депутатським корпусом, органами державної влади, територіальними громадами та іншими суб'єктами публічного управління. В умовах воєнного стану безперебійне функціонування систем електронного документообігу набуває особливого значення, оскільки від оперативності обробки документів

залежить своєчасність прийняття управлінських рішень та ефективність виконання покладених на орган місцевого самоврядування завдань.

Відповідно до Закону України «Про електронні документи та електронний документообіг» [29], електронний документообіг визначається як сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та, за необхідності, підтвердження факту одержання таких документів. Отже, одним із ключових завдань інформаційної безпеки є забезпечення цілісності, достовірності та доступності електронних документів протягом усього життєвого циклу їх використання.

Організація документообігу в Хмельницькій обласній раді здійснюється відповідно до Інструкції з діловодства [11] та із використанням системи електронного документообігу АСКОД [1], яка забезпечує автоматизацію основних процесів роботи з документами. Система АСКОД дозволяє здійснювати реєстрацію документів, погодження проєктів рішень, контроль виконання доручень, накладення кваліфікованих електронних підписів, формування електронних справ та зберігання документів в електронному архіві. Використання такої системи значно підвищує оперативність управлінської діяльності, однак одночасно формує додаткові вимоги до забезпечення кібербезпеки та захисту інформації.

Особливу увагу необхідно приділяти захисту інформації, що циркулює в системі АСКОД. Відповідно до Закону України «Про захист інформації в інформаційно-комунікаційних системах» [32], захист інформації забезпечується шляхом реалізації комплексу організаційних та технічних заходів, спрямованих на запобігання несанкціонованим діям щодо інформації. У практичній діяльності Хмельницької обласної ради це означає необхідність створення безпечного середовища для обробки документів, захисту баз даних, використання сучасних засобів криптографічного захисту та контролю доступу користувачів до інформаційних ресурсів.

Порушення цілісності, конфіденційності або доступності документів, що обробляються в системі електронного документообігу, може призвести до суттєвих негативних наслідків. Серед них – затримка розгляду проєктів рішень, втрата службової інформації, розголошення відомостей з обмеженим доступом, блокування діяльності структурних підрозділів або навіть дестабілізація роботи органу місцевого самоврядування. Особливо небезпечними в умовах воєнного стану є цілеспрямовані кібератаки на державні та муніципальні інформаційні ресурси, метою яких може бути порушення функціонування органів влади або отримання доступу до критично важливої інформації.

У зв'язку з цим важливими складовими системи інформаційної безпеки Хмельницької обласної ради є багаторівневий контроль доступу до системи АСКОД та інших інформаційних ресурсів. Такий підхід передбачає розмежування прав користувачів залежно від посадових обов'язків, використання персональних облікових записів, застосування засобів автентифікації та ідентифікації користувачів, а також ведення журналів подій для фіксації дій із документами. Реалізація зазначених заходів відповідає принципу мінімально необхідного доступу, за якого працівник отримує лише ті права, які необхідні для виконання його службових функцій.

Важливим інструментом забезпечення безпеки електронного документообігу є використання кваліфікованих електронних підписів. Відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги» [30], електронний підпис забезпечує автентичність автора документа та підтверджує цілісність електронних даних. Завдяки цьому система АСКОД забезпечує юридичну значимість електронних документів та унеможливлює їх несанкціоновану зміну після підписання.

Не менш важливим заходом є регулярне резервне копіювання інформації. У Стратегії кібербезпеки України наголошується на необхідності забезпечення стійкості державних інформаційних ресурсів та їх здатності до швидкого відновлення після кібератак або технічних збоїв [36]. Для Хмельницької обласної ради це означає створення резервних копій баз даних системи АСКОД,

документів та іншої службової інформації, що дозволяє мінімізувати ризики втрати даних і забезпечити безперервність управлінських процесів.

Таким чином, система електронного документообігу АСКОД є одним із ключових елементів цифрової інфраструктури Хмельницької обласної ради та одночасно одним із найбільш критичних об'єктів інформаційного захисту. Ефективне функціонування системи потребує поєднання організаційних, правових і технічних механізмів безпеки, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації в умовах зростання кіберзагроз та воєнного стану.

Не менш важливим напрямом є захист офіційного вебсайту та засобів електронної комунікації, через які забезпечується реалізація принципів відкритості та прозорості діяльності органів місцевого самоврядування. Відповідно до Закону України «Про доступ до публічної інформації» органи влади зобов'язані забезпечувати відкритість інформації про свою діяльність, проте така відкритість повинна поєднуватися з дотриманням вимог щодо захисту інформації з обмеженим доступом та персональних даних.

Важливою складовою забезпечення інформаційної безпеки залишається людський фактор. Значна частина кіберінцидентів виникає внаслідок фішингових атак, використання слабких паролів, порушення правил роботи з електронною поштою або недостатнього рівня цифрової грамотності персоналу. З огляду на це державні органи та органи місцевого самоврядування посилюють заходи з навчання працівників основам кібергігієни, правилам безпечної роботи в мережі Інтернет, розпізнаванню шахрайських повідомлень та реагуванню на потенційні кіберзагрози. Такий підхід відповідає сучасним пріоритетам державної політики у сфері кібербезпеки та сприяє формуванню комплексної системи захисту інформаційних ресурсів в умовах воєнного стану.

Система забезпечення інформаційної безпеки Хмельницької обласної ради має комплексний характер та охоплює нормативно-правові, організаційні, технічні й кадрові складові (табл.2.1).

Таблиця 2.1 Основні напрями забезпечення інформаційної безпеки Хмельницької обласної ради в умовах воєнного стану

Напрям забезпечення інформаційної безпеки	Основні заходи	Нормативно-правове підґрунтя	Результат
1	2	3	4
Нормативно-правове забезпечення	Розроблення та актуалізація внутрішніх документів з питань захисту інформації; регламентація доступу до службової інформації; контроль дотримання вимог інформаційного законодавства	Конституція України; Закони України «Про інформацію», «Про доступ до публічної інформації»; Регламент Хмельницької обласної ради; Інструкція з діловодства в Хмельницькій обласній раді; Положення про виконавчий апарат Хмельницької обласної ради; внутрішні розпорядження та накази щодо роботи з інформацією	Формування єдиних правил роботи з інформаційними ресурсами та забезпечення правомірного доступу до інформації
Організаційне забезпечення	Розподіл повноважень між структурними підрозділами; визначення відповідальних осіб за інформаційну безпеку; внутрішній контроль дотримання вимог захисту інформації	Закон України «Про основні засади забезпечення кібербезпеки України»; Положення про виконавчий апарат Хмельницької обласної ради; посадові інструкції працівників; внутрішні регламенти роботи	Підвищення ефективності управління процесами інформаційної безпеки
Захист інформаційно-комунікаційних систем	Використання антивірусного захисту; встановлення міжмережевих екранів; оновлення програмного забезпечення; моніторинг стану інформаційних систем	Закон України «Про захист інформації в інформаційно-комунікаційних системах»; внутрішні інструкції щодо експлуатації інформаційних систем; технічні регламенти	Зменшення ризику несанкціонованого доступу та кіберінцидентів
Контроль доступу до інформаційних ресурсів	Розмежування прав доступу; використання багатофакторної автентифікації; ведення журналів подій; контроль облікових записів користувачів	Закон України «Про захист інформації в інформаційно-комунікаційних системах»; внутрішні політики доступу до інформаційних ресурсів; накази щодо адміністрування інформаційних систем	Мінімізація ризиків витоку, втрати або спотворення інформації
Захист електронного документообігу	Використання кваліфікованих електронних підписів; шифрування документів; резервне копіювання електронних документів; контроль руху документів	Закон України «Про електронні документи та електронний документообіг»; Закон України «Про електронну ідентифікацію та електронні довірчі послуги»; Інструкція з діловодства в Хмельницькій обласній раді	Забезпечення цілісності, достовірності та збереження електронних документів

Продовж.табл.2.1

1	2	3	4
Забезпечення безперервності діяльності та резервування даних	Створення резервних копій; використання захищених сховищ даних; підготовка планів відновлення після кіберінцидентів; тестування процедур резервування	Стратегія кібербезпеки України; Закон України «Про основні засади забезпечення кібербезпеки України»; внутрішні плани реагування на надзвичайні ситуації	Підтримання стабільної роботи ради навіть у разі кібератак або технічних збоїв
Захист офіційного вебсайту та електронних комунікацій	Моніторинг роботи вебсайту; використання захищених протоколів зв'язку; захист корпоративної електронної пошти; протидія DDoS-атакам	Закон України «Про доступ до публічної інформації»; Закон України «Про інформацію»; внутрішні правила використання електронної пошти та вебресурсів	Забезпечення безперервного інформування громадян та захисту офіційних інформаційних ресурсів
Захист персональних даних та службової інформації	Обмеження доступу до персональних даних; контроль передачі інформації; захист баз даних; дотримання режиму службової інформації	Закон України «Про захист персональних даних»; Закон України «Про інформацію»; внутрішні положення про обробку та захист персональних даних	Недопущення розголошення інформації з обмеженим доступом та персональних даних
Підготовка персоналу та забезпечення кібергігієни	Проведення навчань і тренінгів; інструктажі з інформаційної безпеки; тестування на стійкість до фішингових атак; підвищення цифрової грамотності працівників	Стратегія кібербезпеки України; рекомендації Держспецзв'язку; внутрішні програми підвищення кваліфікації працівників	Зниження ризиків, пов'язаних із людським фактором
Моніторинг та реагування на кіберінциденти	Виявлення підозрілої активності; фіксація та аналіз кіберінцидентів; взаємодія з CERT-UA та іншими суб'єктами кібербезпеки; удосконалення механізмів реагування	Закон України «Про основні засади забезпечення кібербезпеки України»; Стратегія кібербезпеки України; внутрішні регламенти реагування на інциденти	Своєчасне виявлення, локалізація та мінімізація наслідків кіберзагроз

Примітка. Складено автором.

Наведені напрями відображають комплексний характер системи забезпечення інформаційної безпеки Хмельницької обласної ради, яка поєднує нормативно-правові, організаційні, технічні та кадрові механізми захисту інформаційних ресурсів. Водночас ефективність їх реалізації потребує подальшого аналізу з урахуванням актуальних викликів воєнного стану, що стане предметом дослідження у наступному підрозділі.

Аналіз організаційної складової системи інформаційної безпеки Хмельницької обласної ради свідчить, що відповідальність за захист інформаційних ресурсів розподіляється між структурними підрозділами виконавчого апарату відповідно до їх функціональних повноважень. Такий підхід дозволяє забезпечити комплексний захист інформації на всіх етапах її створення, обробки, передачі, зберігання та використання.

Координація діяльності у сфері інформаційної безпеки здійснюється керівництвом обласної ради та керуючим справами виконавчого апарату, які забезпечують організацію роботи структурних підрозділів, контроль за дотриманням вимог внутрішніх нормативних документів та впровадженням державної політики у сфері захисту інформації. Саме на цьому рівні приймаються рішення щодо використання інформаційно-комунікаційних систем, організації електронного документообігу, функціонування офіційного вебсайту та інших цифрових ресурсів ради.

Ключову роль у забезпеченні інформаційної безпеки відіграє відділ документаційного забезпечення, який відповідає за організацію документообігу, реєстрацію вхідної та вихідної кореспонденції, адміністрування процесів проходження документів у системі електронного документообігу АСКОД, контроль дотримання Інструкції з діловодства та формування електронних архівів документів. Саме цей підрозділ забезпечує цілісність документопотоків та контроль доступу до документів відповідно до визначених маршрутів погодження.

Важливі функції із захисту персональних даних та кадрової інформації покладаються на відділ організаційного і кадрового забезпечення. Підрозділ

здійснює обробку персональних даних працівників, ведення кадрової документації та контроль доступу до інформації, що містить персональні дані, відомості про проходження служби та іншу службову інформацію з обмеженим доступом.

Відділ забезпечення діяльності керівництва обласної ради забезпечує інформаційний супровід діяльності голови обласної ради та його заступників, організовує роботу зі службовою документацією керівництва, координує інформаційний обмін між керівництвом і структурними підрозділами. У зв'язку з цим на нього покладається відповідальність за дотримання вимог щодо конфіденційності службової інформації та захисту документів управлінського характеру.

Важливим елементом системи інформаційної безпеки є відділ з питань місцевого самоврядування та комунікацій, який забезпечує взаємодію з громадськістю, територіальними громадами та засобами масової інформації, а також бере участь в адмініструванні інформаційного наповнення офіційного вебсайту обласної ради. У межах своїх повноважень підрозділ здійснює контроль за достовірністю та актуальністю інформації, що оприлюднюється, а також забезпечує баланс між принципами відкритості діяльності ради та вимогами щодо захисту інформації з обмеженим доступом.

Правовий супровід діяльності у сфері інформаційної безпеки забезпечує юридичний відділ, який здійснює експертизу проєктів нормативних та організаційно-розпорядчих документів, контролює відповідність внутрішніх процедур вимогам законодавства про інформацію, доступ до публічної інформації, захист персональних даних та кібербезпеку.

Окремі аспекти інформаційної безпеки пов'язані з діяльністю відділу фінансового забезпечення та бухгалтерського обліку та відділу з питань бюджету та моніторингу програм, які працюють із фінансовою інформацією, бюджетною документацією, звітністю та іншими даними, що можуть становити значний інтерес для зловмисників. Для цих підрозділів особливого значення

набувають заходи щодо розмежування доступу до інформаційних ресурсів, резервного копіювання даних та захисту електронних документів.

Управління з питань спільної власності територіальних громад здійснює роботу з інформацією про об'єкти комунальної власності, договори, майнові комплекси та результати їх використання. Відповідно, одним із напрямів забезпечення інформаційної безпеки є захист баз даних та електронних документів, пов'язаних із управлінням майном територіальних громад області.

Функціонування технічної складової інформаційної безпеки частково забезпечується відділом господарського забезпечення, який бере участь в організації матеріально-технічного забезпечення роботи виконавчого апарату, підтриманні працездатності комп'ютерної техніки, серверного обладнання, мережевої інфраструктури та засобів зв'язку. Від належного технічного стану цих ресурсів залежить безперервність функціонування інформаційно-комунікаційних систем ради.

Дані таблиці 2.2 свідчать, що система забезпечення інформаційної безпеки Хмельницької обласної ради базується на функціональному розподілі повноважень між структурними підрозділами виконавчого апарату. При цьому найбільше навантаження у сфері захисту інформаційних ресурсів припадає на відділ документаційного забезпечення, який забезпечує функціонування електронного документообігу, а також на підрозділи, що працюють із персональними, фінансовими та майновими даними. Водночас ефективність системи значною мірою залежить від координації діяльності між підрозділами та використання єдиних процедур управління інформаційною безпекою.

Важливого значення в цих умовах набуває своєчасний обмін інформацією між структурними підрозділами щодо виявлених ризиків, інцидентів інформаційної безпеки та заходів реагування на них, що дозволяє забезпечити цілісність системи захисту інформаційних ресурсів ради. Крім того, зростання кількості кіберзагроз в умовах воєнного стану обумовлює необхідність постійного удосконалення внутрішніх регламентів роботи з інформацією, розвитку цифрових компетентностей працівників та впровадження сучасних

організаційно-технічних механізмів захисту інформаційно-комунікаційної інфраструктури.

Таблиця 2.2 Розподіл функцій забезпечення інформаційної безпеки між структурними підрозділами Хмельницької обласної ради

Структурний підрозділ	Інформаційні ресурси та процеси, за які відповідає підрозділ	Функції у сфері інформаційної безпеки	Потенційні ризики
1	2	3	4
Керівництво обласної ради та керуючий справами виконавчого апарату	Управлінська документація, стратегічні рішення, внутрішні регламенти	Координація діяльності структурних підрозділів; затвердження внутрішніх процедур; контроль дотримання вимог інформаційної безпеки	Несвоєчасне реагування на загрози; недостатня координація заходів безпеки
Відділ забезпечення діяльності керівництва обласної ради	Службова документація керівництва, доручення, проєкти рішень	Контроль конфіденційності документів; організація безпечного обміну інформацією між керівництвом та підрозділами	Витік службової інформації; несанкціонований доступ до управлінських документів
Відділ організаційного і кадрового забезпечення	Персональні дані працівників, кадрова документація	Захист персональних даних; контроль доступу до кадрової інформації; дотримання вимог законодавства щодо обробки персональних даних	Витік персональних даних; порушення режиму конфіденційності
Відділ документаційного забезпечення	Система АСКОД, електронний документообіг, архів документів	Реєстрація та контроль руху документів; адміністрування маршрутів погодження; контроль доступу до документів; забезпечення цілісності електронного документообігу	Втрата документів; порушення цілісності даних; несанкціоноване редагування документів
Відділ з питань місцевого самоврядування та комунікацій	Офіційний вебсайт, публічна інформація, інформаційні повідомлення	Контроль достовірності оприлюднених даних; забезпечення інформаційної відкритості; взаємодія із громадськістю	Поширення недостовірної інформації; кібератаки на вебресурси
Юридичний відділ	Нормативно-правова документація, договори, внутрішні акти	Правова експертиза внутрішніх документів; контроль відповідності законодавству у сфері інформації та кібербезпеки	Юридичні ризики; невідповідність внутрішніх процедур вимогам законодавства

Продовж.табл.2.2

1	2	3	4
Відділ фінансового забезпечення та бухгалтерського обліку	Фінансова документація, бухгалтерські бази даних	Захист фінансової інформації; контроль доступу до фінансових документів; резервування даних	Несанкціонований доступ до фінансових даних; фінансове шахрайство
Відділ з питань бюджету та моніторингу програм	Бюджетна інформація, звітність, програмні документи	Захист аналітичної та бюджетної інформації; контроль електронного документообігу	Викривлення даних; витік інформації про бюджетні процеси
Управління з питань спільної власності територіальних громад	Реєстри майна, договори оренди, документи щодо об'єктів комунальної власності	Захист майнової інформації; контроль доступу до електронних реєстрів та документів	Втрата або спотворення даних щодо об'єктів спільної власності
Відділ господарського забезпечення	Комп'ютерна техніка, серверне обладнання, мережі та засоби зв'язку	Технічне забезпечення функціонування інформаційної інфраструктури; підтримка працездатності обладнання; участь у резервуванні технічних ресурсів	Технічні збої; відмова обладнання; порушення доступності інформаційних систем

Примітка. Складено автором на основі даних Хмельницької обласної ради.

Таким чином, проведений аналіз засвідчив, що система забезпечення інформаційної безпеки Хмельницької обласної ради сформована відповідно до вимог чинного законодавства та базується на поєднанні нормативно-правових, організаційних, кадрових і технічних механізмів захисту інформаційних ресурсів. Її функціонування забезпечується через розподіл повноважень між структурними підрозділами виконавчого апарату, використання системи електронного документообігу АСКОД, регламентацію процесів роботи з інформацією та застосування заходів контролю доступу до інформаційних ресурсів. Водночас цифровізація управлінських процесів, розширення використання електронних комунікацій та зростання інтенсивності кіберзагроз в умовах воєнного стану підвищують вимоги до стійкості інформаційно-комунікаційної інфраструктури, рівня міжвідомчої координації та цифрових компетентностей персоналу. Це обумовлює необхідність подальшого дослідження наявних загроз, вразливостей і ризиків інформаційній безпеці в

діяльності Хмельницької обласної ради з метою визначення напрямів її вдосконалення.

2.2. Оцінювання загроз, ризиків та проблем забезпечення інформаційної безпеки в діяльності Хмельницької обласної ради

Функціонування Хмельницької обласної ради в умовах воєнного стану супроводжується зростанням кількості інформаційних загроз та кіберризиків, що пов'язано із широким використанням цифрових технологій, систем електронного документообігу, електронних комунікацій та мережевої взаємодії з органами державної влади, територіальними громадами й громадянами. Особливістю сучасного етапу є те, що інформаційна інфраструктура органів публічного управління фактично стала об'єктом постійного впливу як випадкових, так і цілеспрямованих загроз.

Відповідно до моделі загроз для інформаційно-комунікаційної системи апарату Хмельницької обласної державної адміністрації, усі загрози інформації можуть бути згруповані у чотири основні категорії: загрози природного походження, випадкові загрози техногенного походження, навмисні загрози техногенного походження дистанційної дії та навмисні загрози техногенного походження контактної дії [9; 21; 22; 24; 20; 23].

З урахуванням особливостей діяльності Хмельницької обласної ради, структури її виконавчого апарату, використання системи електронного документообігу АСКОД, офіційного вебсайту та інших інформаційно-комунікаційних ресурсів було здійснено ідентифікацію основних загроз інформаційній безпеці органу місцевого самоврядування (табл. 2.3).

Дані таблиці 2.3 свідчать, що найбільш чисельною групою є загрози техногенного походження, пов'язані як із функціонуванням інформаційно-комунікаційної інфраструктури, так і з людським фактором. Водночас в умовах воєнного стану суттєво зростає ймовірність реалізації навмисних дистанційних

загроз, спрямованих на порушення функціонування інформаційних систем органів публічного управління.

Таблиця 2.3. Ідентифікація загроз інформаційній безпеці Хмельницької обласної ради

Категорія загроз	Конкретна загроза	Об'єкт впливу	Можливі наслідки для діяльності обласної ради	Рівень ризику
1	2	3	4	5
Природні	Надзвичайні ситуації природного характеру (буревії, пожежі, підтоплення тощо)	Серверне обладнання, локальні мережі, архіви документів	Пошкодження інформаційної інфраструктури, втрата доступу до документів, призупинення роботи окремих підрозділів	Середній
Техногенні (випадкові)	Тривале відключення електроенергії	АСКОД, сервери, телекомунікаційне обладнання	Порушення електронного документообігу, неможливість роботи з електронними документами, затримка прийняття управлінських рішень	Високий
	Відмова серверного або мережевого обладнання	Бази даних, електронний архів, вебресурси	Часткова або повна втрата доступності інформаційних ресурсів	Високий
	Збої програмного забезпечення або оновлень	АСКОД, інформаційні системи	Помилки обробки документів, втрата окремих даних, порушення бізнес-процесів	Середній
	Помилки користувачів під час роботи з документами	Електронні документи, бази даних	Видалення, дублювання або спотворення інформації; порушення маршрутів погодження документів	Високий
	Втрата носіїв інформації або резервних копій	Архіви документів, резервні сховища	Втрата інформації або її потрапляння до сторонніх осіб	Середній
Навмисні дистанційні	Фішингові атаки на працівників виконавчого апарату	Корпоративна електронна пошта, облікові записи	Отримання доступу до внутрішніх інформаційних ресурсів, викрадення службової інформації	Критичний
	Використання шкідливого програмного забезпечення (віруси, трояни, ransomware)	Робочі станції, сервери, мережі	Блокування роботи інформаційних систем, викрадення або шифрування даних	Критичний
	Несанкціонований доступ до системи АСКОД	Система електронного документообігу	Незаконна зміна документів, порушення цілісності інформації, компрометація управлінських процесів	Критичний
	Несанкціонований доступ до корпоративної пошти	Електронні комунікації	Розсилання шкідливих повідомлень від імені посадових осіб, витік службової інформації	Високий

Продовж.табл.2.3

1	2	3	4	5
Навмисні дистанційні	DDoS-атаки на офіційний вебсайт ради	Вебсайт Хмельницької обласної ради	Порушення доступності публічної інформації та сервісів для громадян	Середній
	Компрометація облікових записів користувачів	АСКОД, електронна пошта, внутрішні сервіси	Отримання прав доступу до інформаційних ресурсів сторонніми особами	Високий
Навмисні контактні	Використання інсайдерського доступу працівниками	Внутрішні документи, бази даних	Розголошення службової інформації, несанкціоноване копіювання документів	Високий
	Несанкціоноване встановлення програмного забезпечення	Робочі станції працівників	Поява технічних вразливостей та каналів витоку інформації	Середній
	Навмисне пошкодження або знищення інформації	Бази даних, електронні документи	Втрата критично важливої інформації, порушення діяльності структурних підрозділів	Високий
Воєнні загрози	Кібератаки з боку держави-агресора та афілійованих груп	Вся інформаційно-комунікаційна інфраструктура ради	Порушення функціонування органу місцевого самоврядування, компрометація інформаційних ресурсів	Критичний
	Пошкодження телекомунікаційної інфраструктури внаслідок воєнних дій	Канали зв'язку, мережеве обладнання	Втрата зв'язку із зовнішніми інформаційними системами та державними реєстрами	Високий

Примітка. Складено автором на основі даних Хмельницької обласної ради.

Одними з найбільш небезпечних для діяльності Хмельницької обласної ради є загрози порушення цілісності, доступності та керованості інформаційних систем. У документах з технічного захисту інформації зазначається, що такі загрози можуть проявлятися у вигляді модифікації інформації, її часткового або повного знищення, блокування доступу до інформаційних ресурсів, а також порушення процедур ідентифікації та автентифікації користувачів [8]. Для Хмельницької обласної ради подібні ризики можуть мати наслідком порушення функціонування системи АСКОД, втрату доступу до електронних документів, затримку погодження проєктів рішень та ускладнення взаємодії між структурними підрозділами.

Особливу групу ризиків становлять випадкові загрози техногенного походження. До них належать збої в роботі комп'ютерної техніки, відмова

серверного обладнання, пошкодження носіїв інформації, тривале відключення електропостачання, руйнування каналів зв'язку та інші технічні несправності. Враховуючи, що документообіг Хмельницької обласної ради значною мірою переведений в електронний формат, виникнення таких подій може призвести до втрати доступності інформаційних ресурсів або тимчасового припинення роботи окремих інформаційних систем.

В умовах воєнного стану суттєво зростає актуальність ризиків, пов'язаних із порушенням енергопостачання та функціонування телекомунікаційної інфраструктури. Відключення електроенергії, пошкодження мереж передачі даних або порушення роботи провайдерів можуть негативно впливати на функціонування систем електронного документообігу, офіційного вебсайту ради та корпоративних засобів зв'язку. За відсутності належного резервування такі події можуть ускладнити виконання управлінських функцій та доступ до службової інформації.

Значну загрозу для інформаційної безпеки становить людський фактор. У моделі загроз окремо виділяються випадкові дії користувачів, які можуть призвести до видалення інформації, порушення налаштувань системи, втрати носіїв даних, недбалого поводження з документами або розголошення службової інформації. Для Хмельницької обласної ради даний ризик є особливо актуальним, оскільки практично всі структурні підрозділи працюють із електронними документами, персональними даними, фінансовою та майновою інформацією.

Окремої уваги потребують ризики несанкціонованого доступу до інформаційних ресурсів. Згідно з моделлю загроз, несанкціонований доступ може виникати через помилки в програмно-апаратних засобах безпеки, недоліки політики безпеки, використання шкідливого програмного забезпечення або отримання атрибутів доступу сторонніми особами. У діяльності Хмельницької обласної ради такі загрози можуть стосуватися системи АСКОД, корпоративної електронної пошти, локальної мережі та інформаційних ресурсів офіційного вебсайту.

Найбільш небезпечними в умовах збройної агресії залишаються навмисні загрози дистанційної дії, зокрема кібератаки, фішингові кампанії, поширення шкідливого програмного забезпечення, спроби викрадення облікових даних та реалізація атак типу «маскарад», коли зловмисник використовує облікові дані зареєстрованого користувача. Реалізація таких загроз може призвести до компрометації інформації, блокування роботи окремих сервісів або порушення цілісності документів.

Для визначення пріоритетних напрямів удосконалення системи інформаційної безпеки Хмельницької обласної ради доцільним є не лише опис виявлених загроз, а й їх оцінювання за рівнем імовірності виникнення та потенційного впливу на діяльність органу місцевого самоврядування. Такий підхід дозволяє встановити, які ризики є найбільш критичними для безперервності управлінських процесів, збереження електронних документів, захисту персональних і службових даних, а також стабільного функціонування системи електронного документообігу АСКОД, офіційного вебсайту та корпоративних каналів комунікації. Узагальнені результати оцінювання наведено в табл. 2.4.

Проведений аналіз дозволяє визначити низку проблем забезпечення інформаційної безпеки в діяльності Хмельницької обласної ради. До них належать зростання залежності від цифрової інфраструктури, підвищення ризиків, пов'язаних із людським фактором, необхідність постійного оновлення програмно-технічних засобів захисту, потреба у вдосконаленні механізмів резервування інформації та реагування на кіберінциденти, а також необхідність систематичного підвищення рівня цифрової грамотності працівників. Додатковим викликом виступає необхідність забезпечення балансу між відкритістю діяльності органу місцевого самоврядування та захистом службової інформації в умовах воєнного стану.

.

Таблиця 2.4. Матриця оцінювання ризиків інформаційної безпеки Хмельницької обласної ради

Ризик	Джерело виникнення ризику	Ймовірність виникнення	Рівень впливу	Можливі наслідки для діяльності ради	Загальний рівень ризику
1	2	3	4	5	6
Помилки працівників під час роботи з електронними документами	Людський фактор, недостатній рівень цифрової грамотності, порушення регламентів роботи з АСКОД	Висока	Середній	Видалення, дублювання або некоректне погодження документів; затримка документообігу; потреба у відновленні даних	Високий
Фішингові атаки на працівників виконавчого апарату	Шкідливі електронні листи, підроблені повідомлення, соціальна інженерія	Висока	Високий	Компрометація облікових записів, несанкціонований доступ до електронної пошти, АСКОД або внутрішніх інформаційних ресурсів	Критичний
Несанкціонований доступ до системи АСКОД	Викрадення паролів, слабка автентифікація, порушення правил доступу	Середня	Високий	Незаконний перегляд, зміна або видалення документів; порушення цілісності управлінських рішень	Високий
Втрата або пошкодження баз даних	Технічні збої, помилки адміністрування, шкідливе програмне забезпечення	Середня	Високий	Втрата електронного архіву, службових документів, фінансової або майнової інформації; ускладнення відновлення роботи	Високий
Відмова серверного або мережевого обладнання	Зношеність обладнання, перевантаження систем, технічні несправності	Середня	Середній	Тимчасова недоступність АСКОД, електронної пошти, локальної мережі або офіційних інформаційних ресурсів	Середній
Тривале відключення електроенергії	Воєнні ризики, аварії енергосистеми, недостатність резервного живлення	Середня	Високий	Зупинка електронного документообігу, обмеження доступу до баз даних, порушення комунікації між підрозділами	Високий
DDoS-атаки на офіційний вебсайт	Цілеспрямовані зовнішні кібератаки	Середня	Середній	Тимчасова недоступність публічної інформації, ускладнення інформування громадян, репутаційні втрати	Середній

Продожв.табл.2.4

1	2	3	4	5	6
Витік персональних даних	Порушення правил доступу, недбале поводження з кадровими документами, компрометація облікових записів	Низька / середня	Високий	Розголошення персональних даних працівників або громадян, юридична відповідальність, втрата довіри	Високий
Використання інсайдерського доступу	Зловживання службовими повноваженнями, копіювання або передача службової інформації	Низька	Високий	Витік службової, фінансової або майнової інформації; порушення режиму доступу до документів	Середній
Несанкціоноване встановлення програмного забезпечення	Порушення правил користування робочими станціями, відсутність контролю за ПЗ	Середня	Середній	Зараження комп'ютерів шкідливим ПЗ, поява технічних вразливостей, порушення стабільності роботи систем	Середній
Шкідливе програмне забезпечення, зокрема ransomware	Відкриття небезпечних файлів, заражені носії, вразливості програмного забезпечення	Середня	Високий	Шифрування або викрадення даних, блокування роботи інформаційних систем, потреба у відновленні резервних копій	Високий
Пошкодження телекомунікаційної інфраструктури	Воєнні дії, аварії, перебої у роботі провайдерів	Середня	Високий	Втрата доступу до зовнішніх сервісів, державних реєстрів, електронної пошти та вебресурсів	Високий
Стихійні лиха та надзвичайні ситуації	Природні або техногенні події, пожежі, підтоплення, пошкодження приміщень	Низька	Високий	Фізичне пошкодження обладнання, носіїв інформації та паперових архівів; порушення безперервності роботи	Середній
Недостатнє резервне копіювання даних	Відсутність регулярного тестування резервних копій, нерегламентованість процедур відновлення	Середня	Високий	Неможливість швидкого відновлення інформації після збою, атаки або помилки користувача	Високий
Недостатній рівень кібергігієни персоналу	Нерегулярне навчання, слабка обізнаність щодо фішингу, паролів і безпечної роботи з даними	Висока	Середній	Зростання ймовірності реалізації фішингових атак, витоку паролів, помилкових дій у системах	Високий

Примітка. Складено автором на основі даних Хмельницької обласної ради.

Проведено оцінювання загроз, ризиків та проблем забезпечення інформаційної безпеки в діяльності Хмельницької обласної ради, що дозволило визначити найбільш уразливі елементи її інформаційно-комунікаційної інфраструктури та встановити ключові чинники ризику в умовах воєнного стану. На основі аналізу ідентифіковано основні категорії загроз, серед яких найбільший вплив на функціонування органу місцевого самоврядування мають навмисні дистанційні кіберзагрози, ризики несанкціонованого доступу до інформаційних ресурсів, помилки користувачів, перебої в роботі інформаційних систем та порушення доступності електронних сервісів.

Результати оцінювання ризиків засвідчили, що найбільш критичними для Хмельницької обласної ради є фішингові атаки, компрометація облікових записів працівників, несанкціонований доступ до системи електронного документообігу АСКОД, пошкодження або втрата даних, а також ризики, пов'язані з перебоями енергопостачання та функціонування телекомунікаційної інфраструктури. Встановлено, що значна частина виявлених ризиків пов'язана з людським фактором, що обумовлює необхідність посилення заходів кібергігієни та підвищення рівня цифрової компетентності персоналу.

Отримані результати підтверджують, що наявна система інформаційної безпеки Хмельницької обласної ради потребує подальшого вдосконалення в частині управління ризиками, захисту інформаційних ресурсів, резервування даних, моніторингу кіберінцидентів та забезпечення безперервності функціонування інформаційно-комунікаційної інфраструктури. Виявлені проблеми та вразливості стали підґрунтям для обґрунтування напрямів удосконалення системи забезпечення інформаційної безпеки Хмельницької обласної ради, які будуть розглянуті в наступному розділі дослідження.

РОЗДІЛ 3. НАПРЯМИ ВДОСКОНАЛЕННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ХМЕЛЬНИЦЬКОЇ ОБЛАСНОЇ РАДИ В УМОВАХ ВОЄННОГО СТАНУ

3.1. Удосконалення організаційно-управлінських механізмів забезпечення інформаційної безпеки Хмельницької обласної ради

Результати оцінювання загроз і ризиків інформаційній безпеці Хмельницької обласної ради засвідчили, що значна частина виявлених вразливостей пов'язана не лише з технічними аспектами функціонування інформаційно-комунікаційної інфраструктури, а й з організацією процесів управління інформаційною безпекою [4; 5]. Це обумовлює необхідність удосконалення організаційних механізмів захисту інформації, спрямованих на підвищення рівня керованості, відповідальності та координації дій усіх учасників процесу обробки інформації (табл.3.1).

Першочерговим напрямом удосконалення є формування цілісної системи управління інформаційною безпекою, яка б охоплювала всі структурні підрозділи виконавчого апарату Хмельницької обласної ради. Така система повинна базуватися на принципах ризик-орієнтованого управління, розподілу відповідальності та безперервного контролю за станом захищеності інформаційних ресурсів. Доцільним є розроблення та затвердження комплексної Політики інформаційної безпеки Хмельницької обласної ради, яка визначатиме основні принципи роботи з інформацією, порядок доступу до інформаційних ресурсів, правила використання електронних сервісів, а також механізми реагування на кіберінциденти.

Важливим напрямом удосконалення є чітке визначення відповідальності посадових осіб за забезпечення інформаційної безпеки. З метою підвищення ефективності управління доцільно закріпити на рівні внутрішніх нормативних документів функціональні обов'язки керівництва ради, керівників структурних підрозділів, адміністраторів інформаційних систем та користувачів щодо

захисту інформації. Особливу увагу необхідно приділити визначенню відповідальних осіб за функціонування системи електронного документообігу АСКОД, захист корпоративної електронної пошти, адміністрування вебресурсів та моніторинг інформаційної безпеки.

Таблиця 3.1. Заходи щодо удосконалення організаційних механізмів забезпечення інформаційної безпеки Хмельницької обласної ради

Виявлена проблема	Запропонований захід	Відповідальний підрозділ (посадові особи)	Очікуваний результат
1	2	3	4
Відсутність комплексного підходу до управління інформаційною безпекою	Розроблення та впровадження Політики інформаційної безпеки Хмельницької обласної ради	Керівництво ради, юридичний відділ, відділ документаційного забезпечення	Формування єдиних правил роботи з інформацією та підвищення керованості процесів захисту
Недостатня координація дій між структурними підрозділами під час виникнення кіберінцидентів	Створення координаційної групи (робочої групи) з питань інформаційної безпеки	Керівництво ради, керівники структурних підрозділів	Підвищення оперативності реагування на кіберзагрози та інциденти
Нечіткий розподіл відповідальності за захист інформаційних ресурсів	Актуалізація посадових інструкцій та закріплення функцій інформаційної безпеки за відповідальними особами	Відділ організаційного і кадрового забезпечення, юридичний відділ	Підвищення персональної відповідальності працівників за захист інформації
Високий ризик помилок користувачів під час роботи з АСКОД та електронними документами	Проведення регулярних навчань і тестувань з кібергігієни та безпечної роботи з інформацією	Відділ організаційного і кадрового забезпечення, відділ документаційного забезпечення	Зменшення кількості інцидентів, пов'язаних із людським фактором
Недостатній рівень обізнаності щодо сучасних кіберзагроз	Запровадження системи постійного інформування працівників про актуальні кіберризики та фішингові кампанії	Відділ з питань місцевого самоврядування та комунікацій, відповідальні за інформаційну безпеку	Підвищення рівня кіберстійкості персоналу
Відсутність формалізованих процедур реагування на кіберінциденти	Розроблення та впровадження Плану реагування на інциденти інформаційної безпеки	Керівництво ради, відповідальні за інформаційну безпеку	Скорочення часу реагування та мінімізація наслідків інцидентів

Продовж.табл.3.1

1	2	3	4
Недостатній контроль дотримання вимог інформаційної безпеки	Запровадження щорічного внутрішнього аудиту інформаційної безпеки	Керівництво ради, юридичний відділ, відповідальні за інформаційну безпеку	Своєчасне виявлення порушень і вразливостей
Відсутність системного підходу до управління ризиками	Впровадження процедури регулярного оцінювання ризиків інформаційної безпеки	Координаційна група з питань інформаційної безпеки	Підвищення ефективності управлінських рішень у сфері інформаційної безпеки
Залежність від окремих працівників під час виконання критичних функцій	Регламентація процедур заміщення відповідальних осіб та документування критичних процесів	Відділ організаційного і кадрового забезпечення	Забезпечення безперервності функціонування інформаційних процесів
Недостатня адаптація внутрішніх процедур до умов воєнного стану	Перегляд внутрішніх регламентів роботи з інформацією з урахуванням актуальних кіберзагроз та воєнних ризиків	Юридичний відділ, керівництво ради	Підвищення стійкості системи інформаційної безпеки до сучасних викликів
Відсутність орієнтації на міжнародні стандарти управління інформаційною безпекою	Поетапне впровадження принципів ISO/IEC 27001 у діяльність обласної ради	Керівництво ради, відповідальні за інформаційну безпеку	Формування сучасної системи управління інформаційною безпекою відповідно до міжнародних практик

Примітка. Запропоновано автором.

Одним із ключових напрямів удосконалення організаційних механізмів забезпечення інформаційної безпеки Хмельницької обласної ради пропонується створення постійно діючої координаційної групи з питань інформаційної безпеки. Необхідність її формування обумовлена зростанням кількості кіберзагроз, підвищенням рівня цифровізації управлінських процесів та потребою у забезпеченні постійної взаємодії між структурними підрозділами, які беруть участь у роботі з інформаційними ресурсами [34].

Основною метою діяльності координаційної групи має стати забезпечення комплексного управління інформаційною безпекою Хмельницької обласної

ради, координація заходів із захисту інформації, моніторинг кіберризиків та організація реагування на інциденти інформаційної безпеки. На відміну від існуючої практики, коли окремі функції захисту інформації виконуються різними підрозділами в межах їх повноважень, координаційна група дозволить забезпечити єдиний центр координації та прийняття рішень у сфері інформаційної безпеки.

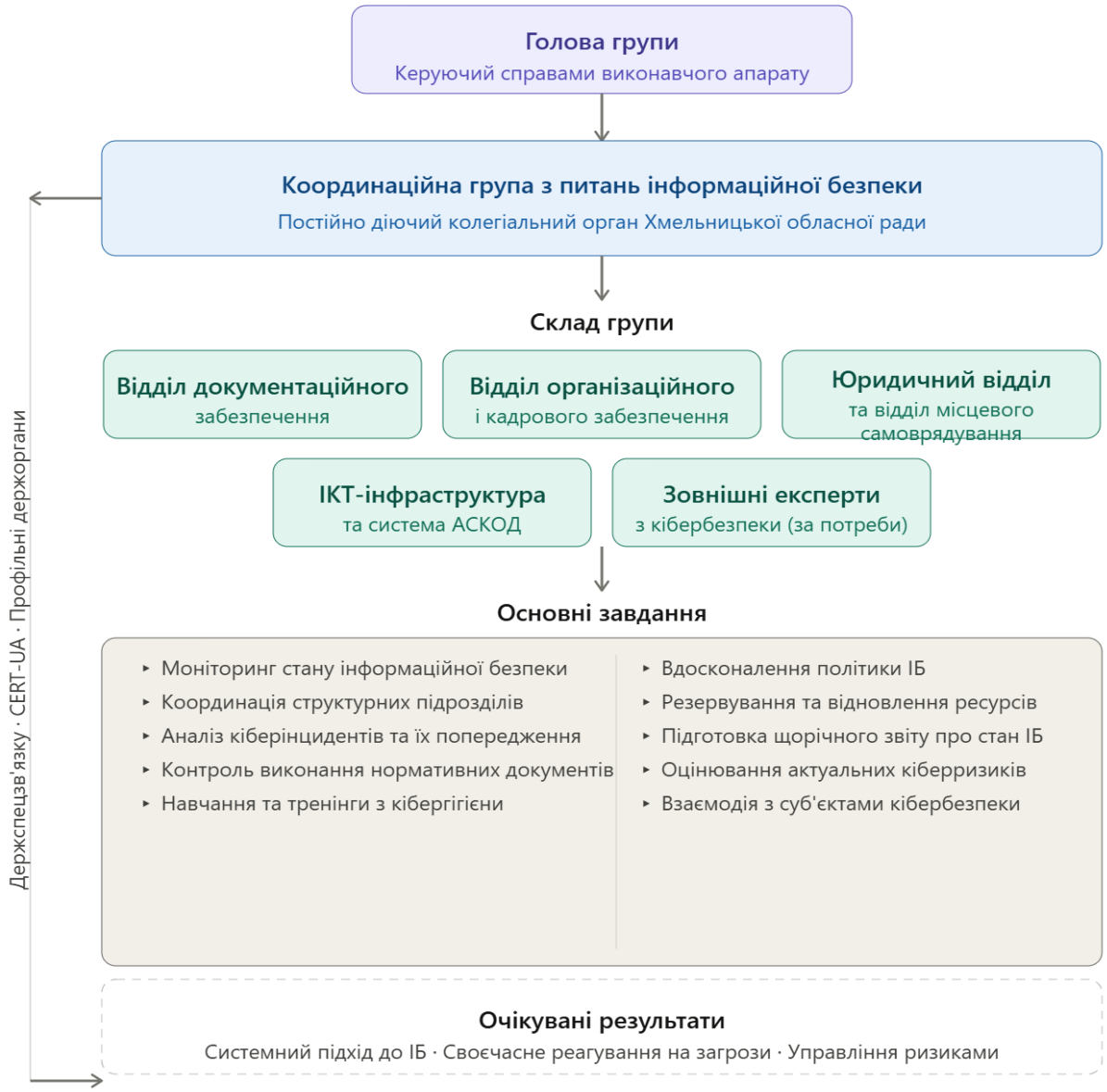

Рисунок 3.1 – Організаційна модель функціонування координаційної групи з питань інформаційної безпеки Хмельницької обласної ради

Примітка. Запропоновано автором.

До складу координаційної групи доцільно включити керуючого справами виконавчого апарату Хмельницької обласної ради як голову групи, представників відділу документаційного забезпечення, відділу організаційного і кадрового забезпечення, юридичного відділу, відділу з питань місцевого самоврядування та комунікацій, а також працівників, відповідальних за функціонування інформаційно-комунікаційної інфраструктури та системи електронного документообігу АСКОД. За необхідності до роботи групи можуть залучатися зовнішні експерти з питань кібербезпеки та представники профільних державних органів.

Основними завданнями координаційної групи пропонується визначити:

– проведення регулярного моніторингу стану інформаційної безпеки та оцінювання актуальних кіберризиків;

– координацію діяльності структурних підрозділів у сфері захисту інформації;

– аналіз причин виникнення кіберінцидентів та розроблення заходів щодо їх недопущення в майбутньому;

– контроль дотримання вимог внутрішніх нормативних документів з питань інформаційної безпеки;

– підготовку пропозицій щодо вдосконалення політики інформаційної безпеки та внутрішніх регламентів;

– координацію заходів із резервування та відновлення інформаційних ресурсів;

– організацію навчань, тренінгів і тестувань працівників з питань кібергігієни;

– взаємодію з Держспецзв'язку, CERT-UA та іншими суб'єктами національної системи кібербезпеки.

Важливою функцією координаційної групи має стати підготовка щорічного звіту про стан інформаційної безпеки Хмельницької обласної ради. У такому звіті доцільно відображати результати оцінювання ризиків, виявлені

порушення, статистику кіберінцидентів, рівень виконання заходів із захисту інформації та пропозиції щодо подальшого вдосконалення системи безпеки.

Очікується, що створення постійно діючої координаційної групи дозволить підвищити узгодженість дій структурних підрозділів, забезпечити своєчасне реагування на сучасні кіберзагрози, покращити процес управління ризиками та сформувати системний підхід до забезпечення інформаційної безпеки Хмельницької обласної ради в умовах воєнного стану.

Окремим напрямом удосконалення є впровадження системного підходу до навчання працівників. Проведений аналіз показав, що людський фактор належить до найбільш суттєвих джерел ризиків інформаційній безпеці. Посадовці у своїй щоденній роботі оперують значними обсягами службової та персональної інформації. В умовах зростання кількості кібератак органи публічної влади стають однією з ключових цілей для зловмисників. Недотримання елементарних правил кібергігієни може призвести до витоку конфіденційних даних, порушення роботи інформаційних систем та навіть до загроз національній безпеці [51].

У зв'язку з цим доцільним є включення питань кібергігієни та захисту інформації до програм підвищення кваліфікації працівників виконавчого апарату. Навчальні заходи повинні охоплювати правила роботи з електронними документами, розпізнавання фішингових повідомлень, безпечне використання корпоративної електронної пошти, порядок роботи з персональними даними та дії у разі виявлення ознак кіберінциденту (додаток А). Під час вебінарів слухачі отримують комплексні знання щодо базові принципи кібергігієни, що є фундаментом захисту як окремих користувачів, так і державних інформаційних систем загалом [13].

Важливим інструментом підвищення ефективності системи інформаційної безпеки є посилення внутрішнього контролю. З цією метою доцільно впровадити практику щорічного аудиту стану інформаційної безпеки, який передбачатиме перевірку дотримання вимог внутрішніх нормативних документів, оцінювання ефективності функціонування механізмів контролю

доступу, аналіз журналів подій та оцінювання готовності структурних підрозділів до реагування на кіберзагрози [26]. Результати таких перевірок повинні використовуватися для актуалізації політик безпеки та планування заходів щодо усунення виявлених недоліків.

З метою підвищення рівня готовності до надзвичайних ситуацій доцільно також запровадити процедури управління інцидентами інформаційної безпеки. Вони повинні передбачати порядок виявлення, реєстрації, аналізу та локалізації інцидентів, а також визначати відповідальних осіб і механізми взаємодії між структурними підрозділами. В умовах воєнного стану особливого значення набуває оперативність реагування на спроби несанкціонованого доступу, фішингові кампанії, витоки інформації та інші кіберзагрози.

Перспективним напрямом розвитку системи інформаційної безпеки є поступове впровадження принципів міжнародного стандарту ISO/IEC 27001, який передбачає функціонування системи управління інформаційною безпекою на основі циклу безперервного вдосконалення [47]. Використання зазначеного підходу дозволить забезпечити системність управління ризиками, підвищити рівень контролю за інформаційними ресурсами та створити умови для подальшого розвитку цифрової стійкості Хмельницької обласної ради.

Отже, удосконалення організаційних механізмів забезпечення інформаційної безпеки Хмельницької обласної ради повинно базуватися на комплексному підході, який поєднує розвиток нормативного забезпечення, удосконалення системи управління ризиками, підвищення рівня відповідальності працівників, розвиток цифрових компетентностей персоналу та посилення внутрішнього контролю. Аналіз нормативного забезпечення інформаційної безпеки Хмельницької обласної ради свідчить про наявність окремих внутрішніх документів, що регламентують питання документообігу, доступу до публічної інформації та діяльності структурних підрозділів. Водночас відсутність комплексного документа стратегічного характеру, який би визначав єдині принципи, цілі, механізми управління ризиками, порядок взаємодії суб’єктів забезпечення інформаційної безпеки та реагування на

кіберінциденти, обумовлює доцільність розроблення та впровадження Комплексної політики інформаційної безпеки Хмельницької обласної ради. Запровадження такого документа дозволить сформувати єдину систему управління інформаційною безпекою, забезпечити узгодженість дій структурних підрозділів та створити організаційне підґрунтя для підвищення стійкості інформаційно-комунікаційної інфраструктури ради й ефективного протистояння сучасним кіберзагрозам в умовах воєнного стану.

З огляду на виявлені в процесі дослідження ризики та проблеми, Комплексна політика інформаційної безпеки Хмельницької обласної ради повинна виступати базовим внутрішнім документом, який визначатиме концептуальні засади функціонування системи захисту інформації, розподіл повноважень між структурними підрозділами та порядок реалізації організаційних і технічних заходів безпеки (табл.3.2). На відміну від чинних локальних документів, які регулюють окремі аспекти роботи з інформацією, запропонована політика має забезпечити інтеграцію всіх складових системи інформаційної безпеки в єдиний механізм управління.

Таблиця 3.2. Пропонована структура Комплексної політики інформаційної безпеки Хмельницької обласної ради

Розділ політики	Основний зміст	Очікуваний результат впровадження
1	2	3
1. Загальні положення	Мета, завдання, сфера застосування політики, основні терміни та визначення	Формування єдиного підходу до забезпечення інформаційної безпеки
2. Принципи забезпечення інформаційної безпеки	Законність, комплексність, ризик-орієнтоване управління, безперервність діяльності, персональна відповідальність, конфіденційність, цілісність та доступність інформації	Визначення концептуальних засад функціонування системи інформаційної безпеки
3. Суб'єкти забезпечення інформаційної безпеки та розподіл повноважень	Повноваження керівництва ради, структурних підрозділів, координаційної групи з питань інформаційної безпеки, адміністраторів та користувачів інформаційних систем	Усунення дублювання функцій та підвищення відповідальності учасників процесу
4. Управління інформаційними активами	Класифікація інформаційних ресурсів, визначення критичних активів, правила роботи з документами та даними	Підвищення рівня захищеності найбільш цінних інформаційних ресурсів
5. Управління ризиками інформаційної безпеки	Порядок ідентифікації, аналізу та оцінювання ризиків; формування реєстру ризиків; механізм їх моніторингу	Своєчасне виявлення та мінімізація загроз інформаційній безпеці

Продовж.табл.3.2

1	2	3
6. Захист електронного документообігу та системи АСКОД	Вимоги до роботи із системою АСКОД, порядок погодження документів, контроль доступу та використання електронних підписів	Підвищення безпеки електронного документообігу та управлінських процесів
7. Управління доступом до інформаційних ресурсів	Політика паролів, автентифікація користувачів, розмежування прав доступу, контроль облікових записів	Зменшення ризику несанкціонованого доступу до інформаційних систем
8. Захист персональних даних та службової інформації	Порядок обробки, зберігання та передачі персональних даних і службової інформації	Дотримання вимог законодавства та зниження ризику витоку інформації
9. Управління кіберінцидентами	Порядок виявлення, реєстрації, класифікації та реагування на інциденти інформаційної безпеки	Скорочення часу реагування на кіберзагрози та мінімізація їх наслідків
10. Резервування та відновлення інформації	Правила резервного копіювання даних, зберігання резервних копій, порядок відновлення інформації	Забезпечення безперервності діяльності та збереження критично важливих даних
11. Навчання та підвищення обізнаності персоналу	Організація навчань, тренінгів, тестувань з кібергігієни та інформаційної безпеки	Зменшення ризиків, пов'язаних із людським фактором
12. Моніторинг, аудит та контроль	Порядок проведення внутрішніх перевірок, аудиту інформаційної безпеки та оцінювання ефективності заходів захисту	Постійне вдосконалення системи інформаційної безпеки
13. Прикінцеві положення	Порядок перегляду та актуалізації політики, відповідальність за її виконання	Підтримання актуальності політики відповідно до нових загроз та змін законодавства

Примітка. Запропоновано автором на основі [31; 14].

Основною метою Комплексної політики інформаційної безпеки пропонується визначити забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів Хмельницької обласної ради, а також підтримання безперервності функціонування інформаційно-комунікаційної інфраструктури в умовах воєнного стану та зростання кіберзагроз. При цьому дія політики повинна поширюватися на всі структурні підрозділи виконавчого апарату ради, систему електронного документообігу АСКОД, офіційний вебсайт, корпоративну електронну пошту, локальні мережі, серверне обладнання, бази даних та інші інформаційні ресурси.

В основу політики доцільно покласти принципи законності, комплексності, ризик-орієнтованого управління, персональної відповідальності, безперервності функціонування інформаційних систем,

своєчасного реагування на інциденти інформаційної безпеки та постійного вдосконалення механізмів захисту інформації. Реалізація зазначених принципів дозволить забезпечити системний підхід до управління інформаційною безпекою та узгодженість дій усіх суб'єктів, залучених до роботи з інформаційними ресурсами.

Важливою складовою політики має стати впровадження процедури регулярного оцінювання ризиків інформаційної безпеки. Пропонується здійснювати таке оцінювання не рідше одного разу на рік, а також після виникнення суттєвих змін в інформаційно-комунікаційній інфраструктурі або після реалізації кіберінцидентів. Результати оцінювання повинні використовуватися для актуалізації заходів захисту інформації та планування ресурсів, необхідних для підвищення рівня безпеки [25; 19].

Окремий розділ політики доцільно присвятити управлінню інцидентами інформаційної безпеки. У ньому необхідно визначити порядок виявлення, фіксації, класифікації та реагування на кіберінциденти, механізми взаємодії між структурними підрозділами, а також порядок інформування керівництва ради про виявлені порушення. Такий підхід сприятиме скороченню часу реагування на загрози та мінімізації можливих наслідків для діяльності органу місцевого самоврядування.

Таким чином, впровадження Комплексної політики інформаційної безпеки Хмельницької обласної ради сприятиме формуванню єдиного організаційного середовища управління інформаційною безпекою, забезпечить систематизацію внутрішніх процедур захисту інформації та створить передумови для підвищення рівня стійкості інформаційно-комунікаційної інфраструктури до сучасних кіберзагроз.

Отже, обґрунтовано напрями удосконалення організаційних механізмів забезпечення інформаційної безпеки Хмельницької обласної ради, які передбачають розвиток нормативного забезпечення, удосконалення системи управління ризиками, підвищення рівня координації між структурними підрозділами та посилення відповідальності працівників за захист

інформаційних ресурсів. Запропоновано створення постійно діючої координаційної групи з питань інформаційної безпеки та розроблення Комплексної політики інформаційної безпеки Хмельницької обласної ради як базового документа системи управління інформаційною безпекою. Реалізація запропонованих заходів сприятиме формуванню цілісної системи управління інформаційною безпекою, підвищенню ефективності реагування на кіберзагрози та створенню організаційних передумов для забезпечення стійкості інформаційно-комунікаційної інфраструктури ради в умовах воєнного стану.

3.2. Напрями підвищення стійкості інформаційно-комунікаційної інфраструктури та електронного документообігу Хмельницької обласної ради

В умовах цифрової трансформації публічного управління інформаційно-комунікаційна інфраструктура стає одним із ключових ресурсів забезпечення ефективної діяльності органів місцевого самоврядування. Для Хмельницької обласної ради особливого значення набуває забезпечення безперервного функціонування систем електронного документообігу, інформаційних ресурсів, засобів електронної комунікації та офіційних електронних сервісів, які забезпечують реалізацію управлінських функцій, взаємодію між структурними підрозділами та комунікацію з громадянами.

Проведене у другому розділі дослідження оцінювання загроз та ризиків засвідчило, що найбільший вплив на функціонування інформаційно-комунікаційної інфраструктури Хмельницької обласної ради здійснюють кіберзагрози, перебої енергопостачання, технічні збої інформаційних систем, ризики несанкціонованого доступу до інформаційних ресурсів, а також помилки користувачів під час роботи з електронними документами. За таких умов забезпечення стійкості інформаційно-комунікаційної інфраструктури повинно розглядатися не лише як технічне завдання, а як важливий напрям

публічного управління, спрямований на підтримання безперервності управлінських процесів та збереження здатності органу місцевого самоврядування виконувати свої функції в умовах кризових ситуацій [46; 47].

Одним із пріоритетних напрямів підвищення стійкості інформаційно-комунікаційної інфраструктури Хмельницької обласної ради пропонується формування системи забезпечення безперервності діяльності. Її впровадження передбачає розроблення Плану забезпечення безперервності діяльності, який визначатиме порядок функціонування виконавчого апарату ради в умовах кіберінцидентів, надзвичайних ситуацій, перебоїв енергопостачання або тимчасової недоступності інформаційних систем.

Основною метою такого плану є забезпечення безперервного виконання критично важливих функцій Хмельницької обласної ради незалежно від характеру та масштабу загроз. При цьому особливу увагу доцільно приділити визначенню критичних управлінських процесів, які повинні функціонувати навіть в умовах часткової втрати доступу до інформаційних ресурсів. До таких процесів можуть бути віднесені підготовка та погодження проєктів рішень обласної ради, забезпечення роботи керівництва, взаємодія з органами державної влади та територіальними громадами, ведення електронного документообігу, а також оприлюднення офіційної інформації.

З метою впровадження системного підходу до забезпечення безперервності діяльності доцільно розробити структуру Плану забезпечення безперервності діяльності Хмельницької обласної ради, наведену в таблиці 3.3.

Запропонований План забезпечення безперервності діяльності спрямований на збереження спроможності Хмельницької обласної ради виконувати свої повноваження в умовах кіберзагроз, надзвичайних ситуацій та інших кризових подій. Його впровадження дозволить забезпечити безперервність критично важливих управлінських процесів, підвищити готовність структурних підрозділів до реагування на інциденти та мінімізувати негативний вплив порушень функціонування інформаційно-комунікаційної інфраструктури на діяльність органу місцевого самоврядування.

Таблиця 3.3 Основні елементи Плану забезпечення безперервності діяльності Хмельницької обласної ради

Елемент плану	Зміст	Очікуваний результат
Мета та сфера застосування	Визначення цілей плану, умов його активації та переліку структурних підрозділів, на які поширюється дія документа	Формування єдиного підходу до забезпечення безперервності діяльності
Визначення критично важливих функцій	Ідентифікація управлінських процесів, від яких залежить функціонування обласної ради (електронний документообіг, підготовка проєктів рішень, інформаційна взаємодія, офіційні комунікації)	Забезпечення пріоритетного відновлення найбільш важливих процесів
Аналіз загроз та сценаріїв кризових ситуацій	Визначення можливих сценаріїв порушення діяльності (кібератаки, відключення електроенергії, пошкодження каналів зв'язку, недоступність АСКОД, витік даних)	Підвищення готовності до реагування на кризові ситуації
Розподіл відповідальності	Визначення повноважень керівництва, координаційної групи з питань інформаційної безпеки та структурних підрозділів	Підвищення оперативності прийняття рішень під час кризових ситуацій
Порядок реагування на інциденти	Алгоритм дій під час виникнення кіберінцидентів, технічних збоїв або порушення функціонування інформаційних систем	Скорочення часу реагування та локалізація наслідків інцидентів
Альтернативні канали комунікації	Визначення резервних способів взаємодії між структурними підрозділами та керівництвом	Забезпечення безперервності управлінських комунікацій
Відновлення інформаційних ресурсів	Порядок відновлення доступу до інформаційних систем, електронних документів та баз даних	Мінімізація часу простою інформаційних систем
Тестування та актуалізація плану	Проведення періодичних перевірок, навчань та оновлення плану відповідно до нових ризиків	Підтримання готовності до кризових ситуацій
Моніторинг виконання	Контроль реалізації заходів та оцінювання ефективності плану	Підвищення рівня стійкості інформаційно-комунікаційної інфраструктури

Примітка. Запропоновано автором.

Водночас забезпечення безперервності діяльності повинно доповнюватися ефективною системою управління ризиками інформаційної безпеки, яка дозволятиме своєчасно виявляти потенційні загрози, оцінювати їх вплив на діяльність обласної ради та формувати комплекс превентивних заходів щодо їх мінімізації. У зв'язку з цим наступним напрямом підвищення стійкості

інформаційно-комунікаційної інфраструктури є удосконалення механізму управління ризиками інформаційної безпеки [50; 52].

Важливою складовою підвищення стійкості інформаційно-комунікаційної інфраструктури Хмельницької обласної ради є впровадження системного підходу до управління ризиками інформаційної безпеки. Проведене в другому розділі дослідження засвідчило, що значна частина загроз інформаційній безпеці має динамічний характер та постійно змінюється під впливом розвитку цифрових технологій, появи нових кіберзагроз і трансформації умов функціонування органів публічного управління в період воєнного стану. За таких умов особливого значення набуває не лише реагування на вже реалізовані інциденти, а й своєчасне виявлення потенційних ризиків та їх попередження.

На сьогодні оцінювання ризиків інформаційної безпеки в більшості органів місцевого самоврядування здійснюється переважно ситуативно та пов'язується із виникненням окремих проблем або необхідністю виконання вимог нормативно-правових актів [19]. Водночас сучасна практика управління інформаційною безпекою передбачає використання ризик-орієнтованого підходу, який дозволяє системно виявляти загрози, визначати ймовірність їх виникнення, оцінювати можливі наслідки та формувати комплекс превентивних заходів щодо їх мінімізації.

З метою підвищення ефективності управління інформаційною безпекою пропонується впровадити в діяльність Хмельницької обласної ради систему управління ризиками інформаційної безпеки, яка передбачатиме регулярний цикл ідентифікації, аналізу, оцінювання, моніторингу та перегляду ризиків. Координацію зазначених процесів доцільно покласти на запропоновану в підрозділі 3.1 координаційну групу з питань інформаційної безпеки.

Ключовим елементом такої системи має стати формування Реєстру ризиків інформаційної безпеки Хмельницької обласної ради. До нього доцільно включати інформацію про джерела загроз, потенційні наслідки їх реалізації, рівень ризику, відповідальних осіб та заходи реагування. Ведення такого

реєстру дозволить забезпечити постійний контроль за актуальними ризиками та своєчасно коригувати заходи захисту інформаційних ресурсів.

Важливим напрямом удосконалення є також запровадження процедури періодичного перегляду ризиків. Пропонується здійснювати комплексне оцінювання ризиків не рідше одного разу на квартал, а також після виникнення кіберінцидентів, модернізації інформаційних систем або внесення змін до організаційної структури виконавчого апарату. Такий підхід дозволить підтримувати актуальність системи управління ризиками та враховувати зміни у зовнішньому і внутрішньому середовищі.

Особливу увагу доцільно приділяти ризикам, які мають найбільший вплив на безперервність діяльності Хмельницької обласної ради, зокрема ризикам компрометації облікових записів користувачів, порушення функціонування системи електронного документообігу АСКОД, втрати доступу до інформаційних ресурсів, витоку персональних даних та порушення роботи інформаційно-комунікаційної інфраструктури. Саме такі ризики повинні перебувати під постійним контролем керівництва та координаційної групи з питань інформаційної безпеки.

Для забезпечення системності процесу управління ризиками доцільно впровадити відповідний організаційний механізм, який наведено на рис. 3.4. Запропонована система управління ризиками інформаційної безпеки передбачає перехід від реагування на окремі інциденти до постійного моніторингу та прогнозування потенційних загроз. Її впровадження дозволить забезпечити своєчасне виявлення ризиків, підвищити ефективність прийняття управлінських рішень та сформувати в Хмельницькій обласній раді ризик-орієнтований підхід до забезпечення інформаційної безпеки. Крім того, систематичне ведення Реєстру ризиків сприятиме підвищенню прозорості процесів управління інформаційною безпекою та створить підґрунтя для подальшого вдосконалення механізмів захисту інформаційних ресурсів.

Етап управління ризиками	*Зміст заходів*	*Відповідальні суб'єкти*	*Очікуваний результат*
Ідентифікація ризиків	Виявлення потенційних загроз інформаційним ресурсам, системі АСКОД, офіційному вебсайту, електронній пошті та інформаційно-комунікаційній інфраструктурі	Координаційна група з питань інформаційної безпеки, керівники структурних підрозділів	Формування актуального переліку ризиків інформаційної безпеки
Аналіз ризиків	Визначення джерел виникнення ризиків, причин їх появи та можливих сценаріїв реалізації	Координаційна група з питань інформаційної безпеки	Встановлення причинно-наслідкових зв'язків між загрозами та можливими наслідками
Оцінювання ризиків	Визначення рівня ймовірності виникнення ризиків та масштабу їх впливу на діяльність обласної ради	Координаційна група, керівництво ради	Ранжування ризиків за ступенем критичності
Формування Реєстру ризиків	Документування ризиків, визначення відповідальних осіб та заходів реагування	Координаційна група з питань інформаційної безпеки	Створення єдиної бази даних щодо ризиків інформаційної безпеки
Планування заходів реагування	Розроблення превентивних та коригувальних заходів щодо мінімізації ризиків	Координаційна група, структурні підрозділи	Зниження ймовірності реалізації ризиків та їх негативних наслідків
Моніторинг ризиків	Постійне відстеження змін у внутрішньому та зовнішньому середовищі, аналіз нових загроз	Координаційна група, відповідальні працівники	Своєчасне виявлення нових ризиків
Перегляд та актуалізація ризиків	Щоквартальне оновлення Реєстру ризиків та перегляд заходів реагування	Координаційна група з питань інформаційної безпеки	Підтримання актуальності системи управління ризиками
Звітування та контроль	Підготовка аналітичних звітів для керівництва ради щодо стану ризиків та ефективності вжитих заходів	Координаційна група з питань інформаційної безпеки	Підвищення обґрунтованості управлінських рішень у сфері інформаційної безпеки

Рисунок 3.1 – Пропонована система управління ризиками інформаційної безпеки Хмельницької обласної ради

Примітка. Запропоновано автором.

Наступним напрямом підвищення стійкості інформаційно-комунікаційної інфраструктури Хмельницької обласної ради є забезпечення цифрової стійкості електронного документообігу. В умовах цифровізації публічного управління система електронного документообігу фактично стала основою організації

внутрішніх управлінських процесів, забезпечуючи підготовку, погодження, реєстрацію, передачу та зберігання документів. Відповідно, будь-які порушення її функціонування можуть негативно впливати на оперативність прийняття управлінських рішень, взаємодію структурних підрозділів та виконання повноважень органу місцевого самоврядування.

У сучасних умовах цифрова стійкість електронного документообігу повинна розглядатися як здатність системи забезпечувати безперервність документування управлінської діяльності [48], збереження інформації та доступність електронних документів навіть за умов виникнення кіберінцидентів, технічних збоїв або інших кризових ситуацій. З огляду на це підвищення цифрової стійкості системи електронного документообігу АСКОД доцільно здійснювати на засадах процесного підходу, орієнтованого на забезпечення стабільності ключових управлінських процесів.

Одним із першочергових напрямів є визначення критично важливих документопотоків та управлінських процедур, які повинні функціонувати безперервно незалежно від зовнішніх чи внутрішніх загроз. До таких процесів доцільно віднести підготовку та погодження проєктів рішень обласної ради, організацію роботи керівництва, взаємодію з органами державної влади та територіальними громадами, а також оприлюднення офіційної інформації. Визначення пріоритетності окремих документопотоків дозволить забезпечити першочергове відновлення найбільш важливих управлінських процесів у разі виникнення кризових ситуацій.

Важливим напрямом підвищення цифрової стійкості є регламентація порядку роботи з електронними документами в умовах надзвичайних ситуацій та кіберінцидентів. З цією метою доцільно передбачити альтернативні механізми погодження документів, резервні канали комунікації між структурними підрозділами, а також процедури тимчасового виконання критично важливих функцій у разі обмеження доступу до окремих інформаційних систем [52]. Такий підхід сприятиме збереженню керованості організаційних процесів навіть за умов часткової недоступності інформаційно-

комунікаційної інфраструктури. Окремого значення набуває впровадження системи моніторингу ефективності електронного документообігу. Для цього доцільно здійснювати регулярне оцінювання показників своєчасності проходження документів, рівня виконання встановлених процедур, кількості збоїв у роботі системи та випадків порушення регламентів роботи з електронними документами. Результати такого моніторингу можуть використовуватися для прийняття управлінських рішень щодо вдосконалення організації документообігу та підвищення його стійкості.

Важливим інструментом підвищення цифрової стійкості електронного документообігу також є проведення періодичного аудиту процесів управління документами [49]. Такий аудит дозволить своєчасно виявляти організаційні недоліки, оцінювати ефективність діючих процедур та визначати напрями їх удосконалення відповідно до актуальних викликів інформаційної безпеки.

З метою систематизації запропонованих заходів доцільно сформувати комплекс заходів щодо підвищення цифрової стійкості електронного документообігу Хмельницької обласної ради, який наведено в таблиці 3.5.

Таблиця 3.5. Заходи щодо підвищення цифрової стійкості електронного документообігу Хмельницької обласної ради

Напрям удосконалення	Зміст заходу	Відповідальний підрозділ	Очікуваний результат
1	2	3	4
Визначення критично важливих докумento-потоків	Ідентифікація документів і процесів, від яких залежить виконання основних функцій обласної ради (проєкти рішень, розпорядчі документи, офіційне листування, звернення громадян тощо)	Відділ документаційного забезпечення, координаційна група з питань інформаційної безпеки	Підвищення пріоритетності захисту найбільш важливих управлінських процесів
Регламентація роботи в кризових умовах	Розроблення порядку роботи з електронними документами під час кіберінцидентів, перебоїв зв'язку або відключення електроенергії	Відділ документаційного забезпечення, юридичний відділ	Забезпечення безперервності документообігу в надзвичайних ситуаціях
Резервування критичних управлінських процесів	Запровадження альтернативних процедур погодження та передачі документів у разі недоступності окремих інформаційних систем	Відділ документаційного забезпечення	Мінімізація ризику зупинення управлінських процесів

Продовж.табл.3.5

1	2	3	4
Моніторинг ефективності електронного документообігу	Регулярний аналіз строків проходження документів, кількості прострочених завдань, випадків порушення регламентів	Відділ документаційного забезпечення	Підвищення оперативності та якості управлінських рішень
Аудит процесів електронного документообігу	Проведення щорічного оцінювання ефективності функціонування системи АСКОД та процедур роботи з документами	Координаційна група з питань інформаційної безпеки, керівництво ради	Виявлення недоліків та своєчасне вдосконалення процесів
Управління доступом до електронних документів	Періодичний перегляд повноважень користувачів відповідно до посадових обов'язків	Керівники структурних підрозділів, відповідальні адміністратори системи	Зменшення ризиків несанкціонованого доступу до інформації
Підвищення цифрових компетентностей працівників	Проведення навчань щодо роботи в АСКОД, правил електронного документообігу та кібергігієни	Відділ організаційного і кадрового забезпечення	Зниження ризиків, пов'язаних із людським фактором
Оцінювання цифрової стійкості документообігу	Запровадження системи показників оцінювання надійності та безперервності електронного документообігу	Координаційна група з питань інформаційної безпеки	Формування інформаційної бази для прийняття управлінських рішень
Інтеграція управління ризиками в процес документообігу	Урахування ризиків інформаційної безпеки під час планування та організації документообігу	Координаційна група з питань інформаційної безпеки	Підвищення стійкості системи до внутрішніх і зовнішніх загроз
Безперервне вдосконалення електронного документообігу	Щорічний перегляд регламентів роботи, процедур та показників ефективності	Керівництво ради, відділ документаційного забезпечення	Адаптація системи до нових викликів цифрового середовища

Примітка. Запропоновано автором.

Запропоновані заходи орієнтовані не стільки на технічну модернізацію системи електронного документообігу, скільки на підвищення її організаційної та управлінської стійкості. Їх реалізація дозволить забезпечити безперервність документообігу, підвищити адаптивність управлінських процесів до кризових ситуацій, посилити контроль за рухом електронних документів та сформувати систему постійного моніторингу ефективності функціонування електронного документообігу в Хмельницькій обласній раді.

Отже, підвищення стійкості інформаційно-комунікаційної інфраструктури та електронного документообігу Хмельницької обласної ради повинно ґрунтуватися на комплексному поєднанні механізмів забезпечення

безперервності діяльності, ризик-орієнтованого управління інформаційною безпекою та вдосконалення організації електронного документообігу. Запропоновані заходи спрямовані на забезпечення стабільності функціонування критично важливих управлінських процесів, своєчасне виявлення та мінімізацію ризиків інформаційної безпеки, підвищення ефективності роботи системи АСКОД і посилення спроможності Хмельницької обласної ради адаптуватися до сучасних викликів цифрового середовища. Реалізація запропонованих напрямів сприятиме зміцненню інституційної стійкості органу місцевого самоврядування, підвищенню надійності управління інформаційними ресурсами та забезпеченню належного рівня інформаційної безпеки в умовах воєнного стану.

ВИСНОВКИ

Бакалаврська робота присвячена вирішенню актуальної науково-практичної проблеми, пов’язаної з удосконаленням механізмів забезпечення інформаційної безпеки в системі публічного управління в умовах воєнного стану та необхідності інтеграції сучасних підходів до управління інформаційними ризиками й забезпечення цифрової стійкості в діяльність Хмельницької обласної ради. У процесі виконання роботи відповідно до поставлених завдань отримано такі узагальнені результати.

1. Встановлено, що інформаційна безпека в системі органів публічного управління в умовах воєнного стану є складною багатоаспектною категорією, яка поєднує стан захищеності інформаційних ресурсів, управлінський процес, інституційну спроможність та стратегічну функцію держави. Визначено, що інформаційну безпеку в системі органів публічного управління в умовах воєнного стану доцільно розглядати як комплексний стан захищеності та водночас динамічний управлінський процес, спрямований на забезпечення цілісності, достовірності, конфіденційності, доступності й безперервності функціонування інформаційних ресурсів, цифрової інфраструктури, офіційних комунікацій, управлінських даних і рішень органів влади від реальних і потенційних загроз, які можуть порушити стабільність державного управління, обороноздатність, суспільну довіру, правопорядок і національну стійкість. Обґрунтовано, що зміст інформаційної безпеки не обмежується технічним або кібернетичним захистом інформації, а охоплює правові, організаційні, кадрові, технологічні, комунікаційні та аналітичні механізми забезпечення стійкості публічного управління. З’ясовано, що особливістю інформаційної безпеки органів публічного управління є її міжсекторальний, превентивний і ризик-орієнтований характер, що передбачає постійний моніторинг загроз, оцінювання ризиків, координацію міжвідомчої взаємодії, захист критичних даних і своєчасне реагування на інформаційні інциденти. Узагальнено, що забезпечення інформаційної безпеки органів публічного управління в умовах воєнного стану виступає необхідною передумовою збереження керованості

держави, захисту інформаційного суверенітету України, протидії інформаційно-психологічним впливам і підтримання національної стійкості.

2. Доведено, що загрози інформаційній безпеці органів публічного управління в умовах воєнного стану мають комплексний, багаторівневий і динамічний характер, оскільки поєднують кібернетичні, інформаційно-психологічні, організаційно-управлінські, правові, кадрові та комунікаційні ризики. Визначено, що їх небезпека полягає не лише у можливому порушенні функціонування інформаційних систем, а й у негативному впливі на безперервність державного управління, якість управлінських рішень, міжвідомчу координацію, суспільну довіру та інформаційний суверенітет держави. З'ясовано, що найбільш значущими критеріями систематизації загроз є джерело походження, об'єкт впливу, характер і спосіб реалізації, ступінь умисності, масштаб наслідків, рівень передбачуваності, керованості, часова тривалість та функціональне спрямування. Обґрунтовано, що в умовах воєнного стану особливої ваги набувають загрози, пов'язані з кібератаками, дезінформацією, інформаційно-психологічними операціями, витоком службової та персональної інформації, порушенням офіційних комунікацій і недостатнім рівнем цифрової культури посадових осіб. Визначено, що запропонована класифікація може бути використана для формування системи моніторингу інформаційних ризиків, визначення пріоритетів захисту державних інформаційних ресурсів, розроблення алгоритмів реагування на інформаційні інциденти та вдосконалення міжвідомчої взаємодії органів публічного управління.

3. Проведено аналіз системи забезпечення інформаційної безпеки Хмельницької обласної ради в умовах воєнного стану. Встановлено, що її функціонування базується на поєднанні нормативно-правових, організаційних, кадрових та технічних механізмів захисту інформації, а реалізація заходів інформаційної безпеки забезпечується через розподіл повноважень між структурними підрозділами виконавчого апарату, використання системи електронного документообігу АСКОД, регламентацію доступу до

інформаційних ресурсів та контроль дотримання вимог інформаційної безпеки. Визначено, що ефективність системи значною мірою залежить від рівня координації діяльності підрозділів, надійності інформаційно-комунікаційної інфраструктури та дотримання працівниками встановлених процедур роботи з інформацією. Особливу увагу в подальшій роботі доцільно приділити підвищенню стійкості цифрової інфраструктури та розвитку організаційних механізмів управління інформаційною безпекою.

4. Здійснено оцінювання загроз, ризиків та проблем забезпечення інформаційної безпеки в діяльності Хмельницької обласної ради. За результатами аналізу ідентифіковано основні категорії загроз, визначено найбільш критичні ризики, пов'язані з фішинговими атаками, несанкціонованим доступом до інформаційних ресурсів, порушенням функціонування системи електронного документообігу АСКОД, помилками персоналу та перебоями в роботі інформаційно-комунікаційної інфраструктури. Обґрунтовано, що в умовах воєнного стану найбільший вплив на рівень інформаційної безпеки здійснюють кіберзагрози та ризики, пов'язані з людським фактором, які можуть негативно впливати на безперервність управлінських процесів та захист службової інформації. Встановлені проблеми та вразливості підтвердили необхідність удосконалення системи управління інформаційною безпекою, посилення заходів кіберзахисту, резервування даних і підвищення цифрових компетентностей працівників, що стало основою для розроблення практичних рекомендацій у наступному розділі дослідження.

5. Обґрунтовано напрями удосконалення організаційних механізмів забезпечення інформаційної безпеки Хмельницької обласної ради в умовах воєнного стану. Запропоновано створення постійно діючої координаційної групи з питань інформаційної безпеки, розроблення Комплексної політики інформаційної безпеки Хмельницької обласної ради, впровадження системи внутрішнього аудиту інформаційної безпеки, формування реєстру ризиків інформаційної безпеки та організацію систематичного навчання працівників з питань кібергігієни і захисту інформації. Визначено доцільність удосконалення

механізмів внутрішнього контролю, регламентації процедур реагування на кіберінциденти та запровадження ризик-орієнтованого підходу до управління інформаційною безпекою. Встановлено, що реалізація запропонованих заходів сприятиме підвищенню рівня координації між структурними підрозділами, удосконаленню системи управління інформаційною безпекою, підвищенню відповідальності працівників за захист інформаційних ресурсів та формуванню цілісного підходу до протидії сучасним інформаційним і кібернетичним загрозам.

6. Розроблено напрями підвищення стійкості інформаційно-комунікаційної інфраструктури та електронного документообігу Хмельницької обласної ради, які передбачають впровадження системи забезпечення безперервності діяльності, удосконалення механізму управління ризиками інформаційної безпеки та підвищення цифрової стійкості електронного документообігу. Запропоновано структуру Плану забезпечення безперервності діяльності, систему управління ризиками інформаційної безпеки та комплекс заходів щодо підвищення цифрової стійкості системи АСКОД. Доведено, що реалізація запропонованих заходів сприятиме забезпеченню безперервності критично важливих управлінських процесів, підвищенню адаптивності обласної ради до сучасних інформаційних загроз та зміцненню інституційної стійкості органу місцевого самоврядування в умовах воєнного стану.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. АСКОД. Система електронного документообігу. URL: https://askod.ua/

2. Баранов О.П. Передумови створення Державної спеціальної служби транспорту та її завдання в системі національної безпеки України. *Вісник Національної академії державного управління при Президентові України.* 2014. No 3. С. 60–65.

3. Бондар І.Р. Інформаційна безпека як основа національної безпеки. *Mechanism of Economic Regulation*. 2014. No 1. С. 68–75

4. Бурик З. М. Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення. *Економіка, управління та адміністрування.* 2021. URL: https://ema.ztu.edu.ua/article/view/242307 [in Ukrainian].

5. Вовк А. Сучасні проблеми публічного управління забезпеченням кібербезпеки в Україні. *Публічне управління: концепції, парадигма, розвиток, удосконалення.* 2024. URL: https://pa.journal.in.ua/index.php/pa/article/view/136.

6. Гурковський В.І. Безпека як об’єкт правовідносин в умовах глобального інформаційного су-спільства. *Правова інформатика.* 2010. No 2(26). С. 72–77.

7. Данильян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: структура та напрям-ки реалізації: навчальний посібник. Х.: Фоліо, 2002. 285 с

8. Деякі питання захисту критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.2019 № 518. URL: Постанова КМУ № 518 від 19.06.2019

9. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Київ: Держстандарт України, 1997. URL: ДСТУ 3396.2-97

10. Золотар О. О., Трубін І. О. Класифікація загроз інформаційній безпеці. *Інформація і право*. 2013. № 3(9). С. 105–112. DOI:

https://doi.org/10.37750/2616-6798.2013.3(9).272386. URL: https://il.ippi.org.ua/article/view/272386

11. Інструкція з діловодства у Хмельницькій обласній раді (чинна редакція, затверджена розпорядженням голови обласної ради).

12. Кириченко Г. Публічне управління у сфері інформаційної безпеки: теоретико-правовий аналіз сучасних викликів. *Herald of Khmelnytskyi National University. Economic Sciences.* 2026. № 2. С. 47–54. DOI: https://doi.org/10.31891/2307-5740-2026-352-5. URL: https://heraldes.khmnu.edu.ua/index.php/heraldes/article/view/2716

13. Кібергігієна як основа кібербезпеки та державної інформаційної безпеки – тема підвищення кваліфікації з питань цифрової грамотності публічних службовців. URL: https://poda.gov.ua/news/258877

14. Комплексна політика інформаційної безпеки Рудківської міської ради. URL: https://rudkivska-gromada.gov.ua/news/1757576662/

15. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

16. Кузьменко Б.В., Чайковська О.А. Захист інформації. Навчальний посібник. Ч.1. (Організаційно-правові засоби забезпечення інформаційної безпеки). К., 2009. 83 с.

17. Ліпкан В.А., Харченко Л.С., Логінов О.В. Інформаційна безпека України: Глосарій. К.: Текст, 2004. 136 с.

18. Миколюк А. В. Публічне управління інформаційною безпекою: діджиталізація та інформаційна війна. Право та державне управління. 2022. № 1. С. 156–161. DOI: https://doi.org/10.32840/pdu.2022.1.23. URL: https://pdu-journal.kpu.zp.ua/archive/1_2022/23.pdf

19. Нагорняк М. Інформаційна безпека у системі публічного управління: виклики та перспективи. *Дніпровський науковий часопис публічного управління, психології, права.* 2024. URL: https://chasopys-ppp.dp.ua/index.php/chasopys/article/view/567.

20. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. URL: НД ТЗІ 1.1-002-99

21. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. URL: НД ТЗІ 1.1-003-99

22. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2000. URL: НД ТЗІ 1.4-001-2000

23. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. URL: НД ТЗІ 2.5-004-99

24. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2005. URL: НД ТЗІ 3.7-003-05

25. Ніколайчук О. В., Шелепало Г. В. Кібербезпека в державних органах та органах місцевого самоврядування. *Проблеми інформаційно-правового забезпечення децентралізації державної влади та цифрової трансформації в Україні.* Вінниця, 2023. С. 113–118. URL: https://dspace.vspu.edu.ua/items/c08c1724-34f5-4ed9-94db-725277713401.

26. Панькова О. В. Органи місцевого самоврядування як суб’єкти забезпечення кібербезпеки України. *Актуальні проблеми державного управління.* 2021. URL: https://uran.oridu.odessa.ua/article/view/237295

27. Присяжнюк М.М. Інформаційна безпека України в сучасних умовах. *Вісник Київського національ-ного університету імені Тараса Шевченка.* Військово-спеціальні науки. 2013. Вип. 30. С. 42–46.

28. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17

29. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15

30. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 01.12.2022 № 2801-IX. URL: https://zakon.rada.gov.ua/laws/show/2801-20

31. Про затвердження Політики інформаційної безпеки у виконавчих органах Хмельницької міської ради. URL: https://www.khm.gov.ua/uk/node/71148

32. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

33. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12

34. Про Консультативну групу з питань інформаційної безпеки при Волинській обласній раді: Рішення Волинської обласної ради від 28.05.2015 №34/91. URL: https://www.volynrada.gov.ua/session/34/91

35. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

36. Про рішення Ради національної безпеки і оборони України від 29 грудня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 01.02.2022 № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/37/2022

37. Регламент Хмельницької обласної ради VIII скликання. URL: https://km-oblrada.gov.ua

38. Рекомендований список онлайн курсів для виконання індивідуальних програм професійного розвитку для категорій посад державної служби «Б» та «В» на 2024 рік за видом підвищення кваліфікації – самоосвіта. URL: https://dasu.gov.ua/attachments/363c885e-da66-4d7c-92d1-3a1283889bce_%D0%A0%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5%D0%BD%D0%B4%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B9_%D1%81%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BD%D0%BE%D0%B2%D0%B8%D0%B9.pdf

39. Типова інструкція з діловодства в міністерствах, інших центральних та місцевих органах виконавчої влади: Постанова Кабінету Міністрів України від 17.01.2018 № 55. URL: https://zakon.rada.gov.ua/laws/show/55-2018-%D0%BF

40. Типова інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну: Постанова Кабінету Міністрів України від 17.01.2018 № 55. URL: https://zakon.rada.gov.ua/laws/show/55-2018-%D0%BF

41. Ткачук Т.Ю., Довгань О.Д. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право.* 2018. No 1 (24). С. 89–104.

42. Харченко С. О. Наукові підходи до класифікації загроз інформаційній безпеці органів Служби безпеки України. *Держава та регіони. Серія: Державне управління.* 2019. № 2(66). С. 191–197. URL: https://pa.stateandregions.zp.ua/archive/2_2019/35.pdf

43. Чмир Я. І. Проблеми забезпечення інформаційної безпеки в системі публічного управління. *Аспекти публічного управління*. 2018. Т. 6, № 9. С. 16–22. DOI: https://doi.org/10.15421/151850. URL: https://aspects.org.ua/index.php/journal/article/view/442

44. Шатун В.Т. Інформаційна безпека – невід'ємна складова національної безпеки України. *Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія».* 2016. Т. 267. Вип. 255. С. 174–180.

45. Шевчук М. О. До питання генези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2023. Вип. 78, ч. 2. С. 134–139. DOI: https://doi.org/10.24144/2307-3322.2023.78.2.21. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/285994

46. Шевчук М. Система управління інформаційною безпекою в контексті сучасних викликів. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки».* 2024. DOI: 10.32999/ksu2307-8049/2024-1-2. URL: https://lj.journal.kspu.edu/index.php/lj/article/view/413

47. AlDaajeh S., Saleous H., Alrabaee S., Barka E., Breitinger F., Choo K.K.R. The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education. *Computers and Security*. 2022. № 119, 102754. https://doi.org/10.1016/j.cose.2022.102754.

48. Jentzsch N. State-of-the-Art of the Economics of Cyber-Security and Privacy (IPACSO Deliverable D4.1), 2018. https://doi.org/10.2139/ ssrn.2671291.

49. McEvoy R., Kowalski S. Cassandra's Calling Card: Socio-Technical Risk Analysis and Management in Cyber Security Systems. *In: CEUR Workshop Proceedings.* 2019. Vol. 2398. P. 65–80

50. Michalec O., Milyaeva S., Rashid A. When the Future Meets the Past: Can Safety and Cyber Security Coexist in Modern Critical Infrastructures? *Big Data & Society.* 2022. № 9(1). 205395172211083. https://doi.org/10.1177/20539517221108369.

51. Pollini A., Callari T.C., Tedeschi A., Ruscio D., Save L., Chiarugi F., Guerri D. Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach. *Cognition, Technology and Work.* 2022. № 24(2). P. 371–390. https://doi.org/10.1007/s10111-021-00683-y.

52. Rosado D.G., Santos-Olmo A., Sánchez L.E., Serrano M.A., Blanco C., Mouratidis H., FernándezMedina E. Managing Cybersecurity Risks of Cyber-Physical Systems: The MARISMA-CPS Pattern. *Computers in Industry*. 2022. № 142. 103715. https://doi.org/10.1016/j. compind.2022.103715.

Виконала: студентка магістратури за спеціальністю 281 Публічне управління та адміністрування заочної форми навчання _____ **А. Рогожа**

Науковий керівник:
доцент кафедри публічного управління та адміністрування, доктор філософії з держ.упр. _____ **О.М. Вжешнєвська**

Робота допущена до захисту:
завідувач кафедри публічного управління та адміністрування, д.держ.упр., професор _____Е.В. Щепанський

Додаток А


6
ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЦИФРОВА ГРАМОТНІСТЬ
PROMETHEUS
Інформаційна гігієна. Як розпізнати брехню в соцмережах, інтернеті та на телебаченні
CLICK
На цьому курсі ви зрозумієте, як не потрапити на гачок маніпуляторів в інтернеті, у соцмережах та онлайн-ЗМІ. А ще ці знання допоможуть пояснити рідним та колегам, які небезпеки чатують на них в онлайні
PROMETHEUS
Інформаційна гігієна під час війни
CLICK
Курс буде корисним тим, хто хоче самостійно розібратися у методах російської пропаганди та зрозуміти, як не наступити на інформаційні міни ворога, а також для тих, хто хоче зрозуміло та просто пояснити рідним шкідливість певної інформації
PROMETHEUS
Основи інформаційної безпеки
CLICK
Курс буде корисним практично кожному, хто у повсякденному житті стикається з комп'ютерами, смартфонами, планшетами, користується соціальними мережами, електронною поштою чи просто шукає інформацію у глобальній мережі Інтернет.
PROMETHEUS
Інформаційна безпека
CLICK
Курс «Інформаційна безпека» пропонує насамперед практичні завдання й навички – як навчитися викривати фейки та захищатися від різного штибу зловмисних інформаційних впливів
PROMETHEUS
Дезінформація: види, інструменти та способи захисту
CLICK
Курс розрахований для будь-кого, хто хоче більше дізнатися про дезінформацію та стати стійкішим до неї – адже це проблема, яка стосується кожного з нас.
Дія
Цифрова держава
Доступ до публічної інформації
CLICK
Як писати звернення про доступ до публічної інформації та отримати потрібний результат
Дія
Цифрова держава
Відкриті дані для державних службовців
CLICK
Як розміщувати відкриті дані та використовувати їх для розробки державних політик.
edera
Захист персональних даних
CLICK
Стаття 32 Конституції України проголошує право людини на невтручання в її особисте життя. Проте з розвитком цифрового світу все складніше захищати межі власного простору та оберігати свою приватність.
Дія
Цифрова держава
Персональні дані
CLICK
Персональні дані і політика приватності: що це та як безпечно ними управляти
PROMETHEUS
Медіаграмотність: практичні навички
CLICK
Мета курсу – надати слухачам зручний інструментарій для вивчення медіаграмотності заради втілення його принципів та засад в українському суспільстві
edera
Very Verified: онлайн-курс з медіаграмотності
CLICK
онлайн-курс з медіаграмотності» поясниє, як орієнтуватися в інформації довкола та як розпізнавати дезінформацію та пропаганду.
Освітній хаб
Критичне мислення і інформаційна культура (у форматі SCORM)
CLICK
Курс присвячений одній з найважливіших навичок 21 ст - мистецтву аналізувати.
Дія
Цифрова держава
Цифрові держслужбовці
CLICK
Все для цифровізації держслужби: SMM, електронний документообіг, Agile, Scrum, Kanban, командна комунікація в Asana, Slack, дистанційна робота

Продовження додатоку А

Джерело: [5].