Міністерство освіти і науки України
Національний університет «Острозька академія»
Навчально-науковий інститут міжнародних відносин та національної безпеки
Кафедра національної безпеки та політології

Кваліфікаційна робота на здобуття освітнього ступеня магістра
на тему: «**Забезпечення охорони інформації з обмеженим доступом в умовах АТО та воєнного стану»**

Виконав студент ІІ курсу, групи МНб-21
спеціальності 256 Національна безпека
(за окремими сферами забезпечення і
видами діяльності)
Данилюк Давід Петрович

Керівник – доктор юридичних наук,
професор, академік АН ВШ України
Романов Микола Степанович

Рецензент – кандидат юридичних
наук, доцент
Стрельбіцька Леся Ярославівна

Острог – 2024

ЗМІСТ

ВСТУП

Актуальність теми. Забезпечення захисту конфіденційної інформації в умовах антитерористичної операції (АТО) та воєнного стану набуває особливої актуальності у наш час, коли інформація стає все більш ключовою у житті суспільства і країни. Зростання значення інформаційних ресурсів і технологій призводить до інтенсифікації інформаційних відносин у всіх галузях, включаючи збір, обмін та збереження інформації. У періоди АТО та воєнного стану, коли національна безпека є пріоритетом, захист конфіденційної інформації набуває критичного значення. Конфліктні ситуації створюють нові загрози для безпеки інформації, такі як дезінформація, кібератаки та шпигунство. Тому забезпечення цілісності, конфіденційності та доступності інформації є невід'ємною частиною стратегії національної безпеки.

У зв'язку з сучасними гібридними загрозами та кібератаками, які часто виникають під час конфліктів, важливо розробляти та впроваджувати ефективні заходи захисту інформації, враховуючи специфіку воєнних дій та зміни загрозного середовища. Це впливає не лише на безпеку держави, а й на успішність проведення військових операцій, захист інформаційних ресурсів та збереження важливої інформації. Тому тема захисту ї інформації з обмеженм доступом в умовах АТО та воєнного стану є ключовою для забезпечення національної безпеки та стабільності.

Аналіз останніх досліджень і публікацій. Наукове дослідження зосереджувалося на працях ряду вчених, які глибоко вивчали питання правового статусу інформації, зокрема, обмеженого доступу, та регулювання її захисту. До числа таких учених належать Б.А. Кормич, В.А. Ліпкан, Р.А. Калюжний, О.В. Олійник, В.Ю. Баскаков, І.С. Чиж, М.Я. Швець, М.О. Шилин, І.В. Арістова, О.О. Кулініч, А.Б. Стоцький, А.І. Марущак, М.І. Дімчогло, М.П. Стрельбицький, В.М. Панченко, А.М. Гуз та інші. Значну кількість наукових праць також присвячено питанню обмеження доступу до інформації, авторами

яких є І. Корж, В. Політанський, Ю. Фігель, І. Арістова, О. Денісов, Б. Кормич, Т. Костецька, А. Марущак, Ю. Тодик, І. Чиж та інші.

Також, дослідження правового регулювання обмеженого доступу до інформації мають у своєму арсеналі праці вчених, таких як Безверха Ю.В., Брижко В.М., Слизьконіс Д.М., Коць Д.В., Галушка В.Ю., Денищук Д.Є., Бем М.В., Баранов О.А., Брайчевський С.М. та інші.

Незважаючи на цей широкий обсяг досліджень, в науковій літературі ще не вистачає робіт, які б докладно розглянули питання захисту інформації з обмеженим доступом у періоди АТО та воєнного стану. Це визначає актуальність подальших досліджень в цій області.

Об'ктом дослідження є охорона інформації з обмеженим доступом в період АТО та воєнного стану.

Предметом дослідження є теоретико-методичні засади, підходи та методи забезпечення охорони інформації з обмеженим доступом.

Мета дослідження – дослідження механізму забезпечення охорони інформації з обмеженим доступом в період АТО та воєнного стану, а також шляхів удосконалення організації охорони інформації з обмеженим доступом в контексті російсько-української війни.

Реалізація поставленої мети зумовила потребу у розв'язанні таких **завдань дослідження**:

– провести аналіз наукових джерел та оцінити рівень дослідження проблематики;

– дослідити сутність інформації з обмеженим доступом у доктрині та законодавстві;

– подати опис видів інформації з обмеженим доступом;

– розглянути обмеження права на доступ до публічної інформації під час АТО та воєнного стану;

– описати технічні заходи захисту інформації у сучасних інформаційних системах;

– дослідити заходи захисту інформації з обмеженим доступом від витоку та несанкціонованого доступу;

– вивчити міжнародний досвід у сфері захисту інформації з обмеженим доступом;

– запропонувати шляхи вдосконалення організації захисту інформації з обмеженим доступом в контексті російсько-української війни.

Експериментальна база та апробація….

Для досягнення мети і вирішення поставлених задач були **використані такі методи**:

1) Загальнонаукові підходи включають аналіз і синтез наукових досліджень, використання індукції та дедукції, проведення зіставлення і порівняння для виявлення сутності інформації з обмеженим доступом. Також вони охоплюють системний аналіз, систематизацію і класифікацію для розрізнення видів інформації з обмеженим доступом та формулювання висновків.

2) Конкретно-наукові підходи використовують методи історичного та логічного аналізу, а також системно-ситуаційний підхід при дослідженні еволюції захисту інформації з обмеженим доступом. Також вони застосовують системно-ситуаційний підхід для аналізу технологічного аспекту захисту інформації з обмеженим доступом.

3) Пошуково-бібліографічний підхід використовується для збору інформації з метою створення основного масиву джерел і подальшої їхньої систематизації.

Теоретична база. У процесі написання роботи були використані роботи широкого спектру вітчизняних та зарубіжних учених, які охоплюють як питання, що безпосередньо стосуються теми дипломної роботи, так і більш загальні аспекти. Джерельною базою дослідження є:

– інтерпретаційні джерела, такі як монографії, дисертації, автореферати дисертацій, праці вітчизняних та зарубіжних вчених; статистичні звіти та довідкова література;

– інтернет-ресурси, що містять матеріали наукових конференцій та наукову літературу.

Структура роботи. Випускна кваліфікаційна робота складається із вступу, трьох розділів, висновків, списку інформаційних джерел, що включає 64 найменувань.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ОХОРОНИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

1.1. Аналіз наукових джерел та стан опрацювання проблематики

У сучасному світі велике значення приділяється інформації, оскільки третє тисячоліття характеризується як епоха знань і сучасних технологій. У такому світі інформація виступає як ключова потреба, що визначає людське функціонування, вона є основою знань, базою для проєктування, планування та моделювання, а також важливим чинником прийняття рішень та управління подіями у суспільстві, науці та техніці. Одночасно із цим в суспільному уявленні інформація стала розглядатися як товар, що призвело до необхідності його захисту від незаконних або небажаних втручань, а також до виникнення інформації, доступ до якої обмежено.

Основними характеристиками інформації як об’єкта захисту вважаються доступність, цілісність та конфіденційність. До цього переліку також можна додати такі властивості, як невідмовність, достовірність, адекватність, актуальність, точність, повнота і т. д.

Згідно з дослідженням Г. В. Бондарука щодо понять «інформація», «інформаційна грамотність», «інформаційна культура», «інформаційна компетентність» у контексті ідей Нової української школи (НУШ) [13], важливим елементом будь-якої компетентності є здатність розуміти та працювати з інформацією. Це сприяє ефективному використанню інформації, яка є основою для навчання та використання у всіх аспектах життя. Тому формування інформаційної грамотності є актуальною задачею, особливо для дітей та молоді, які тільки починають розуміти важливість інформації. У зазначеній статті розглядається сутність понять «інформація», її різновиди, властивості, інформаційні процеси, а також уточнюється розуміння таких

термінів, як «інформаційна грамотність», «інформаційна культура», «інформаційна компетентність» у контексті Нової української школи.

У суспільстві почали сприймати інформацію як продукт, що спричинило потребу у його захисті від неправомірних або небажаних втручань. Основними характеристиками, які прийнято вважати важливими для захисту інформації, є доступність, цілісність та конфіденційність. До цього переліку можна додати такі властивості, як невідмовність, достовірність, адекватність, актуальність, точність, повнота тощо.

За словами А.В. Дідука, інформація – це повідомлення, що містить відомості, включаючи конфіденційні, до яких можна отримати доступ за умови фактичного дозволу на знайомство з ними. Цей доступ надається обмеженому, чітко визначеному колу осіб і називається фактичним правом доступу, при цьому інформацію відносять до сфери обмеженого доступу. Інформація, що вважається конфіденційною, можуть переглядати представники органів влади в межах своєї компетенції та виконання покладених на них завдань, але не використовувати її для комерційних цілей чи інших неприпустимих метах [12, с. 17].

У документі «Глобальні принципи з національної безпеки та права на інформацію (Цванські принципи)» [16] відзначається, що національна безпека є однією з найважливіших соціальних підстав для обмеження, проте наголошується на необхідності беззаперечного дотримання чітко визначених стандартів і правил обмеження доступу до інформації. Наведені кілька важливих принципів зазначені у цьому документі:

Принцип 3: Інформацію слід зберігати у таємниці лише у випадках, коли розкриття її може створити конкретні ризики завдання значної шкоди законним інтересам національної безпеки.

Принцип 5: Жодній урядовій особі не можна категорично забороняти розкриття інформації.

Принцип 8: У надзвичайних обставинах держава може тимчасово відмовитися від своїх зобов'язань стосовно права на пошук, отримання та поширення інформації, якщо це суворо вимагають невідкладні обставини та тільки на обмежений період.

Принцип 10: Інформацію про серйозні порушення міжнародних прав людини та гуманітарного права слід розкривати незалежно від умов.

Принцип 16: Інформацію можна приховувати у відповідності до національної безпеки тільки на той час, поки вона необхідна для захисту законних інтересів національної безпеки, при цьому рішення про обмеження доступу до інформації має періодично переглядатися.

Принцип 40: Державні службовці, які діють у інтересах суспільства і викривають зловживання уряду, повинні бути захищені від помсти.

Крестьянінов О.О. [33] уточнює, що система правових норм створюється для забезпечення обробки та захисту інформації. Ця система включає в себе правила, умови і заходи, спрямовані на організацію обігу, обмеження доступу та забезпечення безпеки інформації. Такий комплекс заходів утворює правовий режим інформації з конкретною метою – забезпечення загальної безпеки в державі [33, с. 4].

Ліпкан В.А., Баскаков В.Ю. [37] підкреслюють, що введення режиму інформації з обмеженим доступом має на меті організацію суспільних відносин у цій сфері та враховує два головні мотиви: забезпечення права на інформацію та захист національних інтересів, які взаємодіють між собою між запитувачами та розпорядниками інформації [37, с. 130-131].

Чернишова Т.В. [60] визначає компоненти правового режиму інформації, включаючи:

– процедуру створення (або збирання) відповідної інформації та її класифікацію як інформації з обмеженим доступом;

– права власності на інформацію;

– умови зберігання, розповсюдження та використання інформації;

– процедуру доступу до інформації;

– правовий захист інформації [60, с. 100].

У своїй статті «Теоретико-правові аспекти інформації з обмеженим доступом» [32], Д. Коц розглядає різницю в уявленні про інформацію з обмеженим доступом між законами та доктриною. Він пропонує власне розуміння цього поняття та виявляє прогалини в національному законодавстві України стосовно юридичної дефініції такої інформації [32].

О. Кулініч у своїй роботі [34] описує характеристики інформації з обмеженим доступом наступним чином:

– зіст такої інформації включає знання, повідомлення та відомості про соціальні процеси та матерію, які використовуються у суспільстві та особами;

– ця інформація існує у формі ідеального, нематеріального об’єкта;

– вона функціонує в рамках взаємодії суб’єктів суспільних відносин, таких як особи, групи та різні соціальні утворення;

– інформація з обмеженим доступом не пов’язана з конкретним матеріальним носієм і є об’єктом правового регулювання;

– вона має якісні та кількісні характеристики, причому їх співвідношення має нелінійний характер;

– інформація цієї категорії не є доступною загалом;

– вона відома та використовується обмеженим колом осіб;

– суб’єкти такої інформації приймають заходи для обмеження доступу третіх осіб до неї;

– інформація з обмеженим доступом має високу соціальну цінність через її обмеженість для третіх осіб, що може призвести до значної шкоди;

– зміст такої інформації відповідає законодавчим обмеженням [34, с. 72-73].

С. Гордієнко у своїй роботі «Конфіденційна інформація та «таємниці»: їх співвідношення» розглядає особливості кожного типу інформації з обмеженим

доступом, такі як характеристики таємності, особи, які мають право на доступ, права та обов'язки осіб, що стосуються цих таємниць, відповідальність за розголошення інформації та особливості її захисту для кожного типу [17, с. 233].

І. П. Кушнір та О. М. Царенко провели комплексне дослідження правового режиму інформації з обмеженим доступом у сфері діяльності Державної прикордонної служби України. Вони розглядають цей режим як «визначені законодавством процедури та правила, пов'язані з наданням дозволу, доступом, охороною, захистом та здійсненням діяльності з інформацією, яка має велику цінність для прикордонної безпеки країни» [35, с. 184].

При аналізі наукових джерел і стану розглянутої проблематики забезпечення охорони інформації з обмеженим доступом в період АТО та воєнного стану було виявлено значний інтерес до цієї теми у наукових дослідженнях. Дослідження у цьому напрямку спрямовані на аналіз правового режиму, визначення особливостей регулювання доступу до конфіденційної інформації та ролі цієї інформації у забезпеченні національної безпеки в умовах конфлікту та воєнного стану.

Аналіз наукових джерел наголошують на важливості ретельного аналізу правових норм і стратегій, спрямованих на захист конфіденційної інформації під час воєнних дій, а також на впровадженні ефективних заходів для її забезпечення. Ключовим аспектом є встановлення критеріїв класифікації обмежено доступної інформації і розробка механізмів для її обробки, зберігання та передачі. Дослідження підкреслюють, що захист інформації у період АТО та воєнного стану є ключовим завданням для національної безпеки та військової ефективності. Розуміння та ефективне використання такої інформації може істотно підвищити результативність воєнних операцій та сприяти успішному виконанню завдань у воєнних умовах.

1.2. Поняття інформації з обмеженим доступом у доктрині та праві

Етимологія слова «інформація» свідчить про його походження від середньофранцузького терміну informacion, що означає «кримінальне розслідування». З латинського слова informatiō(n) виникають кілька значень, таких як роз'яснення, виклад фактів, подій, витлумачення, представлення, поняття, ознайомлення та просвіта [63, с. 128].

У «Енциклопедії сучасної України» інформацію визначають як відомості, які передаються різними способами за допомогою умовних сигналів і технічних засобів. Тут інформація розглядається з погляду її змісту, структури організації та динаміки, що охоплює процеси створення, передавання, сприйняття, використання та зберігання [24, с. 479-480].

За «Тлумачним словником української мови» термін «інформація» має такі значення: перше – це те саме, що інформування, тобто, повідомлення про що-небудь та доведення до відома, а друге – відомості про якісь події або діяльність, повідомлення про щось [55, с. 42].

Н. Вінер розуміє інформацію як ознаку змісту, яка надходить до нас з зовнішнього світу під час нашого адаптування до нього та адаптації наших почуттів. Його визначення стверджує, що процес отримання та використання інформації полягає у нашому адаптуванні до непередбачуваності зовнішнього оточення та нашої діяльності в цьому контексті [52, с. 97].

Отже, інформація представляє собою набір відомостей, концепцій та змісту явищ і процесів, які передаються та обробляються для розуміння та усвідомлення конкретних значень.

Інформація відіграє значущу роль у суспільстві. Вона сприяє освіті, виконанню конкретних завдань, пізнанню різних сфер та реалій суспільного життя.

Крім того, інформація є не лише набором фактів, але і важливою складовою емоційної та духовної сфери людини. Люди через інформацію

виражають свої почуття, емоції та думки. Духовний аспект людини тісно пов’язаний із інформацією, оскільки та безпосередньо впливає на її психологічний стан. Тому важливо, щоб вчитель подавав інформацію таким чином, щоб вона була максимально зрозумілою та сприйнятою учнями. Ця інформація також має бути надійною, щоб вона могла виконати свою функцію належним чином.

Інформацію можна класифікувати за способом сприйняття на наступні види: візуальну (зорову), аудіальну (слухову), нюхову, смакову та тактильну (дотикову). Згідно з дослідженнями, більшість (приблизно 90%) інформації, яку ми сприймаємо, є візуальною, аудіальна становить 9%, тоді як всі інші види інформації разом складають лише 1%. Таким чином, основним способом сприйняття інформації є аудіо-візуальний [12].

Щодо форми подання, інформацію поділяють на образно-знакову та сигнальну. Люди сприймають інформацію через образи та знаки, тоді як технічні системи обробляють сигнали. Образно-знакова інформація має різноманітні форми: числову, текстову, графічну, звукову інформацію.

Щодо застосування, інформація може бути навчальною, науково-технічною, суспільно-політичною, художньо-естетичною та іншими.

За результатом інтелектуальної діяльності відзначають особисту (досвід окремої людини), суспільну (діяльність суспільства) та загальнолюдську (надбання людства загалом) інформацію.

Щодо доступності, інформацію розподіляють на відкриту та обмежену. Відкрита інформація доступна для всіх і користується загальним доступом. Обмежена інформація не може бути розголошена, оскільки її розголошення може завдати шкоди державі, групі людей або окремій особі [12].

Конституція України встановлює широкий спектр прав і свобод для кожної людини та громадянина, що регулюють їх правовий статус у сфері інформаційних відносин. Наприклад, згідно зі статтею 34, кожен має право

вільно збирати, зберігати, використовувати та розповсюджувати інформацію у будь-якій формі на свій розсуд.

Одним із гарантованих прав є доступ до інформації, який закріплено в законі України «Про доступ до публічної інформації» [2]. Цей закон передбачає систематичне та оперативне оприлюднення інформації через офіційні друковані видання, веб-сайти, державний веб-портал відкритих даних, інформаційні стенди та інші канали, а також відповідь на запити громадян.

Також, сучасне законодавство України (частина 2 статті 21 Закону «Про інформацію») встановлює принцип, що будь-яка інформація є відкритою, за винятком тієї, яка законом визначена як інформація з обмеженим доступом [1].

Відповідно до Закону України «Про інформацію» [1], інформація класифікується на різні види: особиста, довідково-енциклопедична, екологічна, товарна, науково-технічна, податкова, правова, статистична, соціологічна та інші. Згідно зі статтею 6 Закону України «Про доступ до публічної інформації», обмеження доступу до інформації має місце в деяких ситуаціях, таких як захист національної безпеки, територіальної цілісності, громадського порядку, здоров’я населення, репутації та прав інших осіб, запобігання розголошенню конфіденційної інформації та збереження авторитету суду. Такі обмеження мають застосовуватися лише у випадках, коли розголошення інформації може завдати серйозної шкоди цим інтересам та коли така шкода переважає суспільний інтерес у доступі до цієї інформації.

Оцінювання за трискладовим тестом застосовується у кожному конкретному випадку, коли необхідно вирішити, чи потрібно розкривати або обмежувати доступ до інформації. Розпорядник інформації повинен надавати інформацію з обмеженим доступом, якщо не існує законних підстав для її обмеження, які були чинними раніше.

Інформацію з обмеженим доступом складають відомості або дані, які можуть бути збережені на різних матеріальних носіях або відображені в електронному вигляді, але доступ до них обмежений відповідно до

законодавства України її власником або добросовісним користувачем (суб'єктом владних повноважень, фізичною або юридичною особою) через їхню особливу цінність на підставі закону [10, с. 49]. Ця визначеність відповідає реальності, оскільки особливість інформації визначається не тільки її матеріальним носієм, на якому вона зберігається [9, с. 11].

За думкою А.І. Марущака, інформація з обмеженим доступом включає в себе конфіденційні або таємні дані, чиї правові аспекти регулюються українським законодавством, і до яких правомірно обмежений доступ власником цих даних [40, с. 44-49]. Це визначення було актуальним до введення в дію нової редакції Закону №2657-XII. Це визначення, застосоване А.І. Марущаком, використовує термін «відомості», хоча поняття «інформація» також охоплює такі дані. У науковому середовищі використовуються різні терміни, такі як «інформація», «відомості», «дані», «знання» [39, с. 23].

М.І. Дімчогло висловлює думку про необхідність включення в законодавчий акт консолідованого підходу до специфіки та різноманіття цих об'єктів (інформація, її види, доступ до неї, режими доступу, інформація з обмеженим доступом, конфіденційна інформація, державна таємниця, банківська таємниця, персональні дані, персональна інформація про особу). Такий законодавчий акт повинен використовувати практику консолідації правових норм, яка була використана у Законі України «Про інформацію» на основі статей [19, с. 14].

Далі досліджуються наукові підходи до тлумачення конфіденційної інформації. Конфіденційна інформація визначається як дані, які є виключною власністю приватних суб'єктів та можуть мати різноманітний характер. Основними характеристиками є те, що вона не є загальновідомою, а доступ до неї мають лише конкретні приватні суб'єкти, які самостійно вирішують, коли і як її розголошувати або обмежувати доступ до неї. Конфіденційна інформація може включати в себе як дані про її власника, так і іншу інформацію, яка перебуває у володінні приватного суб'єкта [23].

Наукова спільнота визначає конфіденційну інформацію як таємницю приватного життя, професійну таємницю, службову таємницю, таємницю слідства і судочинства, комерційну таємницю [31, с. 15]. В. Ліпкан і Л. Капінус уточнюють, що під конфіденційною інформацією слід розуміти перш за все дані про фізичну особу, які є непридатними для розголошення, і доступ до яких обмежений самою фізичною чи юридичною особою (яка на законних підставах володіє такою інформацією), і їх поширення можливе лише за їхнім бажанням відповідно до умов, передбачених ними ж. Такі права можуть бути обмежені законом [38, с. 48]. Ця концепція визначення актуальна лише для інформації про особу та інформації, доступ до якої обмежено фізичною чи юридичною особою. Інші види інформації, такі як інформація про особливості виробничого процесу, корисні моделі та подібна інформація, які перебувають у власності юридичної особи і доступ до яких обмежено юридичною особою, виходять за межі цього визначення.

Юристи вітчизняної правової науки розглядають службову інформацію як певний тип інформації з обмеженим доступом, призначений для виконання службових обов'язків і зібраний у процесі різних службових діяльностей, таких як оперативно-розшукова або контррозвідувальна, а також в сфері оборони країни. Ця інформація не класифікується як державна таємниця.

Колектив авторів посібника «Службова інформація: порядок віднесення та доступ» пропонує механізм визначення службової інформації серед публічної інформації і рекомендує використовувати такий підхід на основі наступних критеріїв:

1) визначення, які саме інтереси будуть порушені в разі розголошення інформації (наприклад, це може бути національна безпека або територіальна цілісність);

2) аналіз можливої шкоди, яка виникне в результаті розголошення такої інформації;

3) встановлення обґрунтування, чому саме шкода від розголошення цієї інформації переважає загальний суспільний інтерес у доступі до неї [53, с. 13].

Тому є необхідність встановлення на рівні закону чіткого механізму (порядку) класифікації інформації як службової, оскільки дотепер питання обмеження обігу такої інформації фактично регулюються міністерствами і відомствами. Це підтверджується положенням частини третьої статті 21 Закону № 2657-XII, яка стверджує, що порядок класифікації інформації як таємної або службової, а також умови доступу до неї визначаються законом [1].

Таємною вважається інформація, що містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу, яка передбачена законом як така. Таємна інформація – це будь-яка інформація з обмеженим доступом, що має характер державної таємниці [9, с. 11]. Проте варто зазначити, що банківська або професійна таємниця також можуть бути приватного характеру. Тому у визначенні таємної інформації необхідно враховувати не лише державний аспект.

Таємна інформація може бути розглянута як одночасно найбільш детально описана у законодавстві і найменш врегульована. Це становище випливає з того факту, що тільки певні види таємної інформації, такі як державна та банківська таємниці, мають вичерпні визначення на рівні законів та підзаконних актів. У той же час, інші види таємної інформації, як от лікарська таємниця, таємниця усиновлення (удочеріння), адвокатська таємниця, таємниця вчинення нотаріальних дій, таємниця голосування, таємниця листування, професійні та інші, не мають достатнього законодавчого врегулювання. Виникає багато питань стосовно класифікації і доступу до цих видів таємної інформації [51, с. 8].

Коц Д. В. [32] визначає інформацію з обмеженим доступом як дані або відомості, що зберігаються на матеріальних носіях або в електронному вигляді та перебувають у законному володінні різних суб’єктів (фізичних чи

юридичних осіб, суб'єктів владних повноважень), до яких доступ обмежується законом у інтересах національної безпеки, територіальної цілісності, громадського порядку, для запобігання злочинам, охорони здоров'я, захисту прав осіб, уникнення розголошення конфіденційної інформації, забезпечення авторитету суду, та що містяться у документах суб'єктів владних повноважень. Така інформація також може становити внутрішню службову кореспонденцію, пов'язану з управлінням діяльністю таких суб'єктів, виконанням контрольних функцій, ухваленням рішень, а також ті, що отримані в ході спеціальних операцій, контррозвідувальної діяльності, у сфері оборони країни, які, у разі розголошення, можуть завдати шкоди особам, суспільству та державі, і в таких випадках переважатиме суспільний інтерес у доступі до цих даних [32, с. 101-111].

Баскаков В. Ю. розглядає поняття інформації з обмеженим доступом таким чином: будь-які відомості або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, доступ до яких обмежений її власником або добросовісним користувачем (суб'єктом владних повноважень, фізичною або юридичною особою) на законних підставах [11].

Висновки, які можна зробити з вивчення поняття інформації з обмеженим доступом в доктрині та праві, полягають у наступному. Ця інформація є важливою складовою сучасного інформаційного суспільства через свою здатність містити конфіденційні дані, які вимагають особливого захисту. Визначення цього поняття у доктрині та праві може варіюватися в залежності від контексту та законодавчих систем кожної країни. Наявність чіткої нормативно-правової бази для регулювання доступу до інформації з обмеженим доступом є ключовою для забезпечення правової стабільності і захисту прав людей та організацій. Таким чином, розуміння та визначення цього поняття в доктрині та правовому полі є важливими аспектами для створення ефективних механізмів захисту конфіденційної інформації і забезпечення безпеки суспільства в цілому.

1.3. Загальна характеристика видів інформації з обмеженим доступом

Згідно із законом країни «Про інформацію», інформація з обмеженим доступом включає в себе конфіденційну, таємну та службову інформацію. Конфіденційною вважається інформація про фізичну особу та інформація, доступ до якої обмежено фізичною або юридичною особою, за винятком суб'єктів владних повноважень. Поширення конфіденційної інформації відбувається лише за згодою відповідної особи та відповідно до її умов або у випадках, передбачених законом. Правовий режим конфіденційної інформації регулюється законом. Порядок класифікації інформації як таємної або службової, а також умови доступу до неї визначаються законодавством [1].

Конфіденційна інформація відрізняється від загальнодоступної тим, що не призначена для широкого кола осіб. Її обмеження доступу повинно бути чітко і відповідно встановлено відповідно до чинного законодавства. Особливість адміністративно-правового регулювання обмеження доступу до інформації полягає у поєднанні приватно-правових та публічно-правових методів регулювання [62, с. 94-98].

Конфіденційна інформація, незалежно від сфери відносин, в яких вона використовується, має значення для власника інформації - держави, фізичної особи або юридичної особи. Ця цінність інформації проявляється у її використанні в сфері державного управління для різних аспектів суспільного життя та в приватній сфері для захисту та виконання прав фізичних та юридичних осіб. Розголошення такої інформації може значно пошкодити як інтересам держави, так і приватним та публічним інтересам [62, с. 94-98].

Класифікація конфіденційної інформації може бути здійснена за кількома критеріями:

1. За правом власності:

– Державна конфіденційна інформація;

– Приватна конфіденційна інформація.

2. За правом доступу:

– Право доступу виконавчих осіб у зв’язку з виконанням службових обов’язків;

– Право доступу власника та осіб, яким це право надано.

3. За сферою застосування:

– Комерційна конфіденційна інформація;

– Банківська конфіденційна інформація;

– Податкова конфіденційна інформація;

– Адвокатська конфіденційна інформація;

– Судова та інші [62, с. 94-98].

Таємною інформацією вважається інформація, що включає відомості, які є державною та іншою, визначеною законом, таємницею, розголошення якої може спричинити шкоду особі, суспільству і державі [1]. Згідно зі статтею 8, таємною інформацією вважається інформація, що містить державну, професійну, банківську таємницю, таємницю слідства та інші, визначені законом, таємниці.

Службова інформація може включати в себе такі елементи:

1) Інформація, яка міститься у документах суб’єктів владних повноважень і є внутрішньою службовою кореспонденцією, доповідними записками, рекомендаціями, якщо вони стосуються розробки стратегій діяльності установи або виконання контрольних та наглядових функцій органами державної влади, процесом ухвалення рішень та передують публічному обговоренню та/або ухваленню рішень;

2) Інформація, зібрана у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яка не відноситься до державної таємниці, згідно зі статтею 9 [2].

Згідно з цим Законом, основним критерієм визначення конфіденційної інформації є можливість її поширення лише за згодою відповідної фізичної або юридичної особи та за умовами, визначеними ними.

Згідно з поглядом Кормича Б.А. [30], таємна інформація може бути класифікована як комерційна або стратегічна. Під комерційною розуміється інформація, що створюється з метою отримання прибутку через її використання іншими, тоді як стратегічна інформація пов’язана безпосередньо з діяльністю держави і має особливий режим збирання, виробництва, зберігання та використання, що включає режим таємності за допомогою державного примусу [30, с. 42-45].

О. Кулініч пропонує класифікацію таємної інформації залежно від способу її отримання, визначаючи таємниці, отримані за допомогою цивільно-правового договору та під час професійної діяльності [34]. В. Ліпкан та В. Баскаков також підтримують цей підхід, але вказують на складність виокремлення видів інформації за цим критерієм, пропонуючи розподіл таємної інформації на ту, що була отримана безоплатно і за гроші [37, с. 97].

Ю. Капіца висловлює недолік в тому, як буде визначатися ступінь конфіденційності інформації у випадках, коли вона не поширюється або коли розповсюдження не визначається її конфіденційністю [28, с. 119].

Г. Андрощук розглядає до конфіденційної інформації ті дані, які стосуються ділових, виробничих, торгових аспектів та інших, і які не можуть бути розголошені через їх секретність [8, с. 28].

В. Ліпкан та В. Баскаков вирізняють дві категорії таємної інформації: конфіденційну, в яку вони включають будь-яку інформацію з обмеженим доступом, що не має відношення до державної таємниці, і таємну, що включає будь-яку інформацію з обмеженим доступом, яка має ознаки державної таємниці [37, с. 96].

О. Г. Семенюк зауважує, що поза зазначеним поділом таємної інформації, який запропонували ці дослідники, залишається конфіденційність інформації, яка стосується фізичних або юридичних осіб. Оскільки розголошення конфіденційної інформації з боку третьої особи не призводить безпосередньо до шкоди, то збереження цієї інформації в таємниці забезпечується шляхом

законодавчого встановлення юридичної відповідальності за її несанкціоноване розповсюдження. Просто розпорядженням власною таємницею будь-яким чином не виникає юридична відповідальність. Це означає, що збереження прихованої інформації в таємниці є правом, а не обов'язком для її власника, який має можливість визначати умови її використання, а також може припинити цей режим без юридичних наслідків для себе [50, с. 44-51].

Власник таємної інформації має право самостійно визначати умови її оприлюднення, необхідність охорони, обмежувати доступ до неї та зберігати її у таємниці. У свою чергу, держава гарантує захист такої інформації шляхом закріплення права на таємницю, встановлює правила поводження з нею та застосовує заходи впливу щодо порушників режиму конфіденційності. Таким чином, якщо інформація вже передана сторонній особі, то ця особа стає носієм інформації, яка не належить їй, тому вона зобов'язана дотримуватися режиму конфіденційності, а не має права самостійно вирішувати, як використовувати таку інформацію. Порушення цих вимог призводить до юридичної відповідальності згідно з чинним законодавством [50, с. 44-51].

З погляду обов'язковості норм поведінки, встановлених правовим режимом конфіденційної інформації, можна сказати, що цей режим має характер імперативний для осіб, які отримали цю інформацію (через закон чи договір), тобто вони мають обов'язок дотримуватися встановлених правил. У той же час, для осіб, які надають цю інформацію та є її власниками, режим є диспозитивним, що означає, що вони самі можуть визначати умови та способи використання цієї інформації.

Щодо терміну дії режиму конфіденційності, слід застосовувати правило, що спеціальні правові режими інформації, як правило, є безстроковими і діють доти, поки існують відповідні стосунки, в рамках яких ця інформація використовується.

О. Г. Семенюк виокремлює такі характеристики конфіденційної інформації:

– це конфіденційна інформація, яка стосується фізичних або юридичних осіб і знаходиться у володінні третьої сторони через виконання професійних або службових обов'язків;

– має фактичну або потенційну цінність для власника;

– характеризується довірчим статусом і не підлягає розголошенню через можливість завдати шкоди власнику;

– доступ до неї обмежений та регулюється законодавством [50, с. 44-51].

Наявність вищевказаних ознак в сукупності вказує на те, що інформація може бути визнана конфіденційною. Якщо хоча б одна з цих ознак відсутня, то інформація не може бути визнана конфіденційною.

Варто зазначити, що конфіденційність не є властивістю самої інформації з природи, але вона виникає через законодавство або визначається рішенням відповідної особи, яка має на це право за законом. З цього випливає, що конфіденційність інформації є вторинною і залежить від визначених у законі правил та обставин.

Отже, суб'єкт, якому надана або стала відомою інформація, зобов'язаний дотримуватися її конфіденційності та використовувати її лише у встановлені законом цілі. Така інформація може бути передана лише тим особам, які визначені в законі, або з відома власника інформації.

Згідно з законом, якщо таємна інформація про фізичну особу або комерційна таємниця стають відомими третім особам через їхні обов'язки, вона може набути статусу різних видів таємниць, таких як банківська, адвокатська, лікарська, таємниця сповіді тощо. Також можливе виникнення статусу слідчої таємниці або службової інформації відповідно до умов, передбачених законом [50, с. 44-51].

Отже, різноманітні види інформації з обмеженим доступом, такі як конфіденційна, таємна та службова, визначаються не лише законом, але й рішеннями власника чи уповноваженої особи. Конфіденційність інформації не

витікає безпосередньо з її характеру, а захищається через законодавство або рішення власника, установленням правового режиму, який визначає умови доступу та обмежує розголошення.

Розглянуті критерії класифікації конфіденційної інформації, такі як право власності, право доступу, сфера застосування, спосіб придбання, розкривають різні аспекти її визначення та регулювання. Наприклад, інформація може бути визнана конфіденційною в зв’язку з комерційними чи професійними обов’язками, має довірчий характер і підлягає особливому правовому захисту.

Висновок цього розділу полягає у визнанні того, що інформація з обмеженим доступом вимагає дотримання спеціальних правил з її збереження, передачі та використання. Захист конфіденційної інформації є важливою складовою сучасного суспільства та правової системи, що визначається не тільки законодавством, але й етичними та професійними стандартами, що регулюють поведінку та взаємовідносини між суб’єктами, які мають доступ до конфіденційної інформації.

Висновки до першого розділу

Таким чином, під час аналізу наукових джерел і стану досліджень забезпечення захисту інформації з обмеженим доступом під час періоду АТО та воєнного стану було виявлено значний інтерес до цієї теми у наукових розвідках. Дослідження в цьому напрямку спрямовані на аналіз правового режиму, визначення особливостей регулювання доступу до конфіденційної інформації, а також роль цієї інформації у забезпеченні національної безпеки під час конфлікту та воєнного стану.

Наукові джерела наголошують на необхідності ретельного аналізу правових норм і політик, спрямованих на захист конфіденційної інформації під час воєнного періоду, а також впровадження ефективних заходів для її захисту. Важливим є визначення критеріїв класифікації інформації з обмеженим доступом, а також розробка механізмів для її обробки, зберігання та передачі. Дослідження підкреслюють, що забезпечення захисту інформації з обмеженим доступом під час АТО та воєнного стану є надзвичайно важливим завданням для національної безпеки та військової діяльності. Розуміння та ефективне використання цієї інформації може значно підвищити результативність операційних дій і сприяти успішному виконанню завдань у умовах воєнного конфлікту.

Інформація з обмеженим доступом представляє собою дані та відомості, які знаходяться на матеріальних або електронних носіях із законним правом власності у фізичних осіб, юридичних осіб або держави. Ця інформація відноситься до таємної, службової або конфіденційної категорій відповідно до встановленого законодавством порядку. Зважаючи на потенційну чутливість цих даних, їх захист вважається ключовим аспектом сучасного інформаційного середовища. У різних правових системах та доктринах існують варіації у визначенні інформації з обмеженим доступом, що залежить від контексту та умов кожної конкретної країни. Однак, наявність чіткої нормативно-правової бази для регулювання доступу до такої інформації є надзвичайно важливою,

оскільки це забезпечує правову впорядкованість і захищає права осіб та організацій.

Різні категорії інформації з обмеженим доступом, такі як конфіденційна, таємна та службова, визначаються законодавством та волями власників або уповноважених осіб. Захист конфіденційної інформації забезпечується не природними характеристиками цієї інформації, а завдяки правовому режиму, який встановлює правила доступу та обмежує можливість її розголошення. Це робить важливим розуміння та чітке визначення цих понять в правових документах для створення ефективних механізмів захисту конфіденційної інформації та забезпечення безпеки суспільства в цілому.

РОЗДІЛ 2. АНАЛІЗ ОХОРОНИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В ПЕРІОД АТО ТА ВІЙСЬКОВОГО СТАНУ

2.1. Обмеження права на доступ до публічної інформації в умовах АТО та воєнного стану

У контексті воєнного стану важливо забезпечити оперативне та достовірне інформування громадян, однак необхідно зберігати баланс між правом доступу до публічної інформації та національною безпекою, а також правами та життям людей. Стандарти ООН, зокрема, Глобальна декларація прав людини, встановлюють, що обмеження прав і свобод може бути лише законним та обґрунтованим за метою захисту інших прав та загального добробуту в демократичному суспільстві [20].

У зв'язку з введенням воєнного стану, Україна тимчасово змінює свої зобов'язання відповідно до Європейської конвенції про захист прав людини, зокрема, щодо свободи вираження та доступу до інформації. Це здійснюється в межах, передбачених міжнародним правом і викликаних гостротою ситуації та потребою захисту національної безпеки в умовах воєнного або іншого серйозного загрозливого стану для країни.

Стаття 64 Конституції України перераховує права та свободи особи, які можуть бути обмежені у випадках введення воєнного стану з метою захисту національної безпеки та територіальної цілісності країни, включаючи право на доступ до інформації. Ця норма відповідає положенням частини 3 статті 34 Конституції України і частини 1 статті 8 Закону України «Про правовий режим воєнного стану».

Згідно з рішенням Конституційного Суду України у справі про постійне користування земельними ділянками від 22 вересня 2005 року № 5-рп/2005, обмеження прав та свобод означає звуження їх змісту, а саме – обмеження можливостей особи, які є необхідними для задоволення її потреб у житті та

розвитку, а також скорочення обсягу сутнісних властивостей, виражених у конкретних правах, які не є однаковими для всіх та не мають загального характеру.

У своєму Рішенні від 29 червня 2010 року №17-рп/2010, Конституційний Суд України розглянув конституційне подання Уповноваженого Верховної Ради України з прав людини про відповідність пункту 5, абзацу 8, частини 1 статті 11 Закону України «Про міліцію». Він вказав, що обмеження основних прав людини і громадянина та їх практичне втілення можливе лише за умови забезпечення передбачуваності застосування встановлених законом обмежень.

Конституційний Суд України повністю врахував критерії легітимності обмежень прав і свобод, які стосуються реалізації конституційних прав. Ці критерії він взяв із правових позицій Європейського суду з прав людини, який є ключовим засобом забезпечення законності у відносинах «людина - держава». Як зазначає професор П. Рабінович, це означає «перевірку та забезпечення справедливої балансованості між інтересами людини та інтересами (потребами) суспільства». Крім того, Суд у рішенні у справі «Young, James та Webster проти Сполученого Королівства» від 13 серпня 1981 року наголошує, що захист прав і свобод інших осіб, які також гарантуються Конвенцією, може спонукати державу до обмеження інших прав і свобод, що є важливою основою демократичного суспільства.

У Рішеннях від 1 червня 2016 року № 2-рп/2016 та від 22 травня 2018 року № 5-р/2018 Конституційний Суд України зазначив, що установлення обмежень повинно відбуватися за певними критеріями: обмеження щодо реалізації конституційних прав і свобод мають бути законними та справедливими, вони повинні бути встановлені виключно Конституцією та законами України, мати легітимну мету, бути обумовлені суспільною необхідністю для досягнення цієї мети, пропорційними та обґрунтованими. У разі обмеження конституційного права або свободи, законодавець зобов’язаний встановити таке правове регулювання, яке дозволить досягти легітимної мети з

мінімальним втручанням у реалізацію цього права або свободи і не порушувати сутність цього права.

Відповідно до пункту 3 статті 34 Конституції України, виконання прав може бути зменшене законом у відповідності із національною безпекою, територіальною цілісністю або громадським порядком для запобігання заворушенням або злочинам, захисту здоров'я населення, захисту репутації або прав інших осіб, уникнення розголошення конфіденційної інформації, а також для підтримки авторитету і безупинності судового процесу. Схоже положення відображено у пункті 1 частини 2 статті 6 Закону України «Про інформацію» від 02.10.1992 року № 2657-XII та пункті 1 частини 2 статті 6 Закону України «Про доступ до публічної інформації».

У зв'язку з збройною агресією російської федерації в Україні, оголошено воєнний стан. Згідно зі статтею 1 Закону України від 12 травня 2015 року № 389-VIII «Про правовий режим воєнного стану» [3], воєнний стан передбачає тимчасові обмеження конституційних прав і свобод громадян та юридичних осіб у зв'язку з загрозою, зазначаючи строк дії таких обмежень.

У контексті воєнного стану, процес надання або обмеження доступу до інформації стає більш складним і вимагає від посадової особи, яка відповідає за інформацію, значної уваги та відповідальності. Від її рішень щодо доступу до конкретної інформації може залежати не лише безпека людей та суверенітет держави, але й їхнє життя та здоров'я. На жаль, у встановленому законом воєнному стані, не існує прямого механізму для накладання будь-яких заборон або обмежень на виконання обов'язків розпорядників інформації, які стосуються розгляду запитів або розкриття публічної інформації.

У таких обставинах вирішення питання щодо обмеження або надання доступу до інформації за умов воєнного стану вимагає використання загального правила, яке застосовується до всіх випадків обмеження доступу до інформації. Це правило відоме як «трискладовий тест», який вимагає, щоб обмеження

доступу до конкретної інформації було обгрунтованим та допустимим згідно з усіма трьома критеріями, встановленими в пунктах 1-3 частини 2 статті 6 Закону України «Про доступ до публічної інформації». Такий підхід визначає, що якщо розпорядник інформації не може виправдати обмеження за хоча б одним із цих критеріїв, то обмеження доступу до публічної інформації вважається необґрунтованим.

Постанова Пленуму Вищого адміністративного суду України № 10 від 29 вересня 2016 року розкриває деталі процедури застосування «тесту» в контексті судової практики щодо доступу до публічної інформації [4].

Крім того, міжнародні та європейські норми у сфері доступу до інформації також визнають можливість обмеження права на отримання публічної інформації, яка має відкритий характер. Ці норми охоплюють Конвенцію про доступ до інформації, участь громадськості в процесі прийняття рішень та доступ до правосуддя у справах, пов’язаних з довкіллям, а також Рекомендацію Ради Європи №R(81)19 щодо доступу до інформації від державних органів, Конвенцію Ради Європи про доступ до офіційних документів, Йоганнесбурзькі принципи з національної безпеки, свободи висловлювання та доступу до інформації, а також «Принципи законодавства про свободу інформації» і т. д.

Рекомендація Rec (2002)2 Комітету міністрів РЄ, прийнята 21 лютого 2002 року, стосується права обмежувати доступ до офіційних документів з дотриманням критеріїв, таких як законність, необхідність в демократичному суспільстві та пропорційність до захисту національної безпеки, оборони та міжнародних відносин, а також громадської безпеки.

У випадках, коли розголошення інформації з офіційного документу може завдати шкоди захищеним інтересам, може бути відмовлено у доступі до документу, якщо суспільний інтерес у розкритті цієї інформації не переважає.

Під час дії воєнного стану в Україні були встановлені обмеження для оприлюднення певних типів інформації. Наприклад, Закон України від 12

травня 2022 року «Про внесення змін до деяких законів України щодо функціонування державної служби та місцевого самоврядування у період дії воєнного стану» [5] у пункті 10 статті 2 передбачає, що певні закони не поширюються на акти органів місцевого самоврядування та інших структур у період воєнного стану, хоча обов'язок оприлюднення певних документів зберігається.

Постанова Кабінету Міністрів України від 12 березня 2022 року № 263 надала органам виконавчої влади, державним підприємствам та іншим організаціям управління право тимчасово припиняти або обмежувати функціонування інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, а також публічних електронних реєстрів, за якими вони мають владу (п.1.4).

У зв'язку з цим були припинені роботу єдиного державного веб-порталу відкритих даних, реєстру корупціонерів, а також єдиного державного реєстру, який містить інформацію про всіх суб'єктів господарювання та інші дані. Це було зроблено для захисту життя та здоров'я суддів та учасників судового процесу та для забезпечення безпеки щодо цілісності бази даних. Повний доступ до судових рішень, зареєстрованих у Єдиному державному реєстрі судових рішень, був обмежений. Згідно з Листом Державної судової адміністрації України від 29.03.2022 року № 15-2665/22, повний доступ до Реєстру може бути відновлений для суддів, членів Вищої ради правосуддя, а доступ залишається обмеженим для працівників апарату судів, секретаріату Вищої ради правосуддя та Вищого кваліфікаційного комітету суддів, а також для суддів певних судів, чия територіальна підсудність зазнала змін.

У вересні 2022 року Мінцифри склали перелік даних, які планується приховати від загальної публіки на час тривання воєнного стану. При формуванні цього переліку були використані два основні критерії: наявність особистих даних фізичних осіб (зокрема, інформація про ФОП, які мають ділові відносини на тимчасово окупованих територіях) та наявність інформації про

конкретне місцезнаходження підприємств, які можна віднести до стратегічних об’єктів, та інформацію про осіб, які займають керівні посади в цих підприємствах. Такі заходи приймаються з метою захисту осіб, підприємств та важливих об’єктів в умовах загострення конфлікту [46].

У спільному зверненні Міністерства культури та інформаційної політики України, Міністерства оборони України та представників ЗМІ, оприлюдненому 27 квітня 2022 року [54], висловлено потребу у забезпеченні балансу між доступом представників преси до подій та безпекою держави. Зокрема, було підкреслено важливість дотримання Наказу Головнокомандувача Збройних Сил України від 3 березня 2022 року №73, що визначає процедуру допуску журналістів на військові об’єкти у районі бойових дій на час воєнного стану.

Згідно із Законом України від 24 березня 2022 року № 2160-IX [6], який доповнює Кримінальний кодекс України статтею 1142, встановлена кримінальна відповідальність за поширення інформації щодо збройних сил та їхнього руху або розміщення в Україні. Ця стаття вже втілена у законодавстві відповідно до Закону № 2178-IX від 01 квітня 2022 року, який набрав чинності 13 квітня 2022 року.

Експерти відзначають складності щодо класифікації дій за зазначеною статтею, що пояснюється нечіткістю її формулювань і відсутністю практики застосування. За словами М. Хавронюка [58], хоча ця стаття не визначає конкретних злочинів, вона може містити ознаки іншого злочину, наприклад, поширення інформації про рух або розміщення військової техніки, яка не є призначеною для бойових дій і не має озброєння; переміщення зброї, озброєння або бойових припасів з України; опис місця, де сталася ракетна або мінова атака; розташування військових формувань країни-агресора; або скупчення цивільних осіб.

Згідно з частиною 6 статті 22 Закону України «Про доступ до публічної інформації», якщо інформацію не можна надати в обумовлені строкі через непереборні обставини, допускається відстрочка у задоволенні запиту на

інформацію. Непереборні обставини включають надзвичайні та невідворотні ситуації, які об’єктивно перешкоджають виконанню зобов’язань, такі як загроза війни, збройний конфлікт, ворожі напади, загальна військова мобілізація, військові операції, оголошена або неоголошена війна та інші [56].

Радою суддів України прийнято рішення №11 від 25.03.2022 року про тимчасове відстрочення надання відповідей на запити про публічну інформацію, які надійшли після введення воєнного стану в Україні 24 лютого 2022 року. Ця відстрочка охоплює період дії воєнного стану і залежить від наслідків непереборної сили, які технічно унеможливлюють надання запитуваної інформації [49]. Наприклад, Вінницькому міському суду Вінницької області за цей період надійшло 30 запитів на публічну інформацію. Зазначене рішення про відстрочку повідомляється запитувачам у письмовій формі, де також пояснюється процедура оскарження такого рішення.

У своїх Рекомендаціях щодо додержання конституційного права на доступ до інформації, Уповноважений Верховної Ради України з прав людини зазначає, що при застосуванні відстрочки у відповіді на запит про публічну інформацію, розпорядники повинні аргументувати, які саме наслідки обмежень не дозволяють вчасно надати інформацію, і повідомляти про очікувану дату надання інформації. Важливо зазначити, що сам факт введення воєнного стану не є достатньою підставою для відстрочки у наданні відповіді на запит [42].

Хоча рішення Ради суддів спрямоване на судові органи, інші розпорядники публічної інформації також почали використовувати тимчасову відстрочку у відповіді на запити, посилаючись на загальні підстави «через військову агресію Російської Федерації проти України» та «запровадження воєнного стану». Деякі навіть відмовляють у наданні інформації, мотивуючи це тим, що збір інформації під час війни може мати ознаки диверсійної діяльності проти України, тому потрібна ретельна перевірка осіб, які збирають таку інформацію, та їхніх мети [49].

Значна кількість скарг на неправомірні дії розпорядників публічної інформації у контексті розгляду запитів і наслідуючі рішення судів на користь заявників свідчать про потребу у відкритості та прозорості владних структур. Це важливо для забезпечення відповідальності держави перед своїми громадянами. Однією з ознак демократичності держави є забезпечення права на інформацію кожної людини та громадянина.

Проте, в період воєнного стану питання обмеження доступу до публічної інформації лишається недостатньо вирішеним. Законодавство не містить чіткого переліку публічної інформації, до якої може бути обмежений доступ під час воєнного стану. Це призводить до того, що розпорядники публічної інформації можуть самостійно обмежувати доступ до неї, що в свою чергу може створювати загрозу національній безпеці та безпеці окремих осіб при розголошенні цієї інформації. Тому важливо розробити чіткі механізми та критерії для обмеження доступу до публічної інформації в період воєнного стану з урахуванням інтересів національної безпеки та безпеки громадянства.

Обмеження доступу до публічної інформації в умовах АТО та воєнного стану є складним завданням, яке вимагає уважного врахування балансу між безпекою суспільства та правом на отримання інформації. У таких критичних ситуаціях безпека країни та захист її інтересів можуть потребувати обмежень у доступі до певних видів інформації, щоб запобігти можливому використанню цієї інформації противником. Проте, ці обмеження повинні бути обґрунтованими, тимчасовими та пропорційними реальній загрозі, яка існує в даний момент, а також повинні відповідати принципам прозорості та демократії.

Для забезпечення правильного балансу між безпекою та правом на інформацію в умовах АТО та воєнного стану необхідно розробляти чіткі та прозорі механізми регулювання доступу до публічної інформації. Це означає, що потрібно встановити чіткі критерії для обмежень, які будуть базуватися на об’єктивних фактах та реальних загрозах, а також регулярно перевіряти та

оцінювати необхідність подальших обмежень. Крім цього, важливо забезпечити доступ до необхідної інформації для журналістів та громадськості, щоб забезпечити прозорість та відкритість у владі та управлінні кризовими ситуаціями.

2.2. Технічний захист інформації в сучасних інформаційних системах

Ефективна система захисту забезпечує інформаційну безпеку всієї організації, забезпечуючи доступність, цілісність та конфіденційність важливих даних. Для досягнення цього метафорично можна порівняти систему захисту зі замком, який потрібно правильно замкнути, щоб нічия не могла незаконно отримати доступ до важливої інформації.

Отже, комплекс заходів має бути спрямований на виявлення та запобігання можливим загрозам, а також на ефективне усунення наслідків недозволених дій зловмисників. Наприклад, це може включати у себе використання сучасних технологій для виявлення вразливостей інформаційних систем, встановлення спеціальних програмних заходів безпеки, навчання персоналу правилам безпеки та контроль за доступом до конфіденційних даних.

Комплексний підхід до захисту інформації включає в себе не лише технічні заходи, а й організаційні та процедурні аспекти. Наприклад, це може включати проведення аудиту інформаційної безпеки, регулярні навчання персоналу з питань безпеки, встановлення чітких правил користування системами та даними, а також використання захисту інформації на різних рівнях доступу до неї.

На сьогодні застосовуються такі стратегії для захисту інформації:

1) Організаційно-правові заходи. Це різні положення та угоди, які встановлюються при будівництві IT-інфраструктури для забезпечення безпеки даних. Це включає стандарти і міжнародні договори, а також правові механізми, що регулюють доступ до інформації та її збереження.

2) Інженерно-технічні заходи. Це основні інструменти, що відповідають за фізичну безпеку. Вони захищають від несанкціонованого доступу, перехоплення і прослуховування інформації, а також від стихійних лих і пожеж. Сюди входить контроль за діяльністю співробітників і їхнім пересуванням.

3) Криптографічні заходи. Це методи шифрування інформації під час її зберігання та передачі. Криптографія допомагає зберегти конфіденційність та цілісність даних, а також підтвердити їхню автентичність, заборонивши доступ стороннім особам.

4) Програмно-апаратні заходи. Це різні інструменти, які допомагають ідентифікувати користувачів, захищати інформацію шляхом шифрування, сповіщати про несанкціонований доступ, а також знищувати дані на носіях. Ці заходи можуть бути вбудовані у обладнання (зокрема, в різні схеми та реєстри), мати фізичну форму як електронно-механічні пристрої (наприклад, магнітні замки та камери спостереження), а також застосовуватися через спеціальне програмне забезпечення [21, с. 22-23].

Ефективний захист технічних систем інформації у сучасних комп’ютерних системах набуває великого значення під час введеного в Україні правового режиму воєнного стану з 24 лютого 2022 року. У цей період наша країна стикається зі значними загрозами для своєї безпеки та територіальної цілісності. В таких умовах ефективне управління інформацією та її захист стають ключовими елементами успішного забезпечення національної безпеки.

До технічних заходів захисту, представлених на рис. 2.1, відносять захист від несанкціонованого доступу до комп’ютерних систем, створення резервних копій важливих компонентів і систем, забезпечення альтернативного джерела електроживлення, розробку та впровадження спеціалізованих програмних і апаратних рішень тощо.

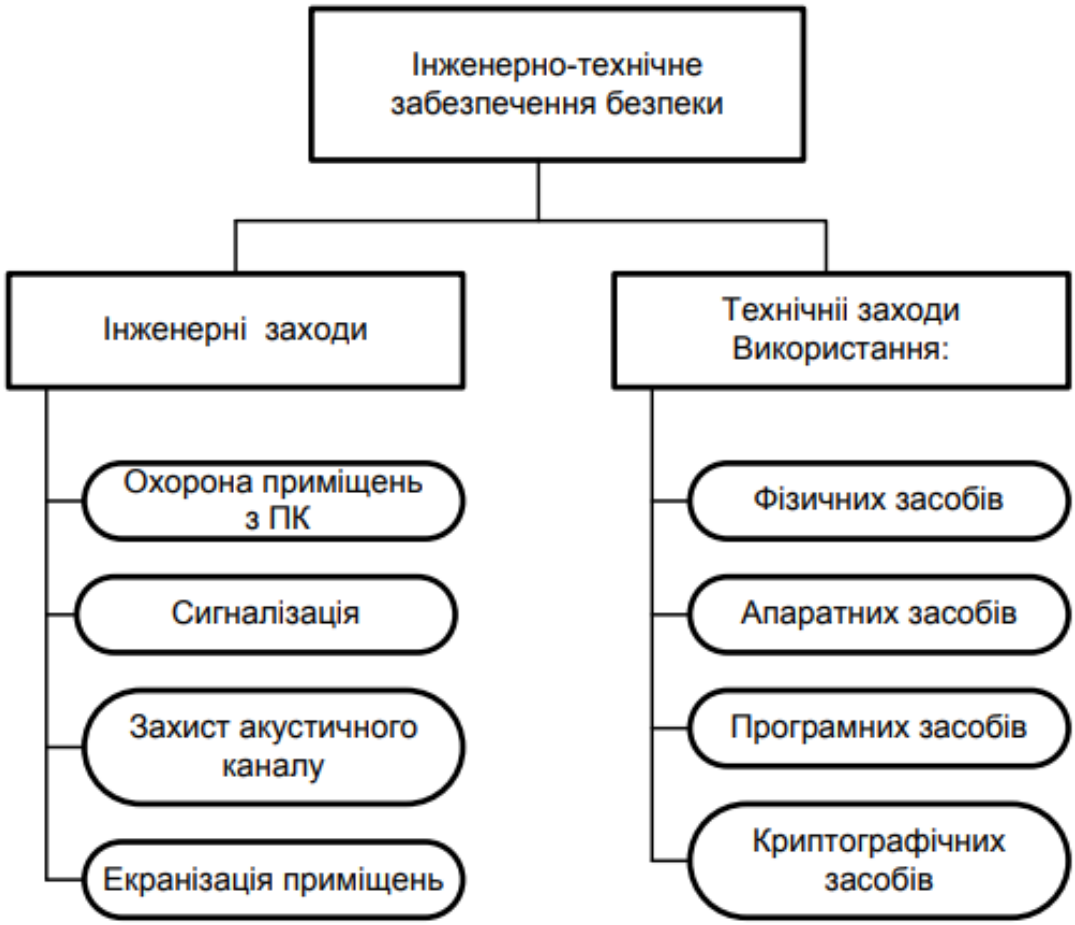

Рис. 2.1. Основні інженерно-технічні заходи захисту інформації

Джерело: сформовано на основі [29]

Фізичні заходи включають в себе різноманітні інженерні засоби, які заважають фізичному проникненню зловмисників на захищені об’єкти. Вони призначені для захисту персоналу, матеріальних цінностей, фінансів та конфіденційної інформації від незаконних дій.

Програмні заходи включають спеціальні програми, комплекси програм та системи, які призначені для захисту інформації в інформаційних системах різного призначення та для обробки даних.

Криптографічні заходи використовують математичні та алгоритмічні методи для захисту інформації під час передачі по каналах зв’язку, збереження та обробки на комп’ютерах за допомогою методів шифрування.

Технічні засоби захисту інформації включають різні механічні, електричні або електронно-механічні пристрої, а також спорудження і матеріали, що призначені для захисту від несанкціонованого доступу, викрадення інформації, попередження її втрати внаслідок порушень робочої здатності компонентів інформаційних систем, стихійних лих, саботажу та інших загроз.

Серед засобів захисту інформації з технічного погляду варто згадати:

– Засоби захисту кабельних систем. За даними досліджень, відмови у кабельних системах становлять більше половини відказів у локальних обчислювальних мережах. Ефективним методом запобігання таким відмовам є створення структурованої кабельної системи, в якій використовуються однакові кабелі для передачі даних у різних інформаційних системах, сигналів від датчиків пожежної безпеки, відеоінформації з охоронних систем, а також для локальної телефонної мережі. Поняття «структурованість» означає, що кабельну систему будинку можна розділити на різні рівні залежно від її призначення та розташування. Для надійної структурованої кабельної системи слід дотримуватися міжнародних стандартів;

– Засоби захисту системи електропостачання. Дослідження компанії Best Power виявили, що на кожному комп’ютері в середньому відбуваються 289 випадків порушень електропостачання щороку, що значно впливає на роботу. Установка джерел безперебійного живлення є найефективнішим способом уникнення втрат даних під час тимчасових відключень електроенергії або стрибків напруги в електромережі. Різноманітність технічних і експлуатаційних характеристик дозволяє вибрати засіб, який відповідає вимогам. За вимоги підвищеної надійності інформаційних систем може бути використано аварійний генератор або резервні лінії електропостачання, підключені до різних підстанцій;

– Засоби архівації та дублювання інформації є важливими елементами забезпечення безпеки даних та їх надійності. При обробці значних

обсягів інформації, доцільно використовувати спеціалізовані сервери для архівації даних, які забезпечують їх ефективне зберігання та організацію доступу до них. Для архівування важливої інформації рекомендується використовувати спеціально обладнані приміщення з відповідними системами безпеки та захисту. У разі пожежі або інших непередбачених ситуацій, варто мати дублікати найбільш цінних архівних даних, розміщені в іншому безпечному місці. Це може бути інший будинок, район чи навіть місто, що гарантує збереження інформації навіть у випадку знищення основного архіву;

– Засоби захисту від відпливу інформації по різних фізичних полях також відіграють важливу роль у забезпеченні конфіденційності та безпеки даних. Це включає в себе заходи для виявлення прослуховувальних пристроїв, електромагнітне екранування пристроїв та приміщень, а також використання радіотехнічного маскування за допомогою широкосмугових генераторів шумів. Такі заходи спрямовані на запобігання несанкціонованого доступу до інформації та захист конфіденційності даних від зовнішніх втручань [29].

До засобів технічного захисту інформації відносяться матеріали, які гарантують безпеку зберігання та перевезення носіїв інформації та захищають їх від несанкціонованого копіювання. Зазвичай це спеціальні тонкоплівкові матеріали зі змінною кольоровою гамою або голографічні мітки, які наносяться на документи, предмети (включаючи комп’ютерну техніку) та дозволяють перевіряти автентичність об’єкта та контролювати доступ до нього.

Зазвичай технічні засоби захисту використовуються разом із програмними. Програмні засоби захисту забезпечують ідентифікацію та аутентифікацію користувачів, розмежування доступу до ресурсів згідно з їх повноваженнями, фіксацію подій в інформаційних системах, шифрування інформації, захист від комп’ютерних вірусів та інші заходи.

Під час захисту від несанкціонованого доступу (НСД) за допомогою програмних засобів здійснюється:

– ідентифікація об’єктів і суб’єктів, що включає визначення та перевірку ідентичності осіб або систем, які намагаються отримати доступ;

– розмежування доступу до інформаційних ресурсів, що означає встановлення прав і обмежень доступу до різних частин системи чи даних залежно від ідентифікації особи або системи;

– контроль і реєстрація дій з інформацією і програмами, що включає моніторинг та фіксацію всіх операцій з даними та програмами для подальшого аналізу і виявлення можливих вторгнень чи незвичайної активності.

Захист інформації від копіювання забезпечується виконанням таких функцій:

– ідентифікація середовища, з якого буде запускатись програма, що означає перевірку середовища та переконання, що воно є довіреним і не має ознак несанкціонованості;

– аутентифікація середовища, із якого запущена програма, що включає перевірку відповідності інформації про середовище до відомих параметрів та ідентифікаторів;

– реакція на запуск із несанкціонованого середовища, що означає вживання заходів для зупинення або ускладнення виконання програми, яка запускається з недовіреного середовища;

– реєстрація санкціонованого копіювання, що включає відслідковування та фіксацію всіх актів легального копіювання для контролю та аналізу;

– протидія вивченню алгоритмів роботи системи, що означає використання захисту від аналізу та розкриття внутрішньої структури програм чи системи для недозволених осіб чи програм [25].

Комп’ютерна стеганографія базується на двох принципах, які становлять її основу. По-перше, ця техніка дозволяє змінювати аудіо- та відеофайли, а також файли з оцифрованими зображеннями, зберігаючи при цьому їхню

функціональність. По-друге, мишеність людини розрізняти дрібні зміни у кольорі або звуці обмежена.

Методи стеганографії надають можливість приховувати конфіденційну інформацію, заміняючи її несуттєвими частинами даних. Зазвичай ця техніка використовується для створення цифрових водяних знаків, які можна розпізнати лише за допомогою спеціального програмного забезпечення. Цифрові водяні знаки записуються як псевдовипадкові послідовності шумових сигналів, що генеруються на основі секретних ключів.

Щодо впровадження засобів програмно-технічного захисту в інформаційних системах, варто розглянути два основні способи:

1) Додатковий захист – це коли засоби захисту діють як доповнення до основних програмних і апаратних компонентів комп’ютерної системи.

2) Вбудований захист – коли механізми захисту реалізовані у вигляді окремих компонентів ІС або вбудовані у різні компоненти системи, що забезпечує більш високий рівень захисту від різних загроз [29].

Перший спосіб захисту, що є більш гнучким, дозволяє додавати та вилучати механізми захисту відповідно до потреб, але при цьому можуть виникати проблеми зі сумісністю між засобами захисту та програмно-технічним комплексом інформаційних систем. У вбудованому захисті, який вважається більш надійним і оптимальним, складніше вносити зміни, що робить його менш гнучким. Ці два підходи до захисту поєднуються в реальних системах, щоб забезпечити оптимальний рівень безпеки.

Технічний захист інформації у сучасних інформаційних системах стає все важливішою складовою для забезпечення безпеки та конфіденційності даних. Оскільки загрози в сфері кібербезпеки стають все складнішими, необхідно постійно удосконалювати заходи захисту. Це охоплює різні види кібератак, витоків даних, шпигунства, вторгнень та інші форми агресії. Тому для успішного управління цими загрозами важливо мати глибокі знання та ефективні стратегії для їх уникнення та протидії.

Системи технічного захисту інформації повинні бути адаптовані до конкретних потреб та характеристик організації, щоб ефективно захищати її дані від загроз. Це означає використання передових методів шифрування для забезпечення конфіденційності та цілісності інформації. Також потрібно звернути увагу на безпеку мережі, використовуючи механізми інтегрованого контролю доступу та мережеві файрволи для фільтрації трафіку та виявлення загроз.

Регулярне оновлення програмного та апаратного забезпечення є ключовим аспектом забезпечення безпеки. Постійні патчі, виправлення вразливостей і оновлення системних компонентів дозволяють уникнути використання вразливостей зловмисниками. Крім того, важливо мати впроваджені системи виявлення та відновлення після інцидентів, які дозволять оперативно реагувати на потенційні загрози, відновлюючи роботу системи та забезпечуючи безпеку даних. Поєднання ретельного планування, реалізації та підтримки технічних заходів захисту дозволить організації забезпечивши надійний захист важливих даних від несанкціонованого доступу та витоку.

2.3. Захист інформації з обмеженим доступом від витоку та несанкціонованого доступу

Ще до початку війни, українські інформаційні системи були мішенню сильних атак російських хакерів. Після початку повномасштабної відкритої агресії з боку РФ, інтенсивність кібератак не тільки не зменшилася, але й зростає. Російські військові хакери активно намагаються отримати доступ до особистих даних українців і завдати шкоди нашим інформаційним системам. Ці атаки вплітаються в загальну стратегію агресії РФ та координуються з атаками на критичну інфраструктуру.

Потенційний витік особистих даних українців становить серйозну загрозу, оскільки військові та спецслужби ворога можуть використати ці дані

для агресивних дій проти населення, зокрема на тимчасово окупованих територіях, де люди є найбільш вразливими. Крім того, витік чутливих даних може націлитися на роботу органів влади та критичну інфраструктуру, і його можуть використати вороги для подальших атак та дестабілізації ситуації.

Отже, під час війни та протистояння російській агресії, захист даних у інформаційних системах стає критично важливим завданням, що вимагає негайних та ефективних заходів для забезпечення безпеки та конфіденційності інформації [15].

Один з найширше поширених і найрізноманітніших методів впливу на інформаційну систему – це несанкціонований доступ. Цей вид атаки може спричинити шкоду будь-якій частині інформаційної безпеки, оскільки передбачає незаконне отримання конфіденційної інформації людиною, яка не має права доступу до неї [61].

Канали несанкціонованого доступу можна класифікувати за компонентами автоматизованих інформаційних систем:

– через людину: включає розкрадання носіїв інформації, зчитування інформації з екрана або клавіатури, отримання інформації з виходу друку.

– через програми: охоплює перехоплення паролів, декодування зашифрованої інформації, відтворення інформації з носія.

– через апаратуру: включає підключення спеціально розроблених апаратних засобів для отримання доступу до інформації, перехоплення побічних електромагнітних випромінювань від апаратури, ліній зв’язку, електромереж тощо [27].

Типи несанкціонованого доступу поділяються на два: організаційні та технічні, і вони використовують як законні, так і незаконні методи.

Організаційні канали можуть мати різноманітні форми. Вони зазвичай базуються на створенні законних відносин між зловмисником і фірмою або її працівником, що дозволяє здійснювати незаконний доступ до цікавої інформації [44].

Існує безліч способів реалізації організаційних каналів витоку інформації. Це може включати залучення зловмисника до роботи або співпрацю з підприємством як партнера, посередника або клієнта. Також можуть використовуватись методи пошуку та заохочення працівників, які допомагають зловмиснику, працюючи на цікавому підприємстві [45]. До інших методів належать використання помилкових або спровокованих дій персоналу, а також погрози, крадіжки документів, дисків, комп'ютерів і т. д.

Прогнозування організаційних каналів є важким завданням, оскільки вони часто вибираються або генеруються зловмисником залежно від його навичок і умов. Щоб виявити втручання через організаційні канали, потрібні серйозні пошукові і аналітичні дії.

Технічні канали витоку інформації виникають без прямого контакту зловмисника з персоналом підприємства або документами. Зловмисник використовує спеціальні технічні засоби промислового шпигунства [44]. Він аналізує фізичні поля та випромінювання, які виникають під час роботи обчислювальної техніки та інших офісних пристроїв. Це дозволяє перехоплювати звукову або візуальну інформацію. Технічний канал витоку є фізичним шляхом передачі інформації від джерела до зловмисника і включає електромагнітний, акустичний, візуально-оптичний та інші типи каналів [59].

Захист від несанкціонованого доступу є одним з найбільш актуальних завдань у сфері кіберзахисту. Російські військові хакери постійно намагаються отримати доступ до облікових записів для подальших атак. Вони уважно стежать за українськими новинами та надсилають фішингові листи, в яких імітується державна підтримка або цифрові послуги, використовуючи актуальні події та болючі питання, такі як війна та втрати українців, для досягнення своїх цілей [57].

У період війни необхідність виконання стандартів захисту інформації залишається незмінною. Зокрема, державні інформаційні ресурси або інформація з обмеженим доступом, які мають бути захищені відповідно до

закону, повинні оброблятися у системі, що відповідає комплексній системі захисту інформації (КСЗІ) з підтвердженою відповідністю. Відповідність КСЗІ підтверджується результатами державної експертизи, проведеної відповідно до вимог законодавства і галузевих стандартів інформаційної безпеки [15].

Комплексна система захисту інформації (КСЗІ) включає в себе технічні та організаційні заходи захисту, які реалізуються як у інформаційній системі власника за допомогою технічних засобів та налаштувань, так і у власника установи через відповідні розпорядження, плани, інструкції та методики тощо.

Для захисту інформаційних систем, які не обробляють інформацію з обмеженим доступом, але вимагають захисту відповідно до українського законодавства, може бути також використана альтернативна система інформаційної безпеки згідно з європейськими стандартами серії ISO/IEC 27.

Процес створення КСЗІ та отримання атестата відповідності залишається незмінним навіть під час воєнного стану. Цю роботу можуть проводити як спеціалізовані організації, так і компанії з відповідними фахівцями. Головне, щоб побудована система відповідала всім вимогам законодавства і була здатна отримати атестат відповідності [15].

Атестат відповідності для КСЗІ є результатом державної експертизи у сфері технічного захисту інформації, яка проводиться відповідно до «Положення про державну експертизу у сфері технічного захисту інформації». Ця процедура регулюється наказом Адміністрації Держспецзв’язку та включає в себе умови та терміни проведення робіт, які можуть варіюватися в залежності від складності системи, досвіду експертів, якості побудови КСЗІ та інших чинників. Зазвичай, середній час проведення експертизи КСЗІ інформаційної системи становить близько трьох місяців. При позитивних результатів експертизи атестат відповідності КСЗІ реєструється Адміністрацією Держспецзв’язку [15].

У певних випадках компанія може створити систему інформаційної безпеки з урахуванням європейських стандартів ISO/IEC 27 серії та вимог

Закону України «Про захист інформації в інформаційно-комунікаційних системах».

Заходи захисту від руйнування інформації розрізняються через широкий спектр причин, які можуть спричинити її втрату або пошкодження. Серед цих причин можна виділити несанкціоновані дії, помилки програмного забезпечення та обладнання, а також комп'ютерні віруси. Для забезпечення надійного захисту передбачаються обов'язкові страхувальні заходи, спрямовані на попередження та профілактику можливих причин руйнування інформації. У таких ситуаціях програмні засоби захисту можуть бути як спеціалізованими, так і універсальними, відповідно до потреб та специфіки конкретної ситуації.

Криптографічні заходи захисту полягають у використанні спеціальних пристроїв і програм, а також виконанні відповідних дій, щоб зробити передаваний сигнал абсолютно незрозумілим для сторонніх осіб. Основна мета таких заходів - забезпечити такий рівень захисту інформації, за якого вона після перехоплення і обробки може бути розшифрована тільки протягом часу, необхідного для втрати своєї цінності. Для цього використовуються різноманітні спеціальні засоби шифрування, які можуть застосовуватися до документів, мови, телеграфних повідомлень та іншого виду інформації.

Забезпечення захисту конфіденційної інформації від витоку та несанкціонованого доступу є надзвичайно актуальною задачею у сучасному світі, особливо у контексті зростаючої складності та кількості кіберзагроз, зокрема під час воєнних дій. Поширення кібератак, витоків даних та несанкціонованих доступів необхідно ефективно контролювати та запобігати, особливо в галузях, де зберігається важлива інформація, така як державні та корпоративні дані, особисті дані клієнтів та інше. Щоб забезпечити ефективний захист інформації, потрібен комплексний підхід, який включає в себе не лише використання сучасних технологій, а й організаційні стратегії та процедури контролю.

У сучасному світі методи захисту інформації включають в себе передові

технології шифрування, системи моніторингу та виявлення вторгнень, захист від вірусів та інших загроз, а також регулярні аудити та тестування на проникнення. Проте, разом з цими технічними заходами, необхідно надавати належну увагу навчанню персоналу правильній культурі безпеки, встановлювати строгі політики доступу та реагувати на будь-які інциденти швидко та ефективно. Лише поєднання передових технологій і відповідних організаційних заходів може гарантувати надійний захист інформації та запобігати негативним наслідкам від можливих загроз.

Отже, захист інформації з обмеженим доступом від витоку та несанкціонованого доступу є надзвичайно важливим завданням у сучасному цифровому середовищі. Ця проблема стає ще актуальнішою в контексті зростаючих кіберзагроз та швидкого розвитку технологій. Ефективний захист інформації потребує комплексного підходу, що включає в себе використання передових технологій, строгі політики безпеки, ретельний моніторинг та аналіз загроз, а також постійне навчання персоналу. Тільки поєднання цих факторів може забезпечити надійний захист конфіденційної інформації та уникнення негативних наслідків від потенційних атак інформаційної безпеки.

Такий підхід також передбачає постійне оновлення заходів захисту відповідно до змін у кіберзагрозах та вимогах безпеки даних. Регулярні аудити та тестування на проникнення є необхідними етапами для виявлення слабких місць інформаційної системи та їх виправлення. Крім того, створення культури безпеки серед персоналу, включаючи навчання щодо виявлення фішингових атак та інших соціально-інженерних методів, грає ключову роль у запобіганні несанкціонованому доступу. Організації також повинні мати чітку стратегію реагування на інциденти безпеки, включаючи швидке виявлення, ізоляцію та відновлення інформаційних ресурсів. В цілому, захист інформації з обмеженим доступом вимагає поєднання технологій, освіти та стратегічного планування для ефективного захисту конфіденційних даних у сучасному цифровому середовищі

Висновки до другого розділу

Тому, обмеження доступу до публічної інформації під час АТО та воєнного стану становить складне етичне та юридичне питання, яке вимагає уважного узгодження між захистом національної безпеки та правом людини на інформацію. Необхідність таких обмежень обумовлена потребою уникнення розголошення конфіденційної інформації, яка може нашкодити національній безпеці та військовій справі. Однак, важливо, щоб ці обмеження були обґрунтованими, тимчасовими та пропорційними, і дотримувалися законодавства, у той час забезпечуючи засади демократії та прав людини. Узагальнюючи, суспільство стоїть перед важливим завданням забезпечити збалансований підхід до доступу до інформації під час АТО та воєнного стану, розробляючи чіткі та прозорі механізми контролю доступу до публічної інформації та забезпечуючи захист національної безпеки, а також забезпечуючи права громадян на інформацію та прозорість діяльності державних органів.

Забезпечення безпеки інформації у сучасних інформаційних системах через технічні заходи має надзвичайну вагу для збереження даних у захищеному та конфіденційному режимі. З розвитком кібербезпеки стає все складніше захищати дані, тому необхідно постійно удосконалювати технічні заходи для ефективного протистояння різноманітним загрозам в онлайн середовищі. Важливо мати на увазі різноманітність загроз, які включають кібератаки, витоки інформації, шпигунство та інші види кіберзлочинності. Для надійного технічного захисту інформації використання передових методів шифрування, захист мережі, регулярне оновлення програмного та апаратного забезпечення, а також впровадження систем виявлення та реагування на інциденти є критично важливими. Тільки комплексний підхід до захисту даних може забезпечити ефективний захист від загроз та зберегти безпеку та конфіденційність інформаційних систем у сучасному цифровому середовищі.

Забезпечення безпеки інформації з обмеженим доступом від витоку та несанкціонованого доступу стає критично важливим завданням у сучасному

цифровому світі. Розповсюдження кіберзагроз та злочинної діяльності в Інтернеті вимагає комплексного підходу до захисту даних, включаючи технічні та організаційні заходи. Ефективний захист інформації потребує постійного вдосконалення технологій, навчання персоналу та впровадження строгих політик безпеки. Організації мають активно протидіяти кіберзлочинцям, регулярно аудитувати системи, розробляти та впроваджувати плани реагування на інциденти та підтримувати високий рівень обізнаності щодо сучасних загроз. Лише поєднання технологій, відповідних стратегій та навичок управління ризиками може забезпечити ефективний захист інформації з обмеженим доступом, що є критично важливим для забезпечення безпеки та довіри у цифровому середовищі.

РОЗДІЛ 3. ПЕРСПЕКТИВИ ОХОРОНИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В ПЕРІОД АТО ТА ВІЙСЬКОВОГО СТАНУ

3.1. Міжнародний досвід охорони інформації з обмеженим доступом

Розглянення зарубіжного досвіду у сфері охорони інформації з обмеженим доступом є надзвичайно важливим для України, яка прагне до інтеграції в Європейське Співтовариство. Особливу увагу слід приділити приведенню чинного законодавства до вимог європейських стандартів. Це передбачає прийняття нових законів, удосконалення та доопрацювання чинних законів на основі передового досвіду зарубіжних країн, з урахуванням національних особливостей України. В сучасних умовах, які важливі для міждержавного співробітництва з країнами, що межують, актуальним стає питання підвищення ефективності захисту державних таємниць, при цьому необхідно скоротити обсяг інформації, що включається до цієї категорії. Завданням держав є розробка розумного механізму захисту різних типів інформації та встановлення меж дії інститутів таємниць.

Наразі, США мають один з найвищих рівнів законодавчого захисту інформації, що виявляється у наявності понад 500 законодавчих актів, спрямованих на цю проблематику. Один з ключових стандартів цього захисту – «Критерії оцінювання довірених комп'ютерних систем», що встановлений Міністерством оборони США. Відомий як «Помаранчева книга» через колір обкладинки, цей стандарт був вперше опублікований у серпні 1983 року. Він визначає не лише безпеку, але й рівень довіри до системи, що є ключовим для забезпечення ефективності та надійності інформаційних систем. «Помаранчева книга» є основним стандартом, який використовується в американському бізнесі і закладений в систему колективної безпеки, впровадженої ще у 90-х роках XX століття. Державний департамент та понад 500 американських

корпорацій регулярно обмінюються інформацією щодо загроз з метою захисту інтересів громадян та підприємництва в країні.

Понад 70% американських підприємців шукають підтримку від відповідних агентств з охорони та детективної діяльності. Успішні підприємства співпрацюють з такими агентствами, щоб зменшити економічні ризики та, в результаті, можуть створювати власні служби безпеки. В США, особливість таких служб полягає у привласненні співробітників Федерального Бюро Розслідувань (ФБР) та Центральної Розвідувальної Агенції (ЦРУ), що дозволяє використовувати їхні знання та досвід для створення спеціалізованих відділів з безпеки. Це включає в себе формування власних структур, де працюють експерти з безпеки, що забезпечує використання внутрішніх ресурсів та бази даних для захисту підприємства. Такий підхід дозволяє державі зберегти свою незалежність від виробничих процесів фірм та зменшує можливість втрат для підприємства.

Розмежування доступу до даних, які зберігаються в пам’яті електронно-обчислювальних машин (ЕОМ), є однією з актуальних проблем. Особливо важливо забезпечити, щоб лише авторизовані особи мали доступ до конфіденційної інформації. Технології автентифікації та шифрування відіграють ключову роль у цьому процесі, надаючи можливість забезпечувати безпеку даних у цифровому середовищі. Крім того, розробка і впровадження строгих політик безпеки та навчання персоналу щодо правильного використання технологій захисту є необхідними кроками для ефективного управління доступом до інформації.

Особливу увагу слід звернути на інтелектуальні карти як ефективний засіб контролю доступу. Однією з передових технологій в цій галузі є Expocard, розроблена американською компанією CHESEPEAKE. Ця карта, розміром як кредитна, містить вбудований комп’ютерний чіп [43], що значно покращує її функціональність порівняно з картками із магнітними мітками. Інформаційна потужність Expocard перевищує магнітні карти приблизно у 500 разів, що

сприяє швидкому проходженню відвідувачів у системах з дозволеним доступом.

У такій пластиковій карті вбудована напівпровідникова пам’ять для зберігання даних про користувача. Для використання Expocard використовуються зчитувальні / записуючі пристрої, що дозволяють не лише читати інформацію, збережену в картці, але і вносити додаткові дані за потребою. Expocard є одним із багатьох видів карток, що розроблені CHESEPEAKE. Ця технологія застосовується у сферах контролю безпеки мереж, будівель, охорони парковок, а також для обліку банківських рахунків, оплати телефонних розмов та інших цілей. Важливо також відзначити, що витрати на експлуатацію Expocard є низькими, що додатково підсилює її ефективність та привабливість для різних сфер використання.

В галузі підготовки кадрів з питань захисту інформації, Сполучені Штати відзначаються своїм передовим досвідом. У цій справі приймаються відповідні рішення на рівні держави, а служби безпеки знаходяться під контролем президента, що робить їхній позитивний досвід цікавим для використання в нашій країні [26].

Основуючись на досвіді Німеччини у сфері організації системи захисту інформації з обмеженим доступом, яка є однією з найбільш розвинених країн Західної Європи в галузі інформаційної безпеки, варто зазначити, що система захисту інформації в цій країні виросла впродовж XIX століття та особливо активно стала формуватися в XX столітті. З середини XX століття Німеччина докладала багато зусиль у захист особистих даних і у 1970 році прийняла перший у світі закон, що регулював цю сферу, ініційований федеральною землею Гесен і згодом підтриманий іншими федеральними землями [20].

На рівні підприємств також відбувається захист персональних даних, навіть у невеликих підприємствах з невеликою кількістю працівників, де упроваджується посада відповідального за захист особистих даних..

В Німеччині приділяється значна увага технічному захисту інформації, що виявляється у створенні федерального відомства для забезпечення безпеки в галузі інформаційної техніки вже у 1993 році. Це відомство не лише забезпечує технічний захист інформації, але й надає консультації громадянам з цього питання, а також відповідає за сертифікацію та стандартизацію засобів безпеки. Крім того, воно активно поширює усвідомлення необхідності захисту інформації на підприємствах.

Далі, розглянемо досвід Великої Британії у сфері захисту інформації на підприємствах та інших суб'єктах господарювання. Оскільки Велика Британія та США мають схожість у соціальній, правовій та економічній системах, можна відзначити схожі підходи до забезпечення безпеки бізнесу в цих країнах.

У цьому контексті важливо відзначити роль приватних агентств, які виконують специфічні завдання, що ставлять перед ними суб'єкти бізнесу, і які часто не потрапляють у компетенцію правоохоронних органів через їх приватний характер або відсутність визначення в законодавстві [31]. Особливо це стосується приватних розшукових агентств, які обслуговують не лише суб'єктів підприємництва, але й приватних осіб у справах їхнього приватного життя. Зауважимо, що кількість таких агентств постійно зростає, оскільки попит на їх послуги зростає як серед бізнесменів, так і серед приватних осіб.

Уряд Великої Британії приділяв увагу проблемам захисту інформації задовго до інших європейських країн, що сприяло накопиченню значного досвіду у цій області. Проте, важливо відзначити, що система захисту інформації у Великій Британії має свої недоліки, зокрема у сфері правового забезпечення. Наприклад, базується вона на законах «Про державні документи» та «Про державну таємницю», а для захисту решти інформації використовуються різноманітні правові акти, включаючи кримінальний кодекс. Особливо важливою є тема захисту комерційної таємниці, яка залишається на відповідальності самої організації через необхідність укладання спеціальних договорів зі співробітниками.

У той же час, Франція до недавнього часу не відрізнялася особливими зусиллями у формуванні системи безпеки бізнесу порівняно з іншими європейськими країнами. Однак, останні роки принесли зміни, і власники підприємств у промисловості, торгівлі, фінансах та кредитах стали активніше залучати приватні детективно-охоронні агентства для посилення системи безпеки. Ця практика також стала поширеною серед інших сфер, таких як страхування, нотаріат, адвокатура, освітні заклади та інші [47].

Експерти приватних агентств, співпрацюючи з органами правопорядку, зосереджують увагу на різних аспектах безпеки, таких як боротьба з порушеннями торгових марок, виявлення недобросовісної конкуренції, протидія промисловому та контршпигунству, а також впровадження заходів безпеки у фінансовій сфері.

Зацікавленість Франції у сфері безпеки персональних комп'ютерів та боротьби з комп'ютерною злочинністю виявляється через розгортання десятків правових актів, що детально регулюють взаємодію суб'єктів інформаційної сфери, правила обміну інформацією та доступ до інформаційних систем і баз даних.

Засоби захисту інформації в підприємницькому секторі Японії та Китаю також є об'єктом підвищеного інтересу через їх відомість у розробці та впровадженні передових технологій захисту, що допомагає підтримувати високий рівень безпеки та конфіденційності інформації в цих регіонах.

Промислово розвинені країни, зокрема Японія, мають значний досвід у законодавчому регулюванні справ у сфері захисту комерційних таємниць. Шляхом укладення договору роботодавець може забезпечити зобов'язання своїх працівників зберігати конфіденційну інформацію, яка їм довірена протягом періоду роботи. Угода про службові винаходи, розроблена патентним відомством, містить положення, що передбачає збереження конфіденційності винаходів та матеріалів, які стосуються діяльності компанії, на необхідний термін. Також можливе обмеження дій працівників після закінчення їхньої

роботи протягом певного періоду. Окрім цього, велика увага приділяється захисту корпоративних секретів під час конфіденційних відносин [41].

У сучасному світі Китай активно розвивається та виявляє лідерські позиції в галузі інформаційного протиборства і захисту інформації у підприємництві. У 2001 році Китай прийняв положення «Про охорону комп'ютерних програм», що стало першим кроком у регулюванні безпеки комп'ютерних систем. Закон «Про авторські права» в 2003 році став ще одним важливим кроком, де комп'ютерні програми вперше були визнані об'єктами авторського права. Органи громадської безпеки несуть відповідальність за забезпечення інформаційної безпеки в Китаї [36].

Отже, найбільш яскраві приклади організації системи захисту інформації в різних країнах світу підкреслюють як переваги, так і недоліки цих підходів. Україні слід уважно вивчати досвід відомих держав у цьому напрямі. В результаті аналізу міжнародного досвіду охорони інформації з обмеженим доступом виявлено, що впровадження ефективної системи захисту конфіденційної інформації є ключовим завданням для будь-якої організації чи установи.

Комплексні стратегії, які поєднують сучасні технології, відповідні правові норми та стандарти, дозволяють ефективно протистояти загрозам від зловмисників та забезпечувати надійність інформаційних потоків. Дослідження підтверджують, що постійне підвищення кваліфікації персоналу, застосування передових технологій шифрування та моніторингу, а також впровадження строгих процедур контролю доступу є важливими компонентами успішної системи охорони інформації з обмеженим доступом.

3.2. Шляхи удосконалення організації охорони інформації з обмеженим доступом в контексті російсько-української війни

Захист інформації під час воєнного стану включає розвиток та впровадження передових технологій захисту інформації, в тому числі криптографічних методів та систем безпеки мереж. Крім цього, надзвичайно важливе навчання військових та цивільних працівників з питань інформаційної безпеки та кіберзахисту. Також потрібно мати ефективний механізм контролю за поширенням дезінформації та пропаганди.

У 2022 році Держспецзв'язок активно працює над впровадженням рішень від Hideez та Yubikey у багатьох державних установах. Hideez та Yubikey - це вироби американських компаній для автентифікації без пароля. Особливо цікаво, що Hideez має українське коріння. Використання рішень Hideez та Yubikey забезпечує надійний захист від кібератак, таких як фішинг, спуфінг та атаки посередників, завдяки застосуванню альтернативних методів автентифікації замість пароля. Також вони надають можливість віддаленого управління обліковими записами, пристроями та методами аутентифікації, що є важливим для доступу до важливих сервісів і робочих станцій [57].

Захист інформаційних ресурсів на підприємстві або в організації означає оптимізацію методів та технічних засобів захисту даних. Управління цими ресурсами взаємозв'язане з масштабами діяльності підприємства. Інформаційна потужність підприємства, яка описує рівень ефективності використання інформаційних активів, є ключовим фактором для збільшення конкурентоспроможності [25].

Для успішного управління інформаційними ресурсами потрібно оптимізувати методи захисту інформації та використовувати технічні засоби, що утворюють її структуру. Однак для досягнення максимальної ефективності необхідно також враховувати інформаційну потужність підприємства.

Інформаційна потужність грає ключову роль у визначенні ефективності використання доступних інформаційних ресурсів для підвищення конкурентоспроможності. Ця ефективність досягається через максимальне використання можливостей і функціоналу інформаційних систем, розробку та впровадження бізнес-рішень, які оптимізовані для конкретних завдань підприємства.

Наприклад, компанія може знизити витрати на захист інформації, використовуючи програмні та технічні рішення, такі як UTM-системи та системи виявлення вторгнень. Це дозволяє ефективно контролювати мережу та вчасно виявляти потенційні загрози. Такий підхід сприяє підвищенню інформаційної потужності підприємства, що забезпечує йому конкурентні переваги та стійкість проти кібератак.

Існують дві основні категорії вразливостей інформаційних систем, які можуть стати об’єктом атак зловмисників: людський фактор користувача та незахищеність чи несправність програмного та системного забезпечення. Перша категорія, а саме людський фактор, охоплює помилки та недбалість користувачів, що може призвести до несанкціонованого доступу через неправильне використання паролів, відкриття шахрайських посилань у електронних листах або надання доступу до конфіденційних даних під час соціальної інженерії. Друга категорія вразливостей, а саме незахищеність програмного та системного забезпечення, включає різноманітні уразливості у програмах, операційних системах та мережевих протоколах. Ці вразливості можуть бути використані для впровадження шкідливого коду, витоку даних або виконання інших видів кібератак. Додатковою загрозою є те, що зловмисники постійно шукають нові методи атак та використовують розвиток технологій для підвищення складності своїх нападів.

Щоб запобігти таким загрозам, необхідно постійно навчати користувачів щодо безпеки в мережі, використовувати надійне програмне забезпечення з регулярними оновленнями, а також встановлювати та налаштовувати захисні

механізми, такі як брандмауери та антивіруси. Лише комплексний підхід до захисту інформаційної системи здатний зменшити ризики та забезпечити надійний рівень безпеки даних. Отже, при проектуванні системи захисту необхідно обов’язково враховувати ці аспекти, будуючи її з урахуванням двох напрямків. На основі проведених досліджень було розроблено наступну концепцію системи захисту (рис. 3.1).

Розроблена концепція представляє собою комплекс заходів, спрямованих на виявлення та запобігання атакам, і базується на двох основних принципах: організаційних та програмно-технічних заходах безпеки.

Організаційні заходи безпеки включають у себе контроль доступу до ресурсів інформаційної системи за допомогою регулювання та політик доступу. Це охоплює керування правами доступу, моніторинг діяльності користувачів та забезпечення внутрішньої безпеки організації.

Програмно-технічні заходи безпеки включають в себе використання спеціальних рішень та технологій, таких як системи виявлення вторгнень (IDS), системи запобігання вторгнень (IPS), UTM-системи та інші. Ці інструменти дозволяють виявляти аномалії в мережі, блокувати небезпечний трафік та забезпечувати безпеку даних.

Система захисту інформації функціонує на трьох основних етапах: передбаченні (перед атакою), реагуванні (під час атаки) та відновленні (після атаки). Це означає вчасне виявлення можливих загроз, оперативну реакцію на інциденти та відновлення нормального функціонування систем після виникнення проблеми.

Рис. 3.1. Концепція системи захисту інформації для створення КСЗІ

Джерело: сформовано на основі [14, с. 56-60]

Ця стратегія дозволяє ефективно впроваджувати та керувати заходами з інформаційної безпеки на підприємстві, забезпечуючи високий рівень захисту даних та інформаційних ресурсів в умовах зростаючих кіберзагроз.

Шляхи удосконалення організації охорони інформації з обмеженим доступом в контексті російсько-української війни включають:

1. Розробка та впровадження передових технологічних засобів захисту даних, включаючи системи шифрування та мережеві заходи безпеки для виявлення та усунення кібератак.

2. Підвищення кваліфікації персоналу через тренінги з кібербезпеки, навчання правилам користування інформаційними системами та реагування на інциденти безпеки.

3. Встановлення строгих процедур контролю доступу, ідентифікації та автентифікації, обмеження прав доступу до конфіденційної інформації та створення аудитів доступу.

4. Розробка кризових планів та дій для реагування на кібератаки, включаючи резервне копіювання даних та відновлення систем.

5. Співпраця з урядовими та міжнародними організаціями для обміну інформацією та спільних проектів з кібербезпеки.

6. Проведення регулярних аудитів та оцінок безпеки для виявлення слабких місць та вдосконалення заходів захисту інформації.

Заропоновані заходи для вдосконалення організації охорони інформації з обмеженим доступом будуть сприяти покращенню цієї організації та зменшенню загроз для національної безпеки під час воєнного стану в країні.

Забезпечення захисту інформації під час воєнного стану в Україні стає надзвичайно важливим завданням, яке вимагає відповідального та проактивного підходу державних органів, військових та цивільних службовців, а також громадських організацій та громадян. Забезпечення безпеки інформації на сучасних підприємствах є однією з ключових тенденцій, яка вимагає постійного проведення нових досліджень та знаходження ефективних засобів та

методів захисту, а також вдосконалення вже існуючих заходів. Для цього потрібно постійно вдосконалювати заходи безпеки, а також вивчати та застосовувати найновіші технології та методи захисту інформації.

Висновок до третього розділу

Отже, розгляд яскравих прикладів організації системи захисту інформації в галузі підприємництва у різних країнах світу показує, що цей досвід має як переваги, так і недоліки, які варто враховувати. Україні було б корисно вивчити цей досвід і взяти з нього приклад для подальшого вдосконалення своїх систем захисту інформації. Під час аналізу міжнародного досвіду охорони інформації з обмеженим доступом стало очевидним, що впровадження ефективної системи захисту конфіденційної інформації є критично важливим завданням для будь-якої організації або установи. Присутність комплексних стратегій, які враховують сучасні технологічні вимоги, правові стандарти та норми, дозволяє ефективно захищати інформаційні потоки та запобігати загрозам з боку зловмисників. Результати досліджень також підтверджують, що постійне підвищення кваліфікації персоналу, використання передових технологій шифрування та моніторингу, а також впровадження строгих процедур контролю доступу є важливими складовими успішної системи охорони інформації з обмеженим доступом.

У контексті російсько-української війни, удосконалення організації охорони інформації з обмеженим доступом стає ключовим завданням для забезпечення національної безпеки та ефективної військової діяльності. Аналіз показує необхідність постійного удосконалення технологічних засобів шифрування та захисту даних, впровадження сучасних систем моніторингу та аналізу загроз, підвищення кваліфікації персоналу і вдосконалення процедур контролю доступу до конфіденційної інформації. Крім цього, активна співпраця з міжнародними партнерами у галузі кібербезпеки та обмін досвідом виявляються ефективними засобами забезпечення надійного захисту інформації під час воєнних конфліктів.

Реалізація цих заходів сприятиме підвищенню стійкості інформаційної інфраструктури та зменшить ризики витоку чи пошкодження конфіденційної інформації у період війни. Постійна адаптація до сучасних кіберзагроз,

впровадження передових технологій та співпраця з міжнародними експертами дозволять забезпечити надійний захист інформаційних ресурсів та підвищити ефективність діяльності під час воєнних дій. У зв’язку зі зростанням обсягу цифрової інформації та загроз кібербезпеки, важливим стає розвиток та впровадження сучасних технологій захисту інформації. Держави мають працювати над створенням інтегрованих систем захисту даних, які б забезпечували не лише високий рівень секретності, а й ефективну відповідь на потенційні кібератаки.

Одним із напрямків розвитку є розробка та впровадження шифрування даних на всіх рівнях інформаційних систем, що забезпечить їх захищеність від несанкціонованого доступу. Крім того, необхідно активно працювати над розробкою адаптивних та інтелектуальних систем виявлення загроз, які здатні вчасно реагувати на нові варіанти кіберзагроз. Для забезпечення ефективності механізмів захисту таємниць, також важливо розробляти та впроваджувати стандарти та норми безпеки, які враховують сучасні виклики та технологічні можливості. Це дозволить забезпечити гармонійний розвиток інформаційних систем у контексті міждержавного співробітництва та зміцнення довіри до механізмів обміну секретною інформацією

.

ВИСНОВКИ

За результатами матеріалу викладеному у дипломній роботі та виконавши мету і завдання доходимо до таких висновків:

1. Під час аналізу наукових джерел і стану досліджень забезпечення захисту інформації з обмеженим доступом під час періоду АТО та воєнного стану було виявлено значний інтерес до цієї теми у наукових розвідках. Дослідження в цьому напрямку спрямовані на аналіз правового режиму, визначення особливостей регулювання доступу до конфіденційної інформації, а також роль цієї інформації у забезпеченні національної безпеки під час конфлікту та воєнного стану.

2. Наукові джерела наголошують на необхідності ретельного аналізу правових норм і політик, спрямованих на захист конфіденційної інформації під час воєнного періоду, а також впровадження ефективних заходів для її захисту. Важливим є визначення критеріїв класифікації інформації з обмеженим доступом, а також розробка механізмів для її обробки, зберігання та передачі. Дослідження підкреслюють, що забезпечення захисту інформації з обмеженим доступом під час АТО та воєнного стану є надзвичайно важливим завданням для національної безпеки та військової діяльності. Розуміння та ефективне використання цієї інформації може значно підвищити результативність операційних дій і сприяти успішному виконанню завдань у умовах воєнного конфлікту.

3. Інформація з обмеженим доступом представляє собою дані та відомості, які знаходяться на матеріальних або електронних носіях із законним правом власності у фізичних осіб, юридичних осіб або держави. Ця інформація відноситься до таємної, службової або конфіденційної категорій відповідно до встановленого законодавством порядку. Зважаючи на потенційну чутливість цих даних, їх захист вважається ключовим аспектом сучасного інформаційного середовища. У різних правових системах та доктринах існують варіації у

визначенні інформації з обмеженим доступом, що залежить від контексту та умов кожної конкретної країни. Однак, наявність чіткої нормативно-правової бази для регулювання доступу до такої інформації є надзвичайно важливою, оскільки це забезпечує правову впорядкованість і захищає права осіб та організацій.

4. Різні категорії інформації з обмеженим доступом, такі як конфіденційна, таємна та службова, визначаються законодавством та волями власників або уповноважених осіб. Захист конфіденційної інформації забезпечується не природними характеристиками цієї інформації, а завдяки правовому режиму, який встановлює правила доступу та обмежує можливість її розголошення. Це робить важливим розуміння та чітке визначення цих понять в правових документах для створення ефективних механізмів захисту конфіденційної інформації та забезпечення безпеки суспільства в цілому.

5. Обмеження доступу до публічної інформації під час АТО та воєнного стану становить складне етичне та юридичне питання, яке вимагає уважного узгодження між захистом національної безпеки та правом людини на інформацію. Необхідність таких обмежень обумовлена потребою уникнення розголошення конфіденційної інформації, яка може нашкодити національній безпеці та військовій справі. Однак, важливо, щоб ці обмеження були обґрунтованими, тимчасовими та пропорційними, і дотримувалися законодавства, у той час забезпечуючи засади демократії та прав людини. Узагальнюючи, суспільство стоїть перед важливим завданням забезпечити збалансований підхід до доступу до інформації під час АТО та воєнного стану, розробляючи чіткі та прозорі механізми контролю доступу до публічної інформації та забезпечуючи захист національної безпеки, а також забезпечуючи права громадян на інформацію та прозорість діяльності державних органів.

6. Забезпечення безпеки інформації у сучасних інформаційних системах через технічні заходи має надзвичайну вагу для збереження даних у захищеному та конфіденційному режимі. З розвитком кібербезпеки стає все

складніше захищати дані, тому необхідно постійно удосконалювати технічні заходи для ефективного протистояння різноманітним загрозам в онлайн середовищі. Важливо мати на увазі різноманітність загроз, які включають кібератаки, витоки інформації, шпигунство та інші види кіберзлочинності. Для надійного технічного захисту інформації використання передових методів шифрування, захист мережі, регулярне оновлення програмного та апаратного забезпечення, а також впровадження систем виявлення та реагування на інциденти є критично важливими. Тільки комплексний підхід до захисту даних може забезпечити ефективний захист від загроз та зберегти безпеку та конфіденційність інформаційних систем у сучасному цифровому середовищі.

7. Забезпечення безпеки інформації з обмеженим доступом від витоку та несанкціонованого доступу стає критично важливим завданням у сучасному цифровому світі. Розповсюдження кіберзагроз та злочинної діяльності в Інтернеті вимагає комплексного підходу до захисту даних, включаючи технічні та організаційні заходи. Ефективний захист інформації потребує постійного вдосконалення технологій, навчання персоналу та впровадження строгих політик безпеки. Організації мають активно протидіяти кіберзлочинцям, регулярно аудитувати системи, розробляти та впроваджувати плани реагування на інциденти та підтримувати високий рівень обізнаності щодо сучасних загроз. Лише поєднання технологій, відповідних стратегій та навичок управління ризиками може забезпечити ефективний захист інформації з обмеженим доступом, що є критично важливим для забезпечення безпеки та довіри у цифровому середовищі.

8. розгляд яскравих прикладів організації системи захисту інформації в галузі підприємництва у різних країнах світу показує, що цей досвід має як переваги, так і недоліки, які варто враховувати. Україні було б корисно вивчити цей досвід і взяти з нього приклад для подальшого вдосконалення своїх систем захисту інформації. Під час аналізу міжнародного досвіду охорони інформації з обмеженим доступом стало очевидним, що впровадження ефективної системи

захисту конфіденційної інформації є критично важливим завданням для будь-якої організації або установи. Присутність комплексних стратегій, які враховують сучасні технологічні вимоги, правові стандарти та норми, дозволяє ефективно захищати інформаційні потоки та запобігати загрозам з боку зловмисників. Результати досліджень також підтверджують, що постійне підвищення кваліфікації персоналу, використання передових технологій шифрування та моніторингу, а також впровадження строгих процедур контролю доступу є важливими складовими успішної системи охорони інформації з обмеженим доступом.

9. У контексті російсько-української війни, удосконалення організації охорони інформації з обмеженим доступом стає ключовим завданням для забезпечення національної безпеки та ефективної військової діяльності. Аналіз показує необхідність постійного удосконалення технологічних засобів шифрування та захисту даних, впровадження сучасних систем моніторингу та аналізу загроз, підвищення кваліфікації персоналу і вдосконалення процедур контролю доступу до конфіденційної інформації. Крім цього, активна співпраця з міжнародними партнерами у галузі кібербезпеки та обмін досвідом виявляються ефективними засобами забезпечення надійного захисту інформації під час воєнних конфліктів.

10. Реалізація цих заходів сприятиме підвищенню стійкості інформаційної інфраструктури та зменшить ризики витоку чи пошкодження конфіденційної інформації у період війни. Постійна адаптація до сучасних кіберзагроз, впровадження передових технологій та співпраця з міжнародними експертами дозволять забезпечити надійний захист інформаційних ресурсів та підвищити ефективність діяльності під час воєнних дій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text. (Дата звернення 15.02.24).

2. Про доступ до публічної інформації: Закон України. Відомості Верховної Ради України (ВВР). 2011. №32. Ст. 314.

3. Про правовий режим воєнного стану: Закон України від 06.04.2000 р. № 389- VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text. (Дата звернення 15.02.24).

4. Про практику застосування адміністративними судами законодавства про доступ до публічної інформації: Постанова Пленуму Вищого адміністративного суду України №10 від 29 вересня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/v0010760-16#Text. (Дата звернення 15.02.24).

5. Про внесення змін до деяких законів України щодо функціонування державної служби та місцевого самоврядування у період дії воєнного стану: Закон України від 12 травня 2022 року № 2259-IX. Офіційний вісник України. 2022. № 42. Ст. 227.

6. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану: Закон України від 24 березня 2022 року № 2160-IX. URL: https://zakon.rada.gov.ua/laws/show/2160-20#Text. (Дата звернення 15.02.24).

7. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова КМУ від 12 березня 2022 р. № 263. URL: https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF#Text. (Дата звернення 15.02.24).

8. Андрощук А. Секретна інформація як об’єкт правової охорони. Інтелектуальна власність. 1999. № 3-4. С. 27-32.

9. Баскаков В. Ю. Адміністративно-правовий режим інформації з обмеженим доступом: авторефе рат дис. ... канд. юрид. наук: 12.00.07. Київ, 2012. 24 с.

10. Баскаков В. Ю. Інформація з обмеженим доступом: поняття та ознаки. Актуальні проблеми державотворення (Імперативи розвитку юридичної та безпекової науки; № 9): матеріали наук.-практ. конф., м. Київ, 28 черв. 2011 р. Київ, 2011. С. 47-49.

11. Баскаков В. Ю. Інформація з обмеженим доступом: аналіз термінологічного-понятійного апарату. URL: https://goal-int.org/informaciya-z-obmezhenim-dostupom-analiz-terminologichno-ponyatijnogo-aparatu/. (Дата звернення 15.02.24).

12. Білоусова Л., Муравка А., Олефіренко Н. Інформатика. 10-11 кл.: навч. посіб. Харків: Факт, 2009. 352 с.

13. Бондарук Г. В. Сутність понять «інформація», «інформаційна грамотність», «інформаційна культура», «інформаційна компетентність» у контексті ідей НУШ. Проблеми модернізації мовної освіти в ЗЗСО. Пріоритети філологічної освіти. Збірник наукових праць. Вип.11, 2023. С. 4-7.

14. Букет Д.А. Управління інформаційною безпекою за допомогою комплексної системи захисту. Сучасний захист інформації №1(49), 2022. С. 56-60.

15. Вимоги до захисту інформації в інформаційних системах у воєнний час: роз’яснення Держспецзв’язку. Асоціації «Телас». URL: https://telas.kiev.ua/hhaluzi/vimogi-do-zakhistu-informatsiji-v-informatsijnikh-sistemakh-u-voennij-chas-roz-yasnennya-derzhspetszv-yazku.html. (Дата звернення 15.02.24).

16. Глобальні принципи з національної безпеки та права на інформацію URL: https://www.justiceinitiative.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles. (Дата звернення 08.02.24).

17. Гордієнко С.Г. Конфіденційна інформація та «таємниці»: їх

співвідношення. Часопис Київського університету права. 2013. № 4. С. 233-238.

18. Дідук А.В. Правовий режим конфіденційної інформації: цивільно-правовий аспект: автореф. дис. … канд. юрид. наук. Харків, 2008. 24 с.

19. Дімчогло М. І. Консолідація інформаційного законодавства України: автореф. дис. ... канд. юрид. наук: 12.00.07. Київ, 2012. 18 с.

20. Економіка – правовий аспект: навчальний посібник. Київ: Атіка, 2005. 432 с.

21. Заболоцький Т. Кіберпростір як інструмент соціального впливу на сучасну молодь. Ввічливість. Humanitas, 2021. № (1). С. 22-27.

22. Загальна декларація прав людини ООН 1948 року. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text. (Дата звернення 08.02.24).

23. Золотар О. О. Обмеження доступу до інформації: інформаційно-правовий аспект. URL: http://archive.nbuv.gov.ua/portal/soc_gum/iblsd/2012_1/_private/13zooala.pdf. (Дата звернення 08.02.24).

24. Інформація. Енциклопедія сучасної України. URL: https://esu.com.ua/article-12485. (Дата звернення 08.02.24).

25. Інформаційна та кібербезпека: соціотехнічний аспект: підручник В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с.

26. Камлик М.І. Економічна безпека підприємниць кої діяльності.

27. Канали несанкціонованого доступу до інформації. URL: http://um.co.ua/4/4-17/4-17814.html. (Дата звернення 08.02.24).

28. Капіца Ю.М. Проблеми правової охорони комерційної таємниці, ноу-хау та конфіденційної інформації в праві України: реферативний огляд чинного законодавства України та практика його застосування; за ред. В.В. Цвєткова, Є.Б. Кубко. К.: Салком, 2000. 296 с.

29. Карачка А.Ф. Технології захисту інформації: Текст лекцій. Тернопіль, ТНЕУ, 2017. URL: http://dspace.wunu.edu.ua/bitstream/316497/26564/1/lekzii.pdf. (Дата звернення 15.02.24).

30. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навч. посібник. К.: Кондор, 2008. 384 с.

31. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України: автореф. дис. ... д-ра юрид. наук: 12.00.07. Харків, 2004. 31 с.

32. Коц Д. В. Теоретико-правові засади інформації з обмеженим доступом. ВІСНИК НТУУ «КПІ». Політологія. Соціологія. Право. Випуск 2 (42), 2019. С. 107-111.

33. Крестьянінов О.О. Правове регулювання митних режимів : автореф. дис. ... канд. юрид. наук: 12.00.07. Харків, 2002. 20 с.

34. Кулініч О.О. Інформація з обмеженим доступом як об'єкт цивільних прав: дис… канд. юрид. наук: 12.00.03. О., 2006. 200 с.

35. Кушнір І. П., Царенко О. М. Правовий режим інформації з обмеженим доступом у діяльності Державної прикордонної служби України. Право та державне управління. № 3 (36) том 1, 2019. С. 180-185.

36. Лапінська Є. І. Зарубіжний досвід захисту інформації у сфері підприємництва та його використання в Україні. Держава та регіони. Серія: Право, 2019 р., № 3 (65). С. 174-177. URL: http://www.law.stateandregions.zp.ua/archive/3_2019/30.pdf. (Дата звернення 15.02.24).

37. Ліпкан В.А., Баскаков В.Ю. Адміністративно-правовий режим інформації з обмеженим доступом в Україні: монографія / за заг. ред. В.А. Ліпкана. Київ: ФОП О.С. Ліпкан, 2013. 344 с.

38. Ліпкан В. А, Капінус Л. І. Доступ до інформації з обмеженим доступом: Проблеми вироблення уніфікованих дефініцій. Науково-практичний юридичний журнал «Публічне право» Київ, 2013. № 4. С 45–53.

39. Марущак А.І. Правові основи захисту інформації з обмеженим доступом: курс лекцій. К.: КНТ, 2007. 208 с.

40. Марущак А. І. Слова свободи та інформація з обмеженим доступом: співвідношення понять. Нау кове фахове видання «Бюлетень міністерства юстиції України». Київ, 2005. № 6. С. 44–49.

41. Низенко Е.І., Калепяк В.П. Забезпечення інформаційної безпеки

підприємництва: навчальний посібник. Київ: МАІП, 2006. 134 с

42. Олексіюк Т., Опришко Л., Буртник Х., Барвіцький В., Кабанов О. Рекомендації Уповноваженого Верховної Ради України з прав людини з питань додержання конституційного права людини і громадянина на доступ до інформації. Рада Європи, грудень 2020 р. URL: https://rm.coe.int/recomendationsfinal-10-02-21/1680a165f7. (Дата звернення 15.02.24).

43. Олійник О.Г. Інформаційна безпека США. Боротьба з організованою злочинністю і коруп цією (теорія і практика), 2015.

44. Організаційні канали розголошення інформації, технічні канали витоку інформації. URL: https://sites.google.com/site/kanalivitokuinformaciie/klasifikacia-kanaliv-vitoku-informaciie/kanali-vtrati-konfidencijnoie-informaciie. (Дата звернення 15.02.24)

45. Основні способи реалізації організаційних каналів витоку інформації. URL: http://um.co.ua/8/8-5/8-52578.html. (Дата звернення 09.03.24).

46. Пилипів І. Майбутнє відкритих даних під питанням. До якої інформації хоче обмежити доступ держава. Економічна правда. 21.09.2022 р. URL: https://www.epravda.com.ua/publications/2022/09/21/691717/. (Дата звернення: 27.02.2024 року).

47. Правове забезпечення безпеки суб'єктів госпо дарської діяльності в Україні: навчально-ме тодичний посібник. Уманський державний педагогічний університет; уклад. О.В. Митяй. Умань: ПП Жовтий, 2013. 128 с.

48. Рабінович П.М. Рішення Європейського суду з прав людини: до характеристи ки концептуально-методологічних засад їх обґрунтування. URL: http://eurocourt.in.ua/Article.asp?AIdx=31. (Дата звернення: 27.02.2024 року).

49. Рішення Ради суддів України № 11 від 25.03.2022 року. URL: http://rsu.gov.ua/ua/documents?id=130&page=3&per-page=8. (Дата звернення: 27.02.2024 року).

50. Семенюк О. Г. Класифікація таємної інформації. Інформація і право. № 1(16). 2016. С. 44-51.

51. Серьогін В. О. Конституційний принцип гласності у діяльності

органів державної влади України: автореф. дис. ... канд. юрид. наук: 12.00.02. Харків, 1999. 18 с.

52. Сіленко А. Інформаційні технології – новий імпульс для пошуку парадигми майбутнього суспільства. Політичний менеджмент. 2007. № 3(24). С. 96–112.

53. Службова інформація: порядок віднесення та доступу. Практичний посібник; за ред. Д. М. Слизьконіс. Київ: Центр політичних студій та аналіт

54. Спільна заява Міністерства культури та інформаційної політики України, Міністерства оборони України та представників ЗМІ. Міністерство культури та інформаційної політики України, Міністерство оборони України, опубліковано 27 квітня 2022 року. URL: https://www.kmu.gov.ua/news/spilna-zayava-ministerstva-kulturi-ta-informacijnoyi-politiki-ukrayini-ministerstva-oboroni-ukrayini-ta-predstavnikiv-zmi. (27.04.2022 року).

55. Тлумачний словник української мови. URL: http://sum.in.ua/

56. Турченко О.Г., Фурман В.В. Обмеження права на доступ до публічної інформації в умовах воєнного стану. Конституційне право, муніципальне право. Електронне наукове видання «Аналітично-порівняльне правознавство». URL: https://app-journal.in.ua/wp-content/uploads/2022/12/22.pdf. (Дата звернення 09.03.24).

57. Україна розгортає рішення Hideez і Yubico в державних установах для забезпечення захисту від несанкціонованого доступу. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/ukrayina-rozgortaye-rishennya-hideez-i-yubico-v-derzhavnikh-ustanovakh-dlya-zabezpechennya-zakhistu-vid-nesankcionovanogo-dostupu. (Дата звернення 09.03.24).

58. Хавронюк М. Поширення інформації про військову допомогу та дії військових України: кримінальна відповідальність. URL: https://pravo.org.ua/blogs/poshyrennya-informatsiyi-pro-vijskovu-dopomogu-ta-diyi-vijskovyh-ukrayiny-kryminalna-vidpovidalnist/. (Дата звернення 09.03.24).

59. Характеристика технічних заходів захисту інформації. URL: https://jktod.donnu.edu.ua/article/view/13127. (Дата звернення 09.03.24).

60. Чернишова Т.В. Правові режими інформації за законодавством України. Право і суспільство. 2012. № 4. С. 97-101.

61. Що таке несанкціонований доступ? URL: https://ua-referat.com. (Дата звернення 08.02.24).

62. Ярмакі Х. П., Музика С. С. Класифікація конфіденційної інформації. Правова система: теорія і практика. Південноукраїнський правничий часопис, 2021. С. 94-98. URL: http://www.sulj.oduvs.od.ua/archive/2021/1/18.pdf. (Дата звернення 08.02.24).

63. Rafael Capurro. Past, present and future of the concept of information. 2009. IpleC 7(2). P. 125–141. URL: http://www.triple-c.at/. (Дата звернення 08.02.24).

64. Young, James та Webster проти Сполученого Королівства (Young, James та Webster v. the United Kingdom): Рішення Європейського суду з прав людини від 13 серпня 1981 р. (заява N 7601/76; 7806/77). URL: http://hudoc.echr.coe.int/eng?i=001-57608. (Дата звернення 15.02.24).