МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

Інститут заочного та дистанційного навчання

Кафедра кримінології та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

для здобуття ступеня вищої освіти магістра

на тему: «Правові та організаційні засади захисту інформації в інформаційно-аналітичних системах МВС України»

Виконав: здобувач 2 курсу 1 групи
Спеціальність: 281 «Публічне управління та адміністрування»

Ус Карина Сергіївна
Індивідуальний навчальний план № 24-97
Мобільний телефон: +380 63-644-26-01

Науковий керівник:
завідувач кафедри, доктор філософії в галузі права, доцент
Школьніков Владислав Ігорович _____
(підпис)

Кваліфікаційна робота допущена до захисту
«11» грудня 2025 р., протокол № 07
завідувач кафедри, доктор філософії в галузі права, доцент
_____ Владислав ШКОЛЬНІКОВ

Київ 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЄІС МВС – Єдина інформаційна система МВС

ІАЗ - Інформаційно-аналітичне забезпечення

КЗЗ – Комплекс засобів захисту

КЗІ – Криптографічний захист інформації

КМУ – Кабінет Міністрів України

КСЗІ – Комплексна система захисту інформації

КТЗ – Комплекс технічних засобів

МВС – Міністерство внутрішніх справ

НАІС – Національна автоматизована інформаційна система

НД – Нормативний документ

НКІ – Носій ключової інформації

НСД – Несанкціонований доступ

ОС – Операційна система

ОТК – Обов'язковий технічний контроль

ПЗ – Програмне забезпечення

ПК – Програмний комплекс

СЗІ – Служба захисту інформації

СУІБ – складові управління інформаційної безпеки

ТЗІ – Технічний захист інформації

ВСТУП

Актуальність теми Інформаційна безпека стає все більш важливою у сучасному світі, оскільки цифрові технології вже проникли у всі сфери життя, включаючи правоохоронні органи. У зв'язку зі зростанням обсягу інформації та збільшенням значення інформаційних ресурсів, забезпечення їхньої безпеки стає головним завданням держави. Це особливо важливо для правоохоронних підрозділів МВС України, яка виконує особливу роль для захисту інформаційного простору держави, людини, суспільства та організацій від різних загроз.

Інформаційно-аналітична робота та її висновки є дуже важливими не тільки для ефективного керівництва підрозділами МВС, але й для створення та виконання різних програм, які борються зі злочинністю, прогнозування правоохоронної та правосудної діяльності в конкретних соціальних, економічних та демографічних умовах, враховуючи поточну ситуацію. Це допомагає керувати системою забезпечення правопорядку в змінному соціальному середовищі, оптимізувати саму систему та вчасно розподілити її ресурси. Усе це неможливе без розвитку інформаційно-технологічного забезпечення та захисту інформації в інформаційно-аналітичних системах МВС України.

Проблематика безпеки інформаційно-аналітичної роботи підрозділів МВС привертала увагу багатьох дослідників. Е. В. Рижков, С. О. Прокопов, Ю. П. Синиціна, О. О. Мельнікова, В. І. Гур'єв, Ю. М. Ткач, Д.Б. Мехед, І. В. Фірсова. та інші науковці присвятили свої роботи безпеці інформаційно-аналітичної роботи МВС.

Мета роботи – дослідити правові та організаційні засади захисту інформації в інформаційно-аналітичних системах МВС України.

Для досягнення поставленої мети сформульовані основні **завдання дослідження**:

Визначити основні поняття захисту інформації в інформаційно-аналітичних системах МВС України.

З’ясувати особливості захисту інформації в інформаційно-аналітичних системах МВС України від несанкціонованого доступу.

Узагальнити міжнародні стандарти правового регулювання захисту інформації в інформаційно-аналітичних системах.

Проаналізувати правове регулювання захисту інформаційно-аналітичних систем в МВС України.

Визначити міжнародний та національний досвід організації захисту інформації в інформаційно-аналітичних системах МВС України.

Розробити методи удосконалення механізмів захисту інформації в інформаційно-аналітичних системах МВС України.

Об’єкт дослідження – процес захисту інформації в інформаційно-аналітичних системах МВС України.

Предмет дослідження – правові та організаційні засади захисту інформації в інформаційно-аналітичних системах МВС України.

Елементи наукової новизни отриманих результатів: визначено що, комплексний підхід до організації захисту інформаційно-аналітичних систем (ІАС), який, на відміну від існуючих, поєднує технічні методи контролю доступу з психолого-організаційними методами роботи з персоналом, що дозволяє враховувати специфіку службової діяльності працівників МВС. Запропоновано систему ієрархічного розподілу прав доступу, що дозволяє посилити контроль за конфіденційними даними без втрати оперативної ефективності роботи.

Методологічна основа дослідження: теоретичний аналіз для вивчення літератури, синтез для узагальнення концепцій, порівняння для оцінки методів захисту інформації, узагальнення для формулювання висновків.

Практичне значення здобутих результатів Удосконалення організаційних заходів що до методів захисту інформаційно аналітичних систем МВС України. Це дослідження допоможе підвищити ефективність роботи

персоналу з інформаційно-аналітичними системами, посилити контроль за доступом до даних та мінімізувати ризик витоку інформації через фактори ризику.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМАХ МВС УКРАЇНИ

1.1. Основні поняття захисту інформації в інформаційно-аналітичних системах МВС України

Інформація та мережі, на яких вона працює, є важливими частинами сучасних інформаційних систем підрозділів МВС. Їх можливість доступу, збереження і захисту від викрадення мають велике значення для забезпечення безпеки. Сучасні інформаційні системи створюють нові шанси для незаконного отримання інформації. Також тенденція до використання розподілених комп'ютерних систем ускладнює роботу фахівців, які мають контролювати інформаційні системи та мережі. Використання інформаційних технологій здатне виступити ключовим фактором для зміцнення верховенства права, гарантування оборонної здатності країни, стабільності соціально-політичного середовища та розвитку демократичних принципів в управлінні МВС України [58 с. 4-8].

Уже давно інформація стала загально відомим поняттям, але до теперішнього часу не існує загального наукового визначення цього слова. З точки зору різних наукових галузей, це поняття пояснюється різними особливими рисами. Сучасна наука виділяє два види інформації: об'єктивну – це властивості матеріальних речей та явлень, які передаються іншим об'єктам і відображаються в їхній структурі; і суб'єктивну – яка відображає зміст об'єктивної інформації, при цьому вона утворюється свідомістю людини за допомогою слів, образів та відчуттів і фіксується на будь-якому матеріальному носієві. У повсякденному розумінні інформація являє собою дані про навколишній світ та процеси, що у ньому відбуваються, які сприймаються людиною чи спеціалізованими пристроями.

Інформаційні системи являють собою організаційно-технічні платформи, які базуються на використанні технологій обробки даних за допомогою апаратного і програмного забезпечення. У їхній структурі можуть бути інтегровані інформаційні підсистеми, що містять бази даних, об'єднані технологічними механізмами для ефективного обміну інформацією. У процесі аналітичної діяльності важливу роль відіграють спеціально розроблені рамкові структури, особливо в умовах роботи зі складними справами, що стосуються функціонування організованих злочинних угруповань. У таких випадках критично важливо ідентифікувати методи, які використовуються під час здійснення протиправних дій, а також простежити багатошарові взаємозв'язки між окремими учасниками.

Інформаційний простір системи МВС України створений на основі єдиного інформаційного простору, який включає суб'єктів інформаційно-аналітичної діяльності, технології управління спеціалізованими базами даних, а також інформаційно-комунікаційні системи та мережу банку даних. Всі ці елементи побудовані за єдиним принципом, щоб забезпечити ефективну взаємодію всередині системи МВС України. Інформаційно-аналітичне забезпечення використовують для виявлення проблем, їх оцінки та визначення ефективності зроблених змін у роботі органів поліції. З ростом злочинності в Україні у правоохоронних органах та Національній поліції запровадили сучасні інформаційно-аналітичні системи. Використання сучасних технологій у цій роботі допомагає зберегти час оперативних працівників та покращити якість їхньої роботи [47 с 40-48].

Інформаційно-аналітична робота підрозділів МВС — це робота, яка вимагає творчості, дослідження, цілісного підходу та спеціальної організації. Вона проводиться з використанням методів, щоб досягти таких цілей: збирати, накопичувати та обробляти дані; шукати, аналізувати та узагальнювати інформацію про стан правопорядку та роботу органів правопорядку; отримувати нові спеціальні знання для покращення боротьби зі злочинністю; підвищувати

ефективність управлінської роботи на різних рівнях, щоб боротися зі злочинністю, забезпечувати охорону свобод та прав людини, підтримувати суспільний порядок та безпеку. Інформаційно-аналітична діяльність (ІАД) - це різновид розумової та інтелектуальної активності особистості. Відповідно, в процесі розумової та інтелектуальної діяльності відбувається продукування нової інформації, що є результатом певного алгоритму послідовних операцій з розшуку, накопичення, опрацювання та аналізу вихідної інформації. Згенерована таким чином, нова, вторинна аналітична інформація, формується у вигляді аналітичних матеріалів, звітів, оглядів, прогнозів і подібного [54. с. 50-53].

Певною мірою, інформаційно-аналітична діяльність забезпечує захист та безпеку для керівників та менеджерів від сучасних загроз, небезпек та викликів. Це, в свою чергу, впливає на прийняття вдалих управлінських рішень, допомагає упереджувати та передбачати можливі наслідки будь-яких загроз, що можуть мати негативний вплив. Саме ухвалення ефективних управлінських рішень щодо нейтралізації несприятливих ризикових ситуацій є ключовим чинником при підготовці аналітичних матеріалів та прогнозів в правоохоронній діяльності.

Наразі неможливо уявити ефективну роботу органів МВС без використання сучасних інформаційних технологій. Дуже багато статистичної, аналітичної та довідкової інформації використовують національна поліція, Державна служба України з надзвичайних ситуацій, Державна міграційна служба, Державна прикордонна служба, Національна гвардія та інші підрозділи МВС України. Для цього застосовують як універсальні, так і спеціалізовані програмні засоби. Слід підкреслити, що інформаційно-аналітична робота та її досягнення відіграють критичну роль не тільки для успішного керівництва структурами МВС, але й для планування та втілення різноманітних програм з протидії злочинності, перспективного прогнозування правоохоронної та правозастосовної діяльності в конкретних соціально-економічних та демографічних обставинах, враховуючи актуальні дані оперативної ситуації [53. с. 183 - 189]. Це забезпечує управління органами МВС як комплексною правоохоронною системою в динамічному

суспільному просторі, покращує організацію системи та ефективний розподіл ресурсів.

Інформаційно-аналітична діяльність являє собою комплекс заходів, які проводяться з використанням визначених підходів, методик, інструментів і документів. Її мета полягає у зборі, систематизації, обробці та аналізі даних, що необхідні для аргументованої підготовки та прийняття рішень [51]. Інформаційно-аналітичне забезпечення – це процес створення найкращих умов для виконання інформаційних завдань та реалізації повноважень державних органів на основі організації та використання інформаційних ресурсів. Інформаційно-аналітична діяльність органів Міністерства внутрішніх справ України – це комплекс заходів, визначених законодавством України та регульованих внутрішніми нормативними актами міністерств, що зосереджені на зборі, обробці, узагальненні, дослідженні, накопиченні та застосуванні інформації, включаючи обмежений доступ, що є важливим для вирішення завдань Міністерства внутрішніх справ щодо забезпечення безпеки громадян, суспільства та держави.

Адміністративно-правове регулювання діяльності інформаційних служб системи МВС слід розуміти як окремий правовий механізм, який має єдину систему управлінських, правових та технічних засобів, методів, способів, форм, які дозволяють виконувати поставлені завдання [46].

Функціонал інформаційної служби охоплює такі ключові аспекти:

- ✓ Імплементація державних стратегій та пріоритетних напрямів щодо формування сучасної інформаційної інфраструктури в Україні в межах компетенції Міністерства внутрішніх справ.
- ✓ Оптимізація рівня інформаційно-аналітичного супроводу оперативно-розшукової діяльності Національної поліції України.
- ✓ Гарантування результативності управлінських рішень, що ухвалюються керівним складом Національної поліції України.

- ✓ Інтеграція та уніфікація інформаційних масивів, отриманих у ході оперативно-розшукової діяльності Національної поліції України, у єдиний інформаційний простір із застосуванням сучасних інформаційних технологій, комп'ютерних систем та телекомунікаційних засобів.
- ✓ Забезпечення превентивних заходів та виконання профілактичних завдань, спрямованих на мінімізацію та уникнення правопорушень.
- ✓ Координування та реалізація інформаційно-аналітичної підтримки оперативно-розшукової діяльності для структурних підрозділів центрального апарату МВС та його головних територіальних управлінь.
- ✓ Здійснення комплексного аналізу криміногенної ситуації та розробка аналітичних й інформаційних матеріалів для обґрунтованого ухвалення управлінських рішень керівництвом МВС. Це передбачає систематизацію процесів збору, обробки та актуалізації даних, що акумулюються у ході діяльності правоохоронних органів. При цьому основним стратегічним завданням є формування централізованих інформаційних ресурсів, які сприяють підвищенню ефективності управління.

Головна мета інформаційно-аналітичного забезпечення правоохоронних органів — створити умови для ухвалення оптимальних державних управлінських рішень, спрямованих на покращення безпеки громадян. [12, с. 29–37].

ІАЗ підрозділів МВС України складається з трьох взаємопов’язаних компонентів:

1) інформаційних систем, у рамках яких збирається, агрегується, систематично обробляється, зберігається та надається споживачам необхідна інформація;

2) аналітичної діяльності, яка включає реалізацію комплексу організаційних і методичних заходів, а також аналіз і узагальнення доступної оперативної та іншої інформації;

3) управлінська діяльність, спрямована на забезпечення прийняття оптимальних і обґрунтованих рішень.

Механізм інформаційно-аналітичної діяльності складається з певних операцій, які виконують суб'єкти цієї діяльності (розшук, реєстрація, отримання, опрацювання, впорядкування, узагальнення, аналіз, прогнозування, збереження та застосування інформації) [32]. Головні функції інформаційно-аналітичної діяльності підрозділів МВС визначені на рис. 1.1.

Рисунок 1.1. Головні функції інформаційно-аналітичної діяльності підрозділів МВС

Джерело: складено автором за [54. с. 40]

Об'єктом інформаційно-аналітичної роботи під час роботи підрозділів МВС є характерні риси чи аспекти об'єктів інформаційно-аналітичної діяльності, що зафіксовані на відповідних носіях, чи в пам'яті людей, або їх віддзеркалення.

Основними інструментами інформаційно-аналітичної роботи підрозділів МВС є:

– оперативна та криміналістична техніка та спеціалізовані технічні засоби, призначені для відкритого та таємного отримання інформації;

– відповідні апаратно-програмні комплекси (автоматизовані інформаційно-пошукові, експертні та логіко-аналітичні системи та інші) і різноманітні технічні

прилади, за допомогою яких реалізується опрацювання, систематизація та аналіз даних. Суттєву роль у цьому відіграють принципи інформаційно-аналітичної діяльності.

До загальних засад інформаційно-аналітичної діяльності відносяться: постійність накопичення відомостей, системний підхід, злагодженість, можливість варіацій, результативність, верифікованість та інші. Ключовими інформаційними джерелами, які застосовуються у процесі інформаційно-аналітичної роботи є: оперативні обліки, що формуються з банків даних кримінологічної, адміністративної, статистичної інформації; банків даних інших міністерств, відомств, підприємств, установ і організацій, що не пов'язані безпосередньо з боротьбою зі злочинністю; банків даних міських та обласних органів влади; операторів мобільного зв'язку; об'єктів надання та отримання охоронних послуг; депутатські запити; звернення та заяви громадян, засоби масової інформації, зокрема інтернет [38,41].

Усю вказану інформацію потрібно захищати. Принципи захисту мають бути різними залежно від того, який тип інформації потрібно охороняти. Якщо інформація, яку треба захищати, належить до одного з рівнів секретності, то основну увагу системи захисту слід зосередити на збереженні конфіденційності. Важливими елементами у процесі виконання КСЗІ є нормативні фактори – закони України, документи у галузі захисту інформації, стандарти, виробничі акти, практики тощо. Організація усіх дій здійснюється з метою виконання правових умов та технічних рішень, спрямованих на забезпечення необхідного рівня захисту активів інформаційної системи МВС України [44].

Об'єкти захисту в ІАС МВС містять:

1. Інформацію обмеженого доступу, що є основним об'єктом та розділяється на державну таємницю, яка об'єднує інформацію у сфері безпеки, оборони, економіки, науки, технологій, зовнішніх відносин, належать до держави та розголошення такої інформації може спричинити шкоди безпеці держави, службову – є інформація, розголошення якої може завадити актуальним чи

потенційним інтересам держави, чи МВС, та відомості про фізичних осіб - персональні дані, які обробляються в ІАС – дані, що є унікальними елементами диференційованої ідентифікації.

2. Інформаційно-аналітичні системи, що представляють апаратне, програмне та мережеве забезпечення для обробки інформації. До них можна віднести сервери, комп'ютери, системи зв'язку, бази даних.

3. Фізичні об'єкти. Призначені для обладнання місць зберігання обладнання та каналів зв'язку для трансляцій інформації.

Суб'єктами захисту інформації є:

1. Власники, які володіють інформацією, а також органи влади, яким ця інформація належить, тобто державні структури та підрозділи МВС України, які володіють інформацією та розробляють механізми її захисту.

2. Адміністратори систем. Це фахівці з обслуговування, моніторингу та налаштування ІАС.

3. Користувачі. Співробітники МВС, що забезпечені доступом до інформації є її користувачами. Вони відповідальні за дотримання встановлених вимог.

Процедура проєктування системи захисту інформації (ЗІ) та вибору засобів захисту в інформаційних системах (ІС) – це багатогранне та комплексне завдання (Додаток А,Б) [48, 49]. У його вирішенні потрібно брати до уваги широкий спектр потенційних загроз, що можуть зашкодити безпечному функціонуванню ІС, враховуючи також витрати на впровадження засобів ЗІ та потреби різних зацікавлених сторін.

Ключовим елементом у процесі забезпечення ЗІ є аналіз потенційних загроз для функціонування ІС. Йдеться про ті загрози, які збільшують вразливість даних, що обробляються в ІС, можуть призвести до їх неконтрольованого розголошення, випадкової чи навмисної зміни або знищення. Загроза інформації – це можливе явище або подія, яка здатна порушити стійку безпеку інформації. Носіями небезпеки для інформаційної безпеки виступають джерела погроз.

Джерела загроз можуть мати різне походження: або від окремих осіб (суб'єктів), або від об'єктивних факторів. Важливо, що джерела погроз здатні знаходитися як у межах організації – внутрішні джерела, так і за її межами – зовнішні. Розподіл на суб'єктивні та об'єктивні джерела виправданий, враховуючи попередній аналіз відповідальності за втрати або ризики інформації, а поділ на внутрішні та зовнішні джерела обумовлений тим, що способи протидії тим самим погрозам можуть суттєво відрізнятися залежно від місця їх виникнення [36 с. 19 - 25]. Класифікація загроз інформації наведено рис.1.2.

Рисунок 1.2 Класифікація загроз інформації

За походженням та характером загрози діляться на:

а) природні, такі як пожежа, землетрус, повінь – фізично пошкоджують обладнання, носії інформації;

б) техногенні, системні – різкі амплітудні коливання в перетворювачах.

в) випадкові або ненавмисні помилки персоналу, які призвели до втрати або пошкодження даних;

г) умисні - навмисні дії, спрямовані на несанкціонований доступ, зміну, знищення або викрадення інформації.

За характером впливу:

а) порушення конфіденційності, тобто несанкціонований доступ до інформації (наприклад, крадіжка пароля, шпигунство, перехоплення даних);

Несанкціонований доступ до інформаційних систем підрозділів Міністерства внутрішніх справ є незаконним доступом до інформації або функцій цих систем без відповідних повноважень чи затвердження, і порушує право на конфіденційність, цілісність та доступність даних, які встановлюються в українському законодавстві для захисту інформації.

б) порушення цілісності - несанкціонована зміна або знищення інформації (наприклад, модифікація даних у базі, саботаж);

в) порушення доступності, тобто блокування доступу до інформації для легітимних користувачів (наприклад, DDoS-атаки, віруси-вимагачі).

Маємо два основних шляхи подолання викликів безпеки ІКС: фрагментарний та комплексний [35 с. 70-76]. Фрагментарний підхід концентрується на нейтралізації конкретно визначених загроз, з урахуванням певних умов. Як приклади втілення цього методу можна назвати використання засобів контролю доступу, автономних шифрувальних інструментів, специфічного антивірусного програмного забезпечення та інших. Значною перевагою такого підходу є його селективність, тобто націленість на певні загрози. Проте, його мінусом є відсутність єдиного захищеного інформаційного простору. Фрагментарні захисні заходи можуть гарантувати безпеку лише для конкретних компонентів ІКС, і навіть незначні зміни в ландшафті загроз можуть звести їхню ефективність нанівець.

Комплексний підхід націлений на формування захищеного простору для обробки даних в ІКС, поєднуючи різні стратегії боротьби з загрозами. Він включає багато різноманітних заходів та розглядає безпеку ІКС як комплексну задачу. Організація захищеної обробки інформації надає можливість забезпечити певний рівень захищеності ІКС, що є беззаперечною однією з переваг комплексного підходу [37]. Проте до його недоліків варто віднести обмеження

свободи дій користувачів ІКС, сприйнятливість до помилок встановлення та налаштування способів захисту, а також складність управління.

Комплексна система інформаційної безпеки з підтвердженою відповідністю являє собою інтегровану сукупність організаційно-технічних заходів, програмно-апаратних засобів та методологічних підходів, призначених для забезпечення захисту даних. Ключове призначення даної системи полягає у гарантуванні конфіденційності, цілісності та доступності інформаційних ресурсів у межах конкретної інформаційної системи (наприклад, системи ІПНП), шляхом впровадження ефективних механізмів протидії несанкціонованим діям. Це включає захист від шкідливого програмного забезпечення, що може спричинити спотворення, неправомірну модифікацію або повне знищення даних. Відповідальність за нагляд та забезпечення дотримання законодавства України у сфері інформаційної безпеки покладається на керівника структурного підрозділу, який здійснює експлуатацію центрального програмно-технічного комплексу системи.

Один із ключових аспектів комплексного підходу до забезпечення безпеки інформаційних і комунікаційних систем (ІКС) полягає у розробленні детальної та ефективної політики безпеки. Ця політика покликана регулювати функціонування захисних механізмів, охоплюючи всі аспекти, пов’язані з обробкою інформації. Формування надійної системи мережевої безпеки є неможливим без нормативного документа, який визначає алгоритми дій системи за різних обставин та враховує спектр потенційних загроз. [54].

1.2. Особливості захисту інформації в інформаційно-аналітичних системах МВС України від несанкціонованого доступу

Інформаційний простір системи МВС України визначається наступним чином. Він базується на створенні єдиного інформаційного простору системи

МВС України, суб'єктів інформаційно-аналітичної діяльності, технологій ведення та використання спеціалізованих баз даних, а також інформаційно-комунікаційних систем та мережі банків даних, що мають єдиний принцип роботи та структуру, що забезпечують інформаційну взаємодію в рамках системи МВС України.

Визначимо ключові аспекти несанкціонованого доступу до інформаційних систем МВС (Рис 1.3.).

Рисунок 1.3. Ключові аспекти несанкціонованого доступу до інформаційних систем МВС

Розглядаючи ключові аспекти захисту інформації (ЗІ) в інформаційних системах МВС, важливо відзначити, що всебічний захист передбачає застосування конкретних правових, фізичних, організаційних та програмно-апаратних механізмів, що мають гарантувати ідентифікацію та автентифікацію користувачів, розмежування прав доступу до технічних ресурсів, інформаційних активів та сервісів ІС, а також реєстрацію та облік спроб несанкціонованого доступу (НСД).

У юридичній літературі захист інформації — це сукупність організаційних і технічних заходів, а також правових норм, які призначені для запобігання

шкоді, яку може завдати особа, що користується інформацією, або власнику самої інформації [11 с. 67]. Одним із ключових засобів забезпечення інформаційної безпеки у складних інформаційних системах є вдосконалення системного підходу до визначеної проблеми. Системний підхід розробляє не лише відповідні механізми захисту, але й впровадження цілісного процесу, який охоплює всі етапи життєвого циклу інформаційної системи, використовуючи при цьому всі доступні ресурси для гарантування безпеки.

Організаційні заходи ЗІ в ІС традиційно націлені на чітке визначення зон відповідальності персоналу в процесі обробки даних, створення багаторівневої системи контролю, нейтралізацію зовнішніх та внутрішніх загроз, а також на запобігання навмисному чи ненавмисному видаленню або модифікації інформації. Доступ до інформаційних ресурсів МВС дозволяється, якщо гарантується захист інформації, відповідно до законів, зокрема для технічного захисту інформації в ІТС.

Забезпечення інформаційної безпеки підрозділами МВС має чотири рівні (Рис 1.4.):

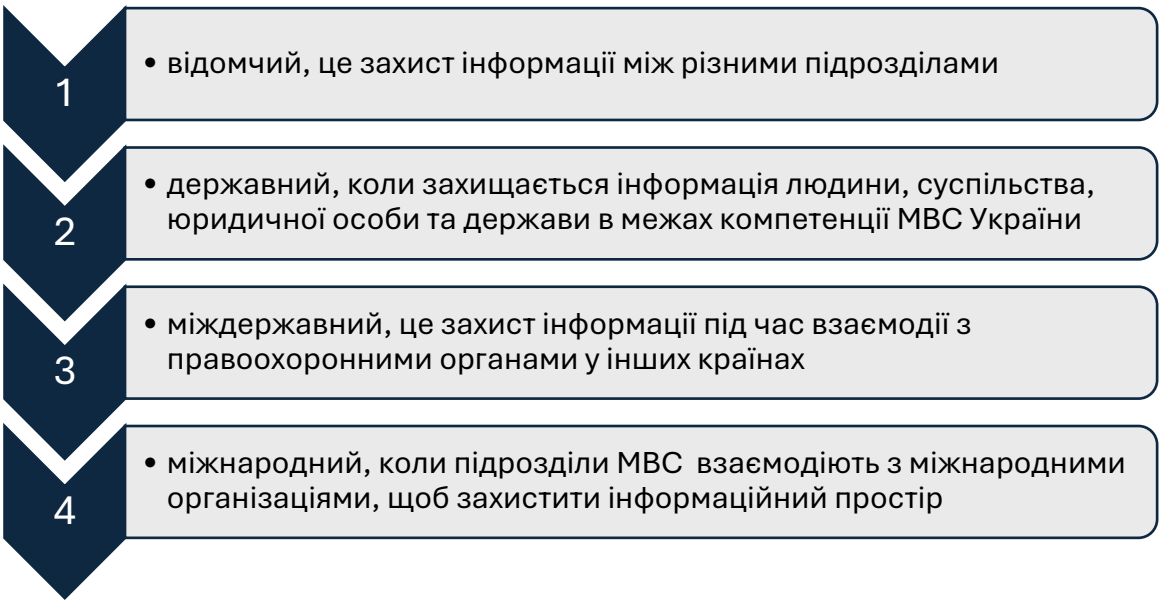


Рисунок 1.4. Рівні забезпечення інформаційної безпеки підрозділами МВС

Забезпечення належного рівня технічного захисту інформації під час експлуатації інформаційних ресурсів Міністерства внутрішніх справ покладається на усі інституції, які здійснюють освітню діяльність,

перекваліфікацію та підвищення професійного рівня користувачів, у рамках їхнього технічного потенціалу та сфери компетенцій. Регулювання доступу сторонніх осіб до інформаційних ресурсів Міністерства внутрішніх справ України здійснюється згідно з положеннями спеціалізованого технічного документу, який визначає організаційно-технічні заходи для забезпечення комплексного захисту даних на типовому робочому місці зовнішнього користувача Національної автоматизованої інформаційної системи МВС України. Цей документ отримав підтвердження відповідності від Державної служби спеціального зв'язку та захисту інформації України.

Аналізуючи загальні принципи захисту інформації в інформаційних системах МВС України, варто зазначити, що комплексний захист інформаційних систем передбачає застосування сукупності спеціальних правових, фізичних, організаційних і програмно-апаратних заходів. Вони спрямовані на забезпечення безпеки даних та інформації, розподіл прав доступу до технічних і інформаційних активів та сервісів системи, контроль за спробами несанкціонованого доступу, а також реєстру.

Законодавчі заходи щодо захисту службової інформації — це виконання чинних законів або прийняття нових документів, які встановлюють відповідальність для працівників за витік, втрату або зміну конфіденційної інформації. Також вони визначають відповідальність інших осіб за несанкціонований доступ до цієї інформації [33, 40]. Ці заходи призначені для запобігання порушенням закону та встановлення відповідальності за такі дії.

Ось ключові завдання забезпечення інформаційної безпеки:

• Захищеність інформації: важливе обмеження доступу до певних даних, що передбачено для конкретного кола користувачів.

• Унеможливлення несанкціонованого доступу: забезпечення секретності конфіденційних даних та виключення їх поширення серед сторонніх осіб.

• Цілісність інформації: гарантування правдивість та незмінності інформації на всіх етапах її життєвого циклу – від створення до виводу, включно з усіма процесами, що її супроводжують (збір, обробка тощо).

• Доступність інформації: організація оперативного та безперешкодного доступу користувачів до необхідних відомостей.

• Зменшення ризиків: мінімізація негативних наслідків шляхом впровадження компенсаційних заходів для забезпечення інформаційної безпеки.

• Облік, контроль та аналіз усіх процесів, що впливають на ризики інформаційної безпеки.

Організаційні заходи захисту в інформаційних системах МВС України, як правило, спрямовані на чіткий розподіл відповідальності серед персоналу в процесах обробки інформації, створення кількох етапів контролю, запобігання зовнішнім та внутрішнім загрозам, навмисному або непередбаченому знищенню та зміні інформації. Організація захисту комп’ютерних інформаційних мереж та систем структурує функціонування ключових підсистем, регламентує застосування обладнання й ресурсів, а також взаємовідносини користувачів, дотримуючись встановлених правових норм і правил. Безпека інформації, забезпечена організаційними методами, є критично важливою для надійності та продуктивності, оскільки несанкціонований доступ і витік даних часто виникають через зловмисні наміри, недбалість користувачів або помилки персоналу. Ці загрози майже нереально усунути чи обмежити виключно за допомогою апаратних, чи програмних засобів, криптографічного захисту чи фізичних бар'єрів, тому комплекс організаційних, організаційно-правових та організаційно-технічних заходів, що інтегровані з технічними методами, покликаний мінімізувати, обмежити або повністю уникнути втрат внаслідок впливу різних деструктивних чинників [35, 36].

Одним з ключових організаційних рішень є формування спеціальних штатів з безпеки інформації всередині закритих інформаційних систем, а саме – посади адміністратора безпеки банків даних, розподілених баз та мережі, де

зберігаються конфіденційні відомості. Без сумніву, організаційні заходи потребують ретельного планування, спрямування та виконання через конкретну організаційну структуру – окремий підрозділ, що формується з урахуванням необхідності укомплектування фахівцями, що забезпечують безпеку функціонування та захист інформації [43, 46].

Організаційні заходи зосереджені на формуванні концепції інформаційної безпеки та охоплюють такі ключові напрями:

- створення посадових інструкцій для користувачів і працівників, які надають відповідні послуги;

- запровадження правил управління компонентами інформаційної системи, процедур зберігання та утилізації носіїв даних, а також механізмів ідентифікації користувачів;

- розроблення планів реагування на спроби несанкціонованого доступу до ресурсів системи, визначення інструментів захисту і алгоритмів дій в умовах небезпечних ситуацій;

- навчання користувачів основним принципам і правилам забезпечення інформаційної безпеки. Технічний захист інформації здійснюється в кілька послідовних етапів.

1. Перший етап зосереджений на визначенні та аналізі потенційних загроз. Проводиться детальне вивчення об’єктів, які потребують захисту, аналізуються умови функціонування інформаційної системи, оцінюється ймовірність виникнення загроз і потенційні збитки у разі їх реалізації.

2. Другий етап передбачає розробку системи захисту інформації, яка включає створення плану заходів із забезпечення безпеки. План охоплює організаційні заходи, початкові технічні дії та основні технічні аспекти. У рамках цього етапу визначаються зони інформаційної безпеки. Організаційні заходи покликані забезпечити впорядкованість інформаційних процесів у відповідності до встановлених вимог і нормативів технічного захисту інформації на всіх етапах життєвого циклу інформаційної системи. Початкові технічні заходи

забезпечують захист без використання спеціалізованих засобів ТЗІ, тоді як основні технічні дії включають застосування таких спеціалізованих засобів.

Ці заходи мають бути пропорційними до актуальних загроз, враховувати можливі витрати та наслідки в разі їх реалізації, а також забезпечувати необхідний рівень ефективності протягом часу, коли доступ до інформації має бути обмеженим або загрози ліквідовані. Для мінімального рівня захисту впроваджуються обмежувальні та вибіркові заходи, які запобігають найбільш серйозним загрозам.

3. На третьому етапі реалізуються всі заплановані організаційні, первинні та основні технічні заходи, спрямовані на забезпечення захисту, визначення зон безпеки, проведення атестації технічних засобів для підтримки інформаційної діяльності й охорони даних. Також перевіряється відповідність робочих місць встановленим вимогам безпеки. Такий підхід дає змогу забезпечити комплексний і системний захист інформації, враховуючи актуальні загрози та потреби.

Робота з технічного супроводу передбачає використання надійного програмного й технічного забезпечення для гарантування інформаційної безпеки, а також регулярний контроль їхньої ефективності. Усі засоби повинні бути сертифіковані на відповідність стандартам або мати дозвіл на використання, виданий офіційними органами КМУ. Крім того, застосовуються спеціалізовані інженерно-технічні споруди, системи й засоби.

На четвертій стадії відбувається аудит функціональних можливостей та ефективності управління системи захисту інформації в інформаційних інфраструктурах. Ключовим завданням цього етапу є визначення ступеня захищеності інформаційних систем, ідентифікація потенційних вразливостей та мінімізація ризиків їхньої реалізації. Такі перевірки здійснюються згідно з регламентованими планами, санкціонованими керівним складом підрозділів, шляхом проведення комплексного аналізу позиції інформаційної безпеки.

Інформаційно-захисні системи, засновані на технологічних інноваціях, розробляються відповідно до низки ключових принципів, що забезпечують їхню здатність ефективно нейтралізувати широкий спектр кіберзагроз. Основним концептуальним підходом у цій галузі є захист превентивного характеру, оскільки ліквідація наслідків потенційних загроз потребує суттєвих фінансових, часових та матеріальних витрат. Істотним аспектом є також диференціація захисних заходів з урахуванням їхньої критичності, вірогідності виникнення загроз та потенційної можливості їхньої реалізації. Принцип ефективної протидії загрозам передбачає досягнення адекватного рівня безпеки без надмірного ускладнення архітектури системи інформаційної безпеки [46].

Інформаційна безпека в діяльності структурних підрозділів Міністерства внутрішніх справ України становить невід'ємну умову та ключовий елемент інтегрованої системи забезпечення національної безпеки. Вона реалізується у сфері правових взаємовідносин між компетентними органами підрозділів МВС, а також між ними та іншими суб'єктами інформаційного середовища, зокрема фізичними особами, суспільством, державними інституціями та юридичними особами. Головною метою цих взаємин є гарантування безпеки інформаційного простору від усіляких деструктивних впливів. Структурні підрозділи МВС, виконуючи свої функціональні обов'язки з надання сервісів, здійснюють охорону прав і свобод громадян, захист інтересів суспільства та держави, а також підтримують публічний порядок і безпеку.

Сучасні методи забезпечення інформаційної безпеки, які використовуються у діяльності Міністерства внутрішніх справ України, відіграють ключову роль у захисті державних інтересів та підтримці безпечного інформаційного середовища, класифікуються таким чином:

- ✓ технічні засоби (активні та пасивні), призначені для запобігання несанкціонованому витоку даних, які експлуатують різні фізичні властивості, що виникають у процесі обробки інформації;

- ✓ апаратно-програмні комплекси, що реалізують розмежування рівнів доступу до інформації, ідентифікацію та автентифікацію користувачів;
- ✓ програмно-технічні рішення, які забезпечують конфіденційність та автентичність інформації під час її передачі по комунікаційних каналах;
- ✓ програмно-технічні інструменти, орієнтовані на збереження цілісності програмного забезпечення та запобігання неправомірному копіюванню;
- ✓ програмні засоби, які забезпечують захист інформації від шкідливого впливу вірусів та іншого небезпечного програмного забезпечення;
- ✓ фізичні та хімічні методи захисту, що підтверджують автентичність документів, гарантують їхню безпечність під час транспортування та виключають можливість підробки.

Сучасний ринок програмного забезпечення надає широкий вибір рішень, орієнтованих на інформаційну безпеку. Захисні програмні системи забезпечують ідентифікацію користувачів, контроль їхніх прав доступу, створюють безпечний доступ до ресурсів, впроваджують криптографічний захист даних, а також ефективно протидіють вірусам та іншим видам загроз. Ці програмні рішення класифікуються як системні та прикладні. Для досягнення високого рівня безпеки необхідно впроваджувати комплексний підхід, який враховує як внутрішні, так і зовнішні загрози. Основою цього підходу стає взаємодія програмних, технічних та організаційних інструментів. Розроблення цілісної та добре спланованої концепції безпеки забезпечить належний захист і допоможе сформувати оптимальну стратегію управління ризиками. Ґрунтовний аналіз інформації та даних виступає ключовим фактором для визначення найбільш ефективної моделі захисту. Забезпечення доступу до чітких і оновлених інформаційних ресурсів правоохоронним органам, співпраця між ними як на міжвідомчому, так і на міжнародному рівні, а також використання сучасних технологій для безпечної роботи з інформацією — це важливі елементи ефективної системи правоохоронних заходів. Постійне вдосконалення

інформаційних технологій та процесів аналізу та обробки даних має визначальну роль у збільшенні ефективності роботи правоохоронних органів та забезпеченні гармонійного розвитку суспільства [44]

В Україні чинні такі стандарти технічного захисту інформації:

– ДСТУ 3396.0-96 «Захист інформації. Технічний захист інформації. Основні положення». Цей нормативний акт окреслює сутність об'єктів, задач та організаційних принципів забезпечення технічного захисту інформації (ТЗІ). Його метою є убезпечення від несанкціонованого доступу до інформації, наслідком якого може бути шкода для громадян, організацій (юридичних осіб) та держави, а також визначення категорій нормативних документів у системі ТЗІ.

– ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок виконання робіт». Цей стандарт визначає обов'язкові вимоги до процесу здійснення робіт, пов'язаних з технічним захистом інформації.

– ДСТУ 3396.2-96 «Захист інформації. Технічний захист інформації. Терміни та визначення». Розглядає визначення понять і термінів у сфері технічного захисту інформації. Серед найпомітніших міжнародних стандартів з інформаційної безпеки можна виділити британський стандарт BS 7799, створений Британським інститутом стандартів (BSI). Цей стандарт складається з двох частин. Серія стандартів управління інформаційною безпекою ISO/IEC 27000 була створена підкомітетом SC 27 технічного комітету ISO/IEC JTC 1.

РОЗДІЛ 2
ПРАВОВІ ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМАХ МВС УКРАЇНИ

2.1. Міжнародні стандарти правового регулювання захисту інформації в інформаційно-аналітичних системах

Міжнародні документи мають важливе значення для правової основи інформаційно-аналітичної діяльності, бо вони встановлюють загальні стандарти та правила, які повинні дотримуватися правоохоронними органами. Правове регулювання інформаційно-аналітичної діяльності ґрунтується на міжнародних угодах. Розглянемо приклади. Наприклад, Конвенція про права людини та основні свободи, прийнята Радою Європи у 1950 році, забезпечує права на особисту та конфіденційну інформацію, а також право на повагу до приватного та сімейного життя, яке може включати збереження конфіденційності (ст. 8)[14]. Також Конвенція ООН проти транснаціональної організованої злочинності визначає відповідність в обміні інформацією між учасниками (ст. 43), що сприяє взаємодії правопорядку між органами. Конвенція ООН проти корупції (ст. 46) зобов'язує сучасні країни забезпечувати конфіденційність інформації, що міститься в документах, спрямованих на боротьбу з корупцією [28].

До ключових суб'єктів міжнародних інформаційно-правових зв'язків, яким надано повноваження щодо формування норм, належать інституції, що займають особливе місце: Рада Європи, ООН, та її Генеральна Асамблея, Всесвітня асамблея зі стандартизації телекомунікацій, Всесвітній конгрес інформаційних технологій, Всесвітній саміт інформаційного суспільства, Європейська комісія з прав людини, Європейський регіональний форум з управління Інтернетом, Міжнародна організація стандартизації, Організація з безпеки та співробітництва в Європі, Міжнародний Союз електрозв'язку та ін.

Основними документами, що створюються міжнародними організаціями, виступають декларації, конвенції, рекомендації, рішення, а також міждержавні договори, які після ратифікації стають основою для розробки норм національного законодавства. На базі закріплених договірних принципів формується правовий режим, що чітко визначає права, зобов'язання та відповідальність суб'єктів міжнародно-правових інформаційних відносин. Цей режим відображається у складній системі дозволів, приписів, обмежень і заборон, які встановлюють нормативні моделі бажаної правової поведінки для як колективних, так і індивідуальних учасників міжнародного права.

Міжнародні документи встановлюють стандартні правила і принципи, які впроваджуються в національне законодавство. Національні органи правопорядку дотримують ці принципи під час своєї роботи зі збору та аналізу інформації. Це допомагає покращити рівень правового захисту людини та зміцнити міжнародну співпрацю у боротьбі зі злочинністю та правопорядком. Міжнародні стандарти інформаційної безпеки — це правила охорони, розроблені для взаємодії між виробниками, споживачами та експертами, що здійснюють кваліфікацію продуктів інформаційних технологій у процесі розробки та експлуатації безпечних систем обробки даних [50].

У Фінляндії, Ірландії та Австрії, як і у всіх державах-членах Європейського Союзу, питання кібербезпеки має велике значення. У документах Європейської комісії, таких як «На шляху до загальної політики у сфері боротьби з кіберзлочинністю», визначено, що кіберзлочинність охоплює кримінальні дії, які здійснюються через електронні комунікаційні мережі або інформаційні системи, а також ті, що спрямовані проти них. Сюди входять такі злочини, як традиційні порушення закону, наприклад крадіжки чи фальсифікації, що здійснюються за допомогою електронних мереж та систем.;

- ✓ розповсюдження незаконного контенту через електронні медіа;
- ✓ специфічні злочини в електронних мережах, такі як атаки на інформаційні системи або хакерство.

Виявлено кілька ключових проблем, пов'язаних із забезпеченням безпеки інформаційних структур, які впливають на їхню ефективність на національному та міжнародному рівнях. По-перше, спостерігається відсутність узгоджених внутрішніх підходів до формування системи безпеки інформаційних структур, що суттєво знижує ефективність реалізації національних заходів. По-друге, на європейському рівні відзначається недостатній рівень співпраці між державними установами та приватним сектором, що створює бар'єри для комплексного підходу до вирішення безпекових завдань. Крім того, обмежені можливості для своєчасного попередження та реагування на інциденти у сфері безпеки обумовлені нерівномірним розвитком систем моніторингу та оповіщення в різних країнах-членах, а також недостатнім міждержавним співробітництвом і обміном інформацією з цього питання. Нарешті, відсутність міжнародного консенсусу щодо визначення пріоритетів у реалізації політики захисту критичної інформаційної інфраструктури значно ускладнює ефективне розв'язання актуальних безпекових викликів.

НАТО та ЄС активно впроваджують політику у сфері інформаційної безпеки. Сьогодні Європейський Союз об'єднує розвинені держави, які здійснюють вагомий вплив на міжнародну взаємодію, впроваджуючи правила та стандарти поведінки країн у різних аспектах: політичному, економічному, соціальному, інформаційному та інших. У 1991 році були розроблені «Європейські критерії безпеки інформаційних технологій», які окреслювали ключові завдання у забезпеченні інформаційної безпеки, зокрема:захист інформаційних ресурсів від несанкціонованого доступу, щоб забезпечити конфіденційність;

- ✓ забезпечення цілісності інформаційних ресурсів через їх захист від несанкціонованої модифікації або знищення;
- ✓ забезпечення працездатності систем шляхом протидії загрозам відмови в обслуговуванні.

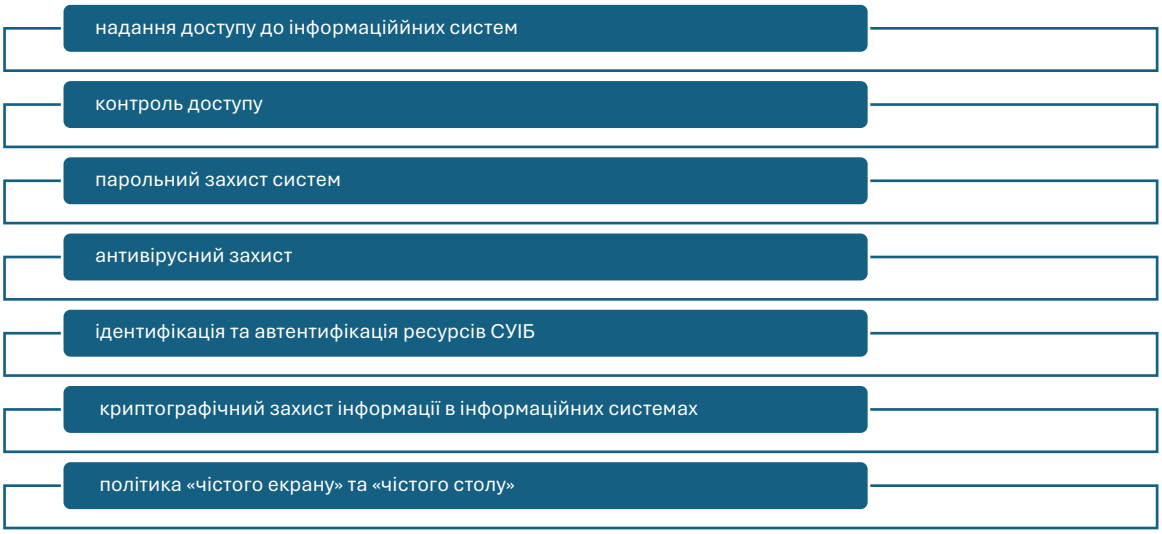


Рисунок 2.1. Міжнародно визнані складові політики інформаційної безпеки

Пріоритетні аспекти забезпечення інформаційної безпеки на глобальному рівні включають:

- Підвищення обізнаності користувачів щодо потенційних загроз, які можуть виникати під час використання комунікаційних мереж.

- Формування загальноєвропейської системи для реагування на нові виклики та повідомлення про них.

- Надання технічної підтримки для забезпечення інформаційної стійкості.

- Впровадження стандартів, які відповідають вимогам ринку, а також сертифікація продукції.

- Забезпечення правового регулювання для захисту персональних даних, встановлення норм у сфері телекомунікаційних послуг і боротьби з кіберзлочинністю.

- Посилення державної інформаційної безпеки через впровадження ефективних, взаємодоповнюючих засобів захисту, а також популяризацію електронного підпису у процесах надання державних онлайн-послуг.

- Стимулювання міжнародного співробітництва у сфері інформаційної безпеки.

Держави-члени Європейського Союзу вибудували частково інтегровану систему захисту інформації. Водночас кожна країна зберігає право на самостійне формування власної нормативно-правової бази та регуляторних положень, що стосуються питань інформаційної безпеки. У контексті забезпечення міжнародної кібербезпеки мандат Організації Об'єднаних Націй спрямований на створення міжнародно-правових інструментів для протидії незаконному використанню новітніх науково-технічних досягнень. Забезпечення глобальної інформаційної безпеки стало одним із пріоритетних завдань спеціалізованих установ ООН, особливо в умовах формування світового інформаційного суспільства. Ця тема має особливе значення для таких організацій, як ЮНЕСКО та Міжнародний союз електрозв'язку, які активно впроваджують гуманітарні й технічні програмні ініціативи та проєкти.

Одним з провідних суб'єктів нормотворення у сфері міжнародної інформаційної безпеки виступає ENISA – Агентство Європейського Союзу з питань мережевої та інформаційної безпеки. Його відповідальність полягає у забезпеченні належного рівня кібербезпеки на території Європи. ENISA було засновано у 2004 році, а його повноваження були розширені з прийняттям Акту ЄС про кібербезпеку. Агентство активно сприяє реалізації кіберполітики ЄС, підвищуючи рівень стійкості та довіри до продуктів, послуг і процесів у сфері інформаційно-комунікаційних технологій (ІКТ) шляхом впровадження механізмів сертифікації кібербезпеки. Воно взаємодіє з державами-членами ЄС та їхніми відповідними національними інституціями, сприяючи готовності Європи до майбутніх кіберзагроз. Завдяки обміну знаннями, нарощуванню потенціалу та підвищенню обізнаності, Агентство співпрацює з ключовими стейкхолдерами, забезпечуючи довіру до цифрової економіки, зміцнюючи резистентність інфраструктури ЄС та, зрештою, гарантуючи захист європейського суспільства та його громадян у цифровому просторі.

Завдяки оперативному запровадженню сучасних інформаційних технологій у всі галузі функціонування інформаційно аналітичних систем, з'явилася

необхідність сформувати єдину систему стандартів інформаційної безпеки, що мала б бути універсальною й ефективною. Нині міжнародні стандарти розробляються спільно Міжнародна організація зі стандартизації (ISO) а також Міжнародна електротехнічна комісія (IES) [2]. Система управління інформаційною безпекою ґрунтується на ряді стандартів. BS 7799-1: 2005 — Британський стандарт, перша частина. BS 7799 Частина 1, відомий як Кодекс практик в управлінні інформаційною безпекою, включає 127 контрольних механізмів, які необхідні для впровадження системи управління інформаційною безпекою. Всі ці механізми розроблені на основі найкращих практик у відповідній сфері.

Система кібербезпеки, яка використовує міжнародні стандарти, дуже важлива сьогодні, коли все стає цифровим. Міжнародні стандарти розробляються разом Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC). Зараз спеціалісти цих організацій створили серію стандартів ISO/IEC 27000, яка постійно розширюється новими документами. В Україні вживаються стандарти серії ДСТУ ISO/IEC 27000, які відповідають міжнародним вимогам ISO/IEC 27000. До них належать наступні:

ДСТУ ISO/IEC 27000:2019 — це документ, який стосується інформаційних технологій, методів захисту і систем управління інформаційною безпекою. Документ надає узагальнений огляд систем управління інформаційною безпекою (СУІБ) та визначає ключові терміни, що застосовуються у рамках стандарту СУІБ. Він є універсальним і підходить для використання в організаціях будь-якого типу — комерційних, державних чи приватних. У тексті наводяться загальні терміни та визначення, пов’язані з сімейством стандартів СУІБ. Водночас, документ не охоплює всіх термінів, присутніх у цих стандартах, і не передбачає створення нових визначень для конкретних понять СУІБ.ДСТУ ISO/IEC 27001:2015 — це стандарт, що стосується інформаційних технологій, а саме методів забезпечення безпеки інформації. Він розроблений для того, щоб

допомогти організаціям розробляти, впроваджувати, підтримувати та постійно покращувати систему управління безпекою інформації, враховуючи конкретні умови кожної організації. Також у стандарті наведено вимоги щодо аналізу та вирішення ризиків, які виникають у зв'язку з потребами організації. Вимоги, що містяться в цьому стандарті, є загальними та призначені для застосування усіма організаціями, незалежно від їх типу, розміру або природи. Вилучити будь-яку вимогу, вказана в розділах 4–10, неправомірно, якщо організація хоче відповідати цьому стандарту.

Документ ДСТУ ISO/IEC 27005:2019 "Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки" (базується на ISO/IEC 27005:2018, IDT) надає рекомендації щодо управління ризиками з метою забезпечення інформаційної безпеки. Він підтримує загальні ідеї, визначені у стандарті ISO/IEC 27001, і призначений для допомоги організаціям у реалізації ефективної інформаційної безпеки, використовуючи підхід до управління ризиками. Важливо знати концепції, моделі, процеси та термінологію, які описані в ISO/IEC 27001 та ISO/IEC 27002, щоб повністю зрозуміти цей документ. Цей стандарт прагне застосовуватися у всіх організаціях, незалежно від їх типу — комерційних, державних або некомерційних — які хочуть керувати ризиками, що можуть вплинути на безпеку їх інформації.

ДСТУ ISO/IEC 27006:2015 — це стандарт, який стосується інформаційних технологій та методів захисту. Він встановлює вимоги та навчає, як повинні діяти організації, які надають послуги з аудиту та сертифікації систем управління інформаційною безпекою (СУІБ), крім того, він враховує вимоги ISO/IEC 17021-1 та ISO/IEC 27001. Основна мета цього стандарту — допомогти організаціям, які проводять сертифікацію СУІБ, отримати акредитацію. Усі вимоги стандарту мають бути зрозумілі кожній організації, яка проводить сертифікацію СУІБ, а приклади, додані до стандарту, пояснюють ці вимоги. Цей стандарт можна використовувати як основу для акредитації, експертного огляду або інших процесів аудиту.

На 72-й сесії Генеральної Асамблеї ООН, що відбулася 11 серпня 2017 року, було оприлюднено повідомлення Генерального секретаря ООН (A/72/315). Цей документ став відповіддю на резолюцію A/RES/71/28, ухвалену 5 грудня 2016 року, яка передбачала інформування країн про їхню позицію щодо загальної оцінки міжнародної інформаційної безпеки та заходів, які вони здійснюють у цьому напрямку. У межах цього повідомлення були представлені офіційні звіти урядів 23 країн, спрямовані на підтримку міжнародної безпеки та розвиток міжнародного співробітництва у зазначеній сфері. [63].

Стрімке поширення кіберзагроз у сучасному світі підштовхнуло Генеральну Асамблею ООН до важливих рішень. У 2019 році було ухвалено резолюцію A/RES/74/28, яка наголошує на необхідності забезпечення відкритого, безпечного, стабільного, доступного та мирного інформаційно-комунікаційного середовища. Цей документ наголошує на важливості формування довіри між державами, розвитку міжнародної співпраці та стимулювання застосування сучасних технологій для зниження ризику виникнення конфліктів, що безпосередньо впливає на підтримання глобальної безпеки.

Ще одним визначним кроком стало ухвалення резолюції A/RES/74/247 від 27 грудня 2019 року, згідно з якою було створено спеціальний міжнародний комітет з відкритим складом. До комітету ввійшли експерти та представники різних регіонів, а його метою стала підготовка універсальної міжнародної конвенції для запобігання злочинному використанню інформаційно-комунікаційних технологій. Пізніше, 26 травня 2021 року, за резолюцією A/RES/75/282, було вирішено, що комітет організує щонайменше шість сесій для завершення роботи над проєкт конвенції. Документ мав бути представлений на 78-й сесії Генеральної Асамблеї ООН, яка проходила у вересні 2023 року.

У цьому контексті можна виокремити різні аспекти міжнародної інформаційної безпеки: глобальна інформаційна безпека, захист інформаційного простору окремих країн, а також забезпечення безпеки установ у міжнародному

інформаційному середовищі. Ці ключові концепції також знайшли відображення в документах ООН [62].

Огляд законодавчої та нормативної бази захисту інформаційно-аналітичних систем вимагає їх систематизації та поділу на групи. Як критерії для цього можна використовувати такі аспекти:

1) характер дії (глобальні, універсальні, спеціальні, регіональні, національні акти);

2) за терміном дії (строкові, безстрокові);

3) за порядком прийняття (акти, прийняті до початку цифрової епохи, сучасні);

4) за юридичною силою (чинні, втративши чинність);

5) за формою закріплення норм (декларації, конвенції, хартії, договори, угоди, резолюції, директиви, рекомендації тощо);

6) за предметом регулювання та пріоритетністю зв'язків між учасниками (гуманітарні, стандартизовано-технічні);

7) за кількістю учасників (односторонні, двосторонні, багатосторонні);

8) за ступенем обов'язковості (обов'язкові для виконання, рекомендаційні);

9) за ступенем офіційності (офіційні, неофіційні);

10) за способом впровадження в національне законодавство (акти безпосередньої дії, акти, які вимагають ратифікації, акти для імплементації);

11) за наявністю контролю за виконанням (акти, які передбачають міжнародний контроль, та акти, де такого контролю немає);

12) за процесуальним потенціалом (акти, що передбачають санкції за порушення чинних норм і використовуються в судових справах, а також акти, що регулюють етичні норми).

Дотримання галузевих, внутрішніх і міжнародних стандартів є важливим свідченням прихильності держави до питань захисту даних, відповідності нормативним вимогам і ефективного управління ризиками. У сучасних умовах глобального обміну інформацією та кроскордонної обробки даних набуває все

більшого значення розробка уніфікованих міжнародних стандартів і правил. Це необхідно для забезпечення гармонізації та взаємної сумісності законодавства, яке регулює функціонування інформаційно-аналітичних систем. Необхідність створення міжнародних документів із єдиними нормами для регулювання інформаційної безпеки стала очевидною через стрімкий розвиток інформаційного суспільства. Інформаційна безпека часто виступає ключовим пріоритетом для держави, оскільки вона визначає, з одного боку, рівень захищеності суспільства від негативного впливу шкідливої інформації, а з іншого – швидкість і ефективність його розвитку в різноманітних сферах завдяки використанню накопиченого досвіду та знань.

У контексті забезпечення інформаційної безпеки національного і міжнародного рівня необхідно посилити та розширити зусилля, спрямовані на формування умов для створення глобальної системи інформаційної безпеки. Ця система має будуватися на загальновизнаних принципах і нормах міжнародного права, які забезпечать її стійкість і ефективність у сучасному динамічному середовищі.

2.2. Правове регулювання захисту інформаційно-аналітичних систем в МВС України

Актуальність сучасного правового регулювання інформаційно-аналітичної діяльності підрозділів МВС України обумовлена низкою чинників. До них належать: безперервне розроблення та імплементація новітніх методик забезпечення інформаційної безпеки систем, що функціонують у відомстві; інтеграція нових інформаційно-аналітичних продуктів у роботу різноманітних підрозділів МВС; послідовна інтеграція інструментів штучного інтелекту для обробки значних обсягів даних; постійна потреба у забезпеченні законності, прозорості та захисту прав і свобод громадян під час здійснення інформаційно-аналітичної роботи підрозділами МВС; а також збільшення кола суб'єктів, яким

надається доступ до інформаційних ресурсів МВС. Отже, перманентна значущість нормативно-правового регулювання інформаційно-аналітичної діяльності підрозділів МВС обумовлює необхідність ґрунтовного наукового дослідження та аналізу.

Правове регулювання інформаційної безпеки (ІБ) на державному рівні охоплює як дотримання чинного законодавства, так і ухвалення нових нормативно-правових актів та інструкцій. Вони покликані встановлювати правову відповідальність для службових осіб за розголошення, втрату, модифікацію або неправомірне використання захищеної службової інформації, включаючи перевищення службових повноважень у цьому контексті. Також передбачається відповідальність сторонніх суб'єктів за навмисні дії з несанкціонованого доступу до інформації. Прикінцева мета цих юридичних заходів полягає у превенції потенційних правопорушень та притягненні до відповідальності за вчинені делікти [2].

Ключовим аспектом забезпечення інформаційної безпеки держави, зокрема у контексті діяльності МВС, є міжнародна активність України, яка передбачає ретельне висвітлення подій, що мають пряме відношення до фундаментальних засад державного існування. Аналіз сучасного інформаційного простору вказує на те, що Україна розглядається як об'єкт інформаційних атак, мета яких – встановлення домінації над усіма сферами життя незалежної держави. Недооцінка значущості використання інформаційного впливу з боку України для просування національних інтересів та державної політики за кордоном, як демонструють останні події, призводить до значних економічних, політичних, репутаційних та інших втрат для держави.

З огляду на інтенсивне впровадження цифрових технологій у всі сфери суспільного життя, на передовий план виходить роль як міжнародних, так і національних правових інструментів, спрямованих на забезпечення безпеки інформаційного простору. Ці інструменти передбачають вдосконалення та уніфікацію нормативно-правової бази у сфері інформаційного захисту на

державному та міжнародному рівнях. Водночас, активне просування парадигми цифрового суверенітету в останні роки генерує потребу у комплексному дослідженні проблематики, пов'язаної із встановленням та підтримкою контролю над інформацією, комунікаціями, даними та відповідною інфраструктурою, включно з інтернет-простором. Це, своєю чергою, зумовлює потребу в аналізі правових механізмів, завдяки яким здійснюється охорона інформаційної безпеки.

Правове регулювання інформаційних відносин в Україні має чітко структуровану ієрархію, що охоплює кілька основних рівнів: Конституцію України, законодавчі акти, укази та розпорядження Президента, постанови і розпорядження Кабінету Міністрів, а також нормативно-правові акти центральних органів виконавчої влади. У межах цієї правової бази формуються і функціонують інформаційні підрозділи Міністерства внутрішніх справ України, які становлять єдину управлінську систему. Основою їхньої діяльності є виконання положень чинного законодавства, обов'язкове дотримання якого виступає ключовою умовою.

Ця нормативно-правова база насамперед включає Конституцію України, яка передбачає, що функціонування правоохоронних органів ґрунтується на відповідних законах. До неї належать також Кримінальний кодекс і Кримінально-процесуальний кодекс України, а також закони України «Про Національну поліцію», «Про доступ до публічної інформації», «Про державну таємницю», «Про звернення громадян», «Про інформацію» та «Про друкарські засоби масової інформації (пресу) в Україні» (Додаток В).

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»- є базовим. Він визначає правові, організаційні та технічні засади захисту інформації, а також встановлює вимоги до створення комплексної системи захисту інформації (КСЗІ). Для ІАС МВС, які обробляють інформацію з обмеженим доступом, створення КСЗІ з атестатом відповідності є обов'язковим.

Закон України «Про кібербезпеку» - встановлює організаційно-правові засади захисту критичної інформаційної інфраструктури, до якої належать ключові ІАС МВС. Законом визначені суб'єкти забезпечення кібербезпеки: МВС є одним із суб'єктів, відповідальних за власний кіберзахист. Закон встановлює механізми виявлення, реагування та усунення наслідків кібератак.

Правове регулювання обігу інформації є фундаментальним аспектом діяльності Міністерства внутрішніх справ. Зокрема, Законом України «Про державну таємницю» визначаються засади доступу, циркуляції та охорони відомостей, що віднесені до державної таємниці, обробка яких здійснюється у спеціалізованих сегментах інформаційно-аналітичних систем (ІАС) МВС. Водночас, Законом України «Про захист персональних даних» встановлюються норми обробки персональних відомостей.

МВС, виступаючи суб'єктом розпорядження значними обсягами даних, несе відповідальність за гарантування їхньої безпеки, запобігаючи несанкціонованому втручанню, модифікації чи деструкції.

Центральним органом, уповноваженим на формування та забезпечення функціональної безпеки інформаційної системи підрозділів МВС, є Департамент інформатизації Міністерства внутрішніх справ України. Згідно з приписами законодавства України та відповідними нормативно-правовими актами центральних органів виконавчої влади, зазначений Департамент функціонує як структурна одиниця апарату МВС. Його діяльність охоплює організацію заходів, спрямованих на надання інформаційно-аналітичної підтримки правоохоронної діяльності в усіх підрозділах системи МВС, а також на забезпечення конфіденційності персональних даних у процесі їх обробки.

Інформаційно-аналітична діяльність (ІАД) підрозділів МВС становить ключовий компонент їхньої функціональності, що сприяє підтриманню правопорядку та національної безпеки. Вона інтегрує процеси збору, обробки, аналізу та застосування релевантної інформації з метою гарантування громадської безпеки, превенції злочинних діянь та захисту прав і свобод

громадян. Завдяки ІАД підрозділи МВС мають змогу здійснювати більш ефективне прогнозування криміногенних подій. Суттєвим аспектом цієї діяльності виступає аналіз акумульованих даних із застосуванням передових інструментів та методологій. Нормативно-правова база, що регламентує цю діяльність, сформована комплексом законодавчих актів, які детермінують її принципи, алгоритми та вимоги до збору, обробки та архівування інформації.

Алгоритм правового регулювання інформаційно-аналітичної діяльності підрозділів МВС України складається з кількох важливих етапів, які чітко визначені законами та правовими документами.

Початковим етапом є формулювання завдань та визначення цілей інформаційно-аналітичної діяльності відповідних відомств, що здійснюється у відповідності до чинного законодавства. На даній стадії встановлюється необхідний обсяг інформаційних ресурсів для збору, систематизації та архівування, з метою забезпечення громадської безпеки та підтримання правопорядку.

На наступній стадії здійснюється розробка та імплементація регламентів, що стосуються збору, обробки та зберігання даних. Це включає визначення процедур накопичення відомостей, застосування спеціалізованих програмних комплексів, а також встановлення періодів збереження отриманої інформації.

Третій етап передбачає створення та впровадження внутрішньовідомчих нормативно-правових актів, які регламентують інформаційно-аналітичну діяльність структурних підрозділів. Ці документи встановлюють чіткі регуляторні норми та процедури функціонування у цій сфері, забезпечуючи неухильне дотримання відповідними підрозділами законодавчих приписів.

На завершальному етапі пріоритетним є гарантування правового захисту персональних даних суб'єктів. Відповідно до статті 32 Конституції України, кожна особа має фундаментальне право на захист своїх приватних відомостей, тому при здійсненні інформаційно-аналітичної діяльності критично важливим є розробка та впровадження ефективних механізмів їхньої протекції. [1-2].

Фундаментальними засадами інформаційно-аналітичної діяльності структурних підрозділів Міністерства внутрішніх справ є принципи законності, об'єктивності, конфіденційності, системності та комплексності. Дотримання цих принципів гарантує ефективність та неупередженість у здійсненні інформаційно-аналітичної роботи згаданих відомств.

Нормативно-правова база, що регулює інформаційно-аналітичну діяльність підрозділів МВС України, ґрунтується на ряді ключових нормативно-правових актів. Серед них особливе значення мають:

Конституція України є основоположним юридичним документом, що визначає загальні принципи забезпечення правового захисту, зокрема закріплюючи право громадян на доступ до інформації, а також передбачаючи правові гарантії її збирання та обробки. Нормативне регулювання інформаційно-аналітичної діяльності відповідних структурних підрозділів Міністерства внутрішніх справ України перебуває в повній відповідності до положень Конституції України. Згідно зі статтею 3 цього документа, Україна проголошується правовою, демократичною та соціальною державою, зобов’язаною забезпечувати дотримання прав і свобод людини й громадянина як основоположної цінності. У статті 34 Конституції наголошується на праві кожної особи на отримання та поширення інформації. Водночас це право може підлягати певним обмеженням у випадках, коли існує загроза національній безпеці чи відбувається порушення прав і свобод інших осіб.

Відповідно до статті 19 Конституції України, органи державної влади, включно зі структурними підрозділами Міністерства внутрішніх справ, зобов’язані діяти виключно у межах своїх законодавчо визначених повноважень та в спосіб, передбачений Конституцією та чинними законами. Таким чином, діяльність у сфері інформаційно-аналітичного забезпечення Міністерства внутрішніх справ має бути суворо підпорядкована встановленим правовим нормам, закріпленим у законодавстві України.

Постанови Кабінету Міністрів України та накази Міністерства внутрішніх справ. Ці документи містять уточнення та конкретні вимоги щодо виконання інформаційно-аналітичної роботи в підрозділах МВС.

Міжнародні угоди та конвенції. Україна, як учасник різних міжнародних організацій, дотримує міжнародні стандарти та зобов'язання щодо інформаційно-аналітичної діяльності правоохоронних органів.

Законодавче забезпечення інформаційно-аналітичної роботи підрозділів МВС ґрунтується на міжнародних підставах, завдяки ратифікації низки міжнародних договорів. Зокрема, Конвенція ООН щодо боротьби з транснаціональною організованою злочинністю встановлює правила обміну даними між державами-учасниками (ст. 43), що сприяє ефективній інформаційній взаємодії правоохоронних органів. Конвенція ООН проти корупції (ст. 46) зобов’язує держави-учасниці гарантувати конфіденційність даних, що фіксуються у документах з протидії корупції. Крім того, Конвенція, прийнята ООН з питань боротьби з корупцією, формулює міжнародні норми, спрямовані на запобігання корупційним явищам та виявлення злочинів. Подібним чином, Конвенція щодо боротьби з тероризмом та Конвенція про організовану злочинність передбачають механізми обміну інформацією і спільних дій між правоохоронними структурами різних країн. Конвенція ООН проти корупції (ст. 13) зобов’язує суб’єктів дотримуватись конфіденційності даних, що містяться в актах протидії корупції

Правове регулювання роботи з інформацією та аналізом у підрозділах МВС України встановлюється наказами МВС. За положенням про єдину інформаційну систему Міністерства внутрішніх справ, затверджене постановою Кабінету Міністрів України від 14 листопада 2018 року № 1024 (у редакції постанови Кабінету Міністрів України від 15 серпня 2023 року № 866), інформаційно-аналітична діяльність має забезпечувати громадський порядок та боротьбу злочинністю. За статтею 8 цього положення, інформація, яка отримується під час

аналізу, має бути правдивою та об’єктивною. До роботи з такою інформацією мають бути допущені лише уповноважені працівники.

Правова регламентація інформаційно-аналітичної діяльності підрозділів Міністерства внутрішніх справ України базується на нормативно-правових актах, схвалених Кабінетом Міністрів України. Ці документи детально визначають процедури збирання, опрацювання та використання інформації у відповідній сфері. Зокрема, Постанова Кабінету Міністрів України від 14 листопада 2018 року № 591, яка затверджує Положення про єдину інформаційну систему Міністерства внутрішніх справ та окреслює перелік пріоритетних електронних ресурсів її структурних суб’єктів, формує основні завдання та цілі здійснення інформаційно-аналітичної діяльності в межах МВС України.

У відповідності зі статтею 6 цього документа, єдина інформаційна система МВС слугує платформою для автоматизації та технологічного забезпечення взаємного обміну інформацією між її суб’єктами. Основною метою функціонування системи є сприяння забезпеченню національної безпеки, охорони прав і законних інтересів громадян, а також загального блага суспільства і держави. Додатково, стаття 3 передбачає гарантовану конфіденційність інформаційно-аналітичних даних та встановлює обмеження доступу до них згідно з вимогами чинного законодавства.

Отже, нормативно-правові акти Кабінету Міністрів України виступають фундаментом для регулювання інформаційно-аналітичної діяльності підрозділів МВС України, забезпечуючи дотримання принципів законності, захисту даних та приватності в рамках виконання їх функцій.

Регулювання цієї діяльності також доповнюється відомчими нормативними документами МВС справ. Відповідно до «Положення про єдину інформаційну систему Міністерства внутрішніх справ», затвердженого постановою Кабінету Міністрів України від 14 листопада 2018 року № 1024 (у редакції постанови КМУ від 15 серпня 2023 року № 866), інформаційно-аналітична діяльність має на меті забезпечення громадського порядку та протидію злочинності. Згідно зі статтею

8 цього положення, відомості, отримані в результаті аналізу, повинні бути достовірними та об’єктивними. Опрацювання такої інформації дозволено виключно уповноваженим на це співробітникам.

Сучасні способи регулювання інформаційно-аналітичної роботи підрозділами МВС України ґрунтуються на комплексному підході до забезпечення правопорядку та безпеки громадян. Основними документами, які визначають ці способи, є закони, нормативні акти та міжнародні стандарти. По-перше, Закон України "Про захист інформації в інформаційно-комунікаційних системах", який встановлює загальні вимоги до захисту інформації, а також на інших нормативних актах, що регламентують діяльність МВС та його підрозділів, таких як Департамент інформаційно-аналітичної підтримки Національної поліції України. Цей закон встановлює основи роботи з аналізом інформації підрозділів МВС та визначає права та обов'язки співробітників у цій галузі.

Використання цифрових інструментів у інформаційно-аналітичній роботі підрозділів МВС проявляється через впровадження сучасних програмних технологій для збору, обробки та аналізу великих обсягів даних. Це дає змогу оперативно та ефективно опрацьовувати інформацію, виявляти тенденції та закономірності у сфері злочинності, а також прогнозувати ймовірність виникнення майбутніх кримінальних подій. Цифрові технології також відкривають нові можливості для співпраці з іншими правоохоронними органами та міжнародними партнерами завдяки швидкому обміну інформацією. Усе це сприяє підвищенню ефективності діяльності МВС і покращенню рівня безпеки громадян.

Правове підґрунтя для інформаційно-аналітичної роботи підрозділів МВС, засноване на принципах ефективності та результативності, забезпечується через відповідні нормативно-правові акти. У цих документах визначаються вимоги та стандарти, які регламентують роботу правоохоронних органів. Для досягнення максимальної результативності своєї діяльності МВС має активно інтегрувати

передові технології та сучасні підходи до обробки інформації. Застосування цифрових рішень, таких як системи аналізу даних і алгоритми машинного навчання, дозволяє швидко й ефективно аналізувати великі обсяги даних, встановлювати причинно-наслідкові зв'язки, визначати тренди у злочинності та прогнозувати можливі кримінальні ситуації.

Тому нормативно-правове регулювання інформаційно аналітичних систем займає суттєву роль у сприянні відповідальним підходам до управління даними, охороні прав і конфіденційності особи, підвищенню довіри до цифрових технологій та систем, що працюють на даних. Дотримання цих норм є критичним для учасників правових взаємовідносин щодо інформації, з метою зменшення юридичних ризиків, дотримання етичних вимог і створити безпечне та надійне середовище даних. Гарантування відкритості, прозорості й дотримання етичних принципів у використанні інформаційно аналітичних систем даних становить ключовий фактор для збереження довіри громадськості та забезпечення стабільності суспільства, і саме цьому має бути присвячене законодавче регулювання інформаційно аналітичних систем даних.

Міжнародні документи є важливою частиною правової основи для інформаційно-аналітичної роботи підрозділів МВС України, оскільки вони визначають міжнародні стандарти та правила, якими мають керуватися правоохоронні органи. Правове регулювання інформаційно-аналітичної діяльності підрозділів МВС України ґрунтується на міжнародних угодах. Наприклад, Конвенція про права людини та основні свободи, прийнята Радою Європи (дата підписання: 04.11.1950; дата ратифікації Україною: 17.07.1997; дата набрання чинності для України: 11.09.1997), забезпечує гарантії щодо права на особисту та конфіденційну інформацію, а стаття 8 цієї Конвенції гарантує право на повагу до приватного та сімейного життя, яке може включати конфіденційність інформації [6].

Всі ці нормативні акти створюють правову основу для проведення інформаційно-аналітичної діяльності в підрозділів МВС України та

встановлюють механізми контролю та забезпечення прав та свобод громадян під час збору, обробки та використання інформації.

Додатково до цього в правовому регулюванні важливу роль відіграють постанови Кабінету Міністрів України. Вони встановлюють точні правила та процедури для роботи з інформацією та аналізом. Ці документи визначають, як правильно організовувати роботу підрозділів МВС України, як вона має взаємодіяти з іншими органами та обмінюватися інформацією. Важливу роль у сучасній правовій системі відіграють також внутрішні документи підрозділів МВС України, особливо накази та інструкції. Вони встановлюють конкретні вимоги та стандартні процедури для роботи з інформацією та аналізом. Крім того, сучасні правові схеми враховують міжнародні стандарти та угоди, які регулюють обробку та збереження особистих даних громадян. Це дозволяє уникати порушень прав людини та забезпечує відповідність роботи підрозділів МВС України міжнародним нормам.

Всі ці елементи створюють повну систему правового регулювання інформаційно-аналітичної діяльності підрозділів МВС України. Вона допомагає забезпечити ефективну роботу правоохоронних органів та безпеку громадян. Загалом, механізми правового регулювання інформаційно-аналітичної діяльності підрозділів МВС України дозволяють вести цю роботу в межах закону та враховують вимоги щодо захисту прав та свобод громадян.

Необхідність ухвалення міжнародних документів, що встановлюватимуть уніфіковані правила та механізми управління міжнародною інформаційною безпекою, випливає з глобального розвитку сучасного інформаційного суспільства. Саме інформаційна безпека, як правило, входить до пріоритетних завдань держави, адже вона визначає, з одного боку, ступінь захищеності та, відповідно, стійкість ключових сфер життєдіяльності суспільства (країни) стосовно небезпечного інформаційного впливу, а з іншого – інтенсивність розвитку в різних галузях завдяки ефективному використанню накопичених знань.

РОЗДІЛ 3
ОРГАНІЗАЦІЙНІ ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМАХ МВС УКРАЇНИ

3.1. Міжнародний та національний досвід організації захисту інформації в інформаційно-аналітичних системах МВС України

Ключовою функцією сучасного міжнародного права є формування та гармонізація загальних нормативних засад державної політики, спрямованих на захист прав людини, забезпечення міжнародного миру, безпеки та порядку. Задля збереження універсальних цінностей на світовому рівні, включно з діяльністю Організації Об'єднаних Націй, та у контексті регіональної взаємодії, міжнародна спільнота здійснює перманентну координацію дій суверенних суб'єктів для урегулювання як глобальних, так і локальних проблем, а також для превенції загроз, що виникають на національному та транснаціональному рівнях. Серед таких дестабілізуючих чинників виокремлюється питання інформаційної безпеки суверенних держав, коли їхній інформаційний домен стає об'єктом агресивних дій з боку інших держав або їхніх представників.

У 2001 році Європейська Комісія оприлюднила документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід». Цей документ став значним етапом у формуванні загальноєвропейської стратегії забезпечення інформаційної безпеки. У ньому було окреслено ключові виклики, пов'язані з інформаційною безпекою, та запропоновано концептуальний підхід до їх вирішення в межах Європейського Союзу. Документ служив засадою для подальших ініціатив у цій галузі, а також орієнтиром для держав-членів ЄС у розробці їхніх національних стратегій. Фундаментальні ідеї, закладені в документі, лягли в основу подальших політичних курсів та нормативно-правових актів у сфері мережевої та інформаційної безпеки. Вони сприяли розробці таких ініціатив, як Директива про безпеку мережевих та інформаційних

систем (NIS Directive), ухвалена у 2016 році. Зазначена директива імперативно вимагає від держав-членів Європейського Союзу імплементувати мінімальні стандарти кібербезпеки на національному рівні.

Проаналізуємо практику інформаційно-аналітичного забезпечення правоохоронної діяльності в різних країнах. У 2001 році в ангельському журналі «Police» була опублікована стаття, у якій говорилося про використання сучасних інформаційних технологій в роботі фінансових слідчих. Відомо, що всі люди залишають за собою електронний слід інформації. Наприклад, у Великобританії у 2001 році існувало близько 300 баз даних, а сьогодні ця кількість значно зросла. Слідчим потрібно збирати дані з цих баз, фільтрувати їх за параметрами розслідування, перевіряти, як всі ці відомості вписуються в загальний контекст розслідування, щоб звести їх у єдину систему і виявити, як ще можна діяти [8; 9]. Західні країни широко використовують автоматизовані системи пошуку інформації, що дозволяють значно швидше та ефективніше виявляти та розслідувати злочини, зокрема, з боку організованих угруповань [10, с. 57]. Сучасні технології дозволяють активно протидіяти транснаціональній етнічній злочинності завдяки безмежності глобальної мережі. Вони полегшують взаємодію та обмін інформацією між правоохоронними органами по всьому світу. Наприклад, можна встановити підозрілу особу через застосування спеціальних програм, які ідентифікують особу за фото або відеозображенням. Такий спосіб вже застосовується в деяких закордонних державних та приватних органах [11–14]. Висновок: використання технології великих даних (Big Data), яка дозволяє обробляти великі обсяги інформації, стає ключовим напрямком для підвищення ефективності запобігальної діяльності. Особливу увагу ці технології отримали у Великій Британії, США, Японії, Австралії. У Великій Британії, наприклад, в стратегії запобігання злочинності окремо викладено використання технологій Big Data. В Австралії застосовуються такі технології для кримінологічного прогнозування злочинності. У Японії розглядається запуск системи, яка буде використовувати технології Big Data і штучного інтелекту для

запобігання злочинності та протидії екстремізму [15, с. 25–29]. Інтерпол забезпечує отримання даних з його інформаційних систем за допомогою письмових електронних запитів. Однак виникає проблема в тимчасовій затримці відповідей. Під час аналізу відповідей Інтерполу було виявлено, що 30% запитів отримують протягом 10 днів, 45% — протягом місяця, 25% — протягом двох місяців [16, с. 133–134].

Правоохоронні органи з інших країн часто використовують автоматизовані системи пошуку та обробки інформації, щоб значно полегшити роботу підрозділів МВС. Ураховуючи досвід інших країн, національна інформаційна система ідентифікації побудована на єдиній технології, яка обробляє різноманітну інформацію. Система охоплює всі ключові пункти роботи з громадянами, включаючи паспортні служби, поліцейські дільниці, поліклініки, каси продажу квитків, системи соціального страхування та інші. Принцип «краще запобігти, ніж карати» має залишатися важливим і при боротьбі з організованою злочинністю. Запобігання організованій злочинності здійснюється головним чином за допомогою оперативних засобів, громадськості, ЗМІ та інших соціальних інститутів [7].

Кожна країна вимушена залучатися до захисту своїх інформаційних інтересів, тому вона звертає увагу на інформаційну безпеку. У зв'язку зі швидким розвитком інформаційних технологій усі держави розробляють власні підходи та галузеві стратегії у сфері інформаційної безпеки. Особливо розвинені системи інформаційної безпеки існують у країнах, які постійно піддаються інформаційному впливу, наприклад, в США, Великобританії, Польщі, Франції, Німеччині та інших.

У різних країнах розроблено основні принципи та інструменти для створення ефективного інформаційного захисту національного простору. Використовуючи різноманітні інструменти, країни-лідери успішно реалізують свою національну політику забезпечення інформаційної безпеки.

Сьогодні відбуваються активні процеси створення міжнародного досвіду у сфері забезпечення інформаційної безпеки, особливо в рамках роботи міжнародних організацій, таких як ООН, Рада Європи, Європейський Союз та інші.

У зв’язку з обсягом глобальних викликів у сфері інформації, розв'язати наведені проблеми може бути неможливим лише через зусилля однієї або кількох держав. Тому необхідно розуміти важливість співпраці між країнами у сфері забезпечення міжнародної безпеки інформації, особливо у рамках ООН, яка здатна комплексно розв'язувати політичні проблеми, умови широкого представництва та врахування інтересів всього людства.

У багатьох країнах світу, зокрема і в Україні, інформаційні технології відіграють дедалі важливішу роль у функціонуванні різноманітних правових інституцій. Наприклад, вже сьогодні можна використовувати сервіс "Електронний суд", який сприяє обміну процесуальними документами, або онлайн замовити в Міністерстві внутрішніх справ довідку про відсутність судимості, звернутися до державних органів та органів місцевого самоврядування через вебсайт або електронну пошту і так далі.

Серед міжнародних організацій, основною метою яких є безпека, НАТО найефективніше вдосконалило політику у справах інформаційної безпеки. Так, організація створила центри в країнах-членах, які є багатонаціональними інституціями. У них розробляють доктрину кібербезпеки, вдосконалюють міждержавну співпрацю, впроваджують теоретичні розробки у практичну діяльність з протидії кіберзагрозам, здійснюють обмін досвідом кіберзахисту представників країн-членів і країн-партнерів. Зараз Центр кібербезпеки НАТО розташований в Естонії. Він не є частиною військового командування або збройних сил НАТО. Персонал і фінансування центру забезпечують держави-спонсори та держави-учасники.

У ЄС, в рамках Шенгенських домовленостей, працює Шенгенська інформаційна система (SIS), яка є однією з найбільших систем у сфері публічної

безпеки у світі, а також найбільшою у Європі. Ця система збирає дані про осіб, які вчинили серйозні злочини, та про тих, хто не має права перебувати в ЄС. У SIS зберігаються інформація про осіб, яких шукають, втрачені документи, автомобілі, які були вкрадені, а також зброю. Система призначена для використання поліцією, прикордонниками та митниками країн-членів ЄС [17, с. 145; 18, с. 408]. За останні десятиріччя, завдяки розвитку інформаційних технологій, було створено багато автоматизованих систем дактилоскопічної ідентифікації, серед яких – MORFO (Франція), NEK (Японія), PRINTRAK (США) та інші [19, с. 50].

За результатами наукових досліджень, сьогодні найголовнішою увагою потребують такі ключові загрози національної та міжнародної безпеки у сфері інформації:

– глобальні зміни та перетворення в інформаційному просторі створюють нові виклики та загрози, які є реальною загрозою для безпеки людства та міжнародного правопорядку;

– в інформаційному просторі зростає тенденція до поширення інформаційної агресії, насильства, маніпуляції свідомістю людини та суспільства, регулярно проводяться інформаційно-психологічні операції;

– більшість країн світу зустрічається з проблемами кібершпіонажу, кібертероризму, кіберзлочинності та кібератак на об’єкти критичної інфраструктури;

– наслідки використання сучасної інформаційної збройної системи можуть призвести до реальної втрати суверенітету та територіальної цілісності країн світу.

Європейський досвід у справі інформаційної безпеки правоохоронних органів визначає два способи покращення ефективності роботи в цьому напрямі: вдосконалення діяльності правоохоронних органів для забезпечення власної інформаційної безпеки зсередини та вдосконалення правового забезпечення інформаційної безпеки на державному рівні. Виконання позиції про

перетворення функціонально окремих підсистем, що входять до механізму правового регулювання, може бути найефективнішим, якщо стратегічне планування включає реорганізацію саме тих елементів цих підсистем, які побудовані за принципом систем інформаційного типу, на основі нормативно-правових актів, виданих для виконання положень стратегій. Наукова думка Т.Ю. Ткачука, який аналізував інформаційну безпеку в законодавстві європейських країн, у цьому зв'язку говорить: «Варто констатувати, що країни ЄС мають у певному сенсі злагоджену систему захисту інформації».

Імплементація досвіду інших країн у сфері інформаційної безпеки дуже важлива для покращення захисту інформаційної інфраструктури України та забезпечення національної безпеки. Досвід країн, таких як США, Великобританія, Німеччина, Франція та Польща, дає корисні та ефективні підходи, які можна використовувати в Україні. Тому впровадження закордонного досвіду у сфері інформаційної безпеки в Україні є складним процесом, який потребує взаємодії державних органів, приватного сектору та міжнародних партнерів. Тільки разом можна забезпечити високий рівень захисту національної інформаційної інфраструктури, що гарантує стабільний розвиток країни в сучасних умовах.

3.2. Удосконалення механізмів захисту інформації в інформаційно-аналітичних системах МВС України

Один з найважливіших факторів, що позитивно впливають на розвиток роботи підрозділів МВС, – це забезпечення інформаційної безпеки, наближення послуг до європейських та світових стандартів, оперативне управління ризиками, а також професійна організація інформаційно-аналітичної роботи. Запорука повноцінної роботи підрозділів МВС України — це добре організований обмін інформацією, який допомагає погоджувати та координувати дії для боротьби зі злочинністю. Інформаційні служби системи МВС України забезпечують

підрозділи необхідною інформацією для виявлення та запобігання злочинам, пошуку злочинців, надання статистичних, аналітичних та пояснювальних даних. У процесі виконання інформаційної політики МВС України підрозділи, які відповідальні за взаємодію з національними, закордонними та відомчими засобами зведення інформації, мають використовувати всі сучасні форми та методи взаємодії. Їхня робота має відповідати потребам громадян, відомчим цілям МВС України, а також ураховувати законодавчі норми щодо нових відносин.

Оскільки не існує єдиного світового акту, який регулює порядок боротьби з інформаційними загрозами, як зовнішніми, так і внутрішніми, то у такому контексті дуже важливо розробити Конвенцію ООН про забезпечення міжнародної інформаційної безпеки. У цій конвенції потрібно було б чітко визначити такі питання: основні загрози миру та безпеки в інформаційному просторі; основні принципи забезпечення міжнародної інформаційної безпеки; детально описати принципи міжнародної співпраці у боротьбі зі злочинами в інформаційній сфері; визначити ефективні механізми правової відповідальності в інформаційному просторі, а також створити спеціальний міжнародний орган для розслідування злочинів у сфері інформації.

Гарантування інформаційної безпеки на національному та міжнародному рівнях потребує продовження і розширення діяльності зі створення умов для формування системи міжнародної інформаційної безпеки на підставі загальновизнаних принципів і норм міжнародного права. На рівні ООН слід підготувати та ухвалити міжнародно-правові акти, які регламентують застосування принципів і норм міжнародного права у сферах використання інформаційно-аналітичних систем.

Щоб покращити законодавство, що регулює інформаційне забезпечення органів виконавчої влади, потрібно звести різні закони та накази в один документ. Цей документ має допомогти повністю розв'язати питання, пов’язані з забезпеченням інформацією та правом для роботи органів виконавчої влади.

Також він має роз’яснити, як правильно збирати, зберігати та обробляти інформацію, а також збільшити відповідальність керівників за організацію цієї роботи. Важливо запровадити одну систему документообігу, яка має нові способи захисту, стандартні бази даних, планування роботи та дистанційний контроль за ефективністю роботи певних структур органів виконавчої влади). Крім того, треба покращити аналіз інформації в управлінській діяльності підрозділів МВС, щоб забезпечити реформи. Це відбувається тому, що результатом має бути оцінка стану реформ, визначення не тільки основних недоліків, а й конкретних способів їх усунення. Інформаційно-аналітичне забезпечення реформ в підрозділів МВС виконує управлінську функцію і є важливою частиною ефективного управління підрозділами МВС.

Інформаційно-аналітичне забезпечення реформ підрозділах МВС має бути ефективним, і для цього в ньому потрібно пройти кілька етапів аналізу:

1) підготовчий;

2) збір, накопичення та обробка даних про напрямки реформ;

3) пошук, аналіз та узагальнення інформації про стан та ефективність реформ;

4) отримання спеціальних знань про впровадження реформ;

5) написання проміжних і підсумкових документів.

Підготовчий етап містити: осмислення та конкретизацію цілей та завдань аналізу, вибір об’єктів та методів дослідження, визначення питань, що потрібно вивчити, складання запитальників, визначення послідовності робіт, визначення виконавців, складання програми обробки даних і загальної програми дослідження, визначення термінів. збір матеріалу та його обробка — це два етапи, які можна провести одночасно з уникненням монотонності та зменшенням часу виконання. аналіз полягає в перероблюванню зібраної інформації за заздалегідь визначеною формою. для зручності на цьому етапі роблять три стадії:

1) зведення даних у спеціальні таблиці, що відображають показники однорідної роботи;

2) підсумовування показників, які характеризують діяльність окремих підрозділів, та визначення середніх значень;

3) порівняння даних поточного періоду з даними минулих років, встановлення змін показників та виявлення причин та умов.

Основним способом забезпечення безпеки інформації у складних системах є покращення системного підходу до цієї задачі. Системний підхід означає не тільки створення необхідних захисних механізмів, але й впровадження регулярного процесу, який застосовується на всьому протязі життєвого циклу інформаційної системи та використовує всі можливі засоби захисту.

1. Узгодження з міжнародними правилами: внесення змін у державне законодавство, щоб воно відповідало міжнародним стандартам і нормам, що підвищить безпеку інформації; працювати разом з міжнародними органами та країнами-сусідами у питаннях законодавства, що забезпечує безпеку інформації.

2.Створення спеціальних законів: прийняти закони, які регулюватимуть окремі питання безпеки інформації, наприклад, захист критичної інфраструктури від кібератак, відповідь на інформаційні війни, захист інформації у державних органах; прийняти документи, які визначать, які повноваження мають державні органи у цій сфері.

3.Зробити краще законодавство для керування та відповідальності: підвищити контроль над виконанням законів у сфері безпеки інформації з боку відповідних державних органів; створити та впровадити санкції за порушення законодавства у цій сфері.

Покращення правового забезпечення інформаційної безпеки України повинно бути комплексним і враховувати як внутрішні, так і зовнішні виклики. Цей підхід сприятиме зміцненню позицій у сфері захисту інформації. Інтеграція інформаційних систем разом зі стандартизацією процесів обробки даних забезпечить ефективність, безпеку та надійність управління інформаційними ресурсами в структурних підрозділах МВС. Такі процеси дозволять

синхронізувати діяльність різних відомств, створивши умови для їх оперативного реагування на зростаючі загрози й змінювані обставини.

Інтеграція інформаційних систем вимагає чіткого узгодження технічних і програмних компонентів, щоб забезпечити стабільний і безпечний обмін даними між платформами та базами даних. Обов'язковою умовою є використання уніфікованих форматів даних, що ґрунтуються на загальноприйнятих стандартах. Для надійного обміну інформацією між системами доцільно застосовувати стандартні протоколи, зокрема API (Application Programming Interface), який забезпечує взаємодію різнорідних програмних додатків. Додатково, використання мідлваре (Middleware) дозволяє спростити комунікацію між програмним забезпеченням і базами даних, виконуючи роль посередника і забезпечуючи їхню сумісність.

Важливим аспектом є безперервний доступ до актуальних даних через узгоджену інтеграцію різних систем і джерел інформації. Стандартизація процесів обробки інформації передбачає створення та запровадження єдиних стандартів щодо зберігання, передачі та управління даними, що оптимізує роботу з ними та підвищує їхню захищеність. Така стандартизація встановлює ясні правила й методології роботи з інформацією.

Один із ключових напрямків інноваційного розвитку — це впровадження штучного інтелекту та аналіз великих масивів даних. У довгостроковій перспективі це зможе значно підвищити ефективність діяльності поліції. Водночас правове регулювання використання штучного інтелекту у сфері інформаційно-аналітичної діяльності НПУ перебуває на етапі формування та тісно пов'язане із розробкою загальнодержавної нормативно-правової бази щодо цієї сфери. У 2020 році Кабінет Міністрів України затвердив Концепцію розвитку штучного інтелекту, яка окреслює основні напрями й завдання для подальшого прогресу [42]. Інтеграція штучного інтелекту в інформаційно-аналітичну діяльність підрозділів МВС відкриває значні перспективи для підвищення ефективності боротьби з правопорушеннями. Зокрема, штучний

інтелект дозволяє оперативно обробляти великі обсяги даних, автоматизувати рутинні процедури та оптимізувати моніторинг, сприяючи швидшому та результативнішому реагуванню правоохоронних органів. Водночас впровадження таких технологій у правоохоронну діяльність, включно з інформаційно-аналітичними процесами, супроводжується низкою складних викликів. Одним із ключових аспектів є потреба у правовому регулюванні, яке забезпечить баланс між ефективністю використання штучного інтелекту та дотриманням прав людини й громадян, а також захистить від витоку персональних даних. Крім того, постає питання відповідальності правоохоронців за рішення, прийняті з використанням штучного інтелекту, та можливих негативних наслідків таких дій. Для мінімізації ризиків у майбутньому доцільно розробити законодавчо закріплений механізм регулювання застосування штучного інтелекту в правоохоронній сфері та впровадити контроль за його законним використанням.

Застосування сучасних аналітичних підходів, таких як машинне навчання і штучний інтелект, дозволяє ефективно обробляти великі масиви даних і виявляти потенційні загрози. Ці технології сприяють виділенню важливої інформації та прогнозуванню ризиків, забезпечуючи високу точність аналітичної роботи[47].

Одним із ключових напрямів є прогнозування та виявлення загроз. Інформаційно-аналітичні системи, створені для оперативного надання даних і рекомендацій, значно підтримують процес ухвалення рішень на різних управлінських рівнях. Такі системи спрямовані на надання актуальних аналітичних матеріалів підрозділам МВС, покращуючи якість управління. Їх функціонал включає:

- Інтерактивні дашборди для забезпечення швидкого доступу до ключових даних, аналітики в реальному часі та показників ефективності.

- Моделювання та симуляцію, що допомагають оцінити різні сценарії впливу на безпеку й сприяють глибшому розумінню можливих наслідків прийнятих рішень.

- Системи експертних оцінок, призначені для аналізу ситуації з урахуванням існуючих даних і знань фахівців, формуючи релевантні рекомендації.

- Інтеграцію з іншими інформаційними системами, яка забезпечує безперервний доступ до важливої інформації та аналітики.

Ці сучасні рішення відіграють важливу роль у підвищенні ефективності управління та оперативному реагуванні на виклики.

Застосування таких технологій та підходів значно підвищить ефективність управління, допоможе підрозділам МВС України швидко реагувати на зміни та виклики, забезпечуючи національну безпеку на високому рівні.

Впровадження комплексних заходів щодо захисту інформаційних систем та даних від несанкціонованого доступу, зловмисного втручання або витоку інформації. Використання сучасних криптографічних методів для шифрування інформації, що передається або зберігається.

Удосконалення механізмів захисту інформації в інформаційно-аналітичних системах МВС України буде вирішене завдяки вирішенню причин, які викликають проблеми в даному напрямку:

– не враховують загальний підхід до аналізу системи захисту інформації;

– не вистачає механізмів для повноцінного та достовірного підтвердження якості системи захисту інформації;

– недостатні нормативно-правове та методичне забезпечення системи захисту інформації;

– недостатні організаційні засоби забезпечення системи захисту інформації;

– недостатні матеріально-технічне забезпечення системи захисту інформації;

– недостатні фінансові ресурси для забезпечення системи захисту інформації;

– недостатні кадрові засоби забезпечення системи захисту інформації.

Виходячи з аналізу, можна зробити такі висновки:

1. Інформаційно-аналітична діяльність структурних підрозділів МВС відіграє важливу роль у забезпеченні громадської безпеки, боротьбі зі злочинністю та підтриманні правопорядку. Ефективне виконання цієї функції залежить від удосконалених правових механізмів, гармонійного впровадження сучасних технологій та застосування передових аналітичних методів.

2. Нормативно-правова база, яка регулює інформаційно-аналітичну діяльність Національної поліції, включає відповідні положення Конституції України, Закон України «Про Національну поліцію», міжнародні конвенції, постанови Кабінету Міністрів України, а також відомчі нормативні акти. Проте вона потребує адаптації з огляду на технологічний прогрес і динамічні зміни суспільних запитів, особливо в умовах воєнного стану.

ВИСНОВКИ

В роботі визначено основні поняття захисту інформації в інформаційно-аналітичних системах МВС України. Інформаційно-аналітичні системи (ІАС) МВС мають дуже велике значення для виконання правоохоронних обов’язків держави, оскільки забезпечують оперативне прогнозування, виявлення та запобігання злочинам. Встановлено, що захист інформації в цих системах має бути комплексним (КСЗІ), що охоплює правові, організаційні, технічні та програмно-апаратні заходи. Визначено, що основними об’єктами захисту є інформація, доступ до якої обмежений (державна таємниця, службова інформація, персональні дані), а також апаратна та програмна інфраструктура. Також з’ясовано, що загрози можуть бути як умисними (наприклад, хакерські атаки, інсайдерство), так і неумисними, і вони є основою для визначення ефективної стратегії безпеки, спрямованої на збереження конфіденційності, цілісності та доступності даних. Особливості захисту інформації в інформаційно-аналітичних системах МВС України від несанкціонованого доступу.

Визначені особливості захисту інформації в інформаційно-аналітичних системах МВС України від несанкціонованого доступу. Забезпечення захисту від несанкціонованого доступу є головним завданням, оскільки інформаційно-аналітичні системи МВС обробляють величезну кількість цінної інформації. Встановлено, що ефективний захист від несанкціонованого доступу досягається за допомогою системи контролю:

1. Перевірка правильності ідентифікації користувачів та обладнання.

2. Обмеження доступу відповідно до принципу мінімальних привілеїв, що дозволяє користувачам отримувати доступ лише до необхідної інформації.

3. Контроль за діями користувачів та ведення аудиту, а також обов'язкова реєстрація спроб несанкціонованого доступу для швидкого виявлення та реагування. Особливу увагу приділено регламентації доступу зовнішніх

користувачів, яка має бути узгоджена з Державною службою спеціального зв'язку та захисту інформації України, щоб забезпечити відповідність державним стандартам безпеки.

Визначені міжнародні стандарти правового регулювання захисту інформації в інформаційно-аналітичних системах. Аналіз міжнародних правових актів показав, що стандарти захисту інформації в інформаційних архівах МВС формується під впливом основних міжнародних документів. Серед найважливіших — Конвенція про захист прав людини та основоположних свобод, особливо щодо захисту приватного життя та особистих даних, а також конвенції ООН і Ради Європи про кіберзлочинність, корупцію та транснаціональну злочинність. Підкреслено, що ці документи встановлюють загальні правила для спільного обміну інформацією між правоохоронними органами різних країн, одночасно забезпечуючи її безпеку. Однак було виявлено, що відсутній єдиний світовий документ про міжнаціональну інформаційну безпеку, що створює проблеми в співпраці та боротьбі з загрозами. Україна, яка інтегрується в європейське простір, має повністю застосовувати ці стандарти, щоб отримати визнання своїх інформаційних архівів на міжнародному рівні.

Визначено правове регулювання захисту інформаційно-аналітичних систем в МВС України. Встановлено, що захист інформаційно-аналітичних систем МВС регулюється Конституцією, законами, відомчими актами та постановами Кабінету Міністрів України. Ці документи створюють правову основу для роботи Єдиної інформаційної системи МВС, визначаючи правила обміну даними між всіма її структурними підрозділами. Основна мета правового регулювання – забезпечення достовірності, об'єктивності та конфіденційності аналітичної інформації. Це досягається через обов'язкову сертифікацію та атестацію всіх компонентів захисту Держспецзв'язком, що збільшує відповідальність керівництва за стан інформаційної безпеки.

В роботі проаналізовано міжнародний та національний досвід організації захисту інформації в інформаційно-аналітичних системах МВС України. Аналіз

досвіду країн, таких як ЄС, США, Великобританія, Німеччина, Франція, Польща, показує, що ефективна робота з охороною інформаційно-аналітичних систем Міністерства внутрішніх справ України потребує одночасного виконання двох стратегічних напрямів: посилення інституцій та гармонізації законодавства. Створення централізованих кіберструктур (приклади NCSC і BSI): Досвід Великобританії та Німеччини демонструє важливість створення або посилення національних центрів, які б відповідали за координацію кіберзахисту на всіх рівнях державної влади, включаючи МВС. Такі центри забезпечують єдиний підхід до стандартів безпеки, обміну інформацією про загрози та оперативного розв'язання питань. Захист критичної інфраструктури: Моделі, які застосовуються в Німеччині та Франції (ANSSI), підкреслюють важливість суворих законодавчих та технічних умов для захисту інфраструктури, яка визначає функціонування держави, зокрема і ключових інформаційно-аналітичних систем МВС.

Міжнародна співпраця та стандарти НАТО/ЄС: Для України особливо важливо повністю впровадити стандарти ISO/IEC 27001 та директиви ЄС, зокрема NIS-2. Приклад Польщі показує, як ефективно можна посилювати кібербезпеку через участь у європейських програмах та адаптацію законодавства. Успішне застосування міжнародного досвіду МВС України можливе лише за умови, щоб цей досвід був адаптований до національного правового поля та інституційної системи, забезпечуючи високий рівень технічного захисту та ефективну міжвідомчу взаємодію, особливо в боротьбі з кіберзлочинністю.

Сформульовані удосконалення механізмів захисту інформації в інформаційно-аналітичних системах МВС України. У підрозділі наведено конкретні пропозиції, які мають підвищити стійкість інформаційно-аналітичних систем МВС до сучасних загроз. Ці пропозиції поділяються на дві групи: правові та технологічні заходи.

Перша група – консолідація та гармонізація законодавства.

Виявилося, що потрібно уніфікувати різні нормативно-правові акти МВС та загальнодержавні стандарти (закони, постанови Кабінету міністрів) в один чіткий документ, наприклад, Відомчий стандарт або Положення. Така дія зменшить юридичні конфлікти, спростить застосування норм безпеки й збільшить гармонію з міжнародними стандартами.

Друга група – інтеграція штучного інтелекту та машинного навчання.

Запропоновано впровадити алгоритми ШІ та МН для автоматичного моніторингу та прогнозування загроз. Такі системи зможуть аналізувати великі обсяги даних, виявляти аномалії та потенційні безпекові інциденти в реальному часі, що значно зменшить час реагування й мінімізує вплив людського фактора.

Для ефективної роботи систем МВС потрібно забезпечити їх архітектурну сумісність та стандартизацію. Для цього необхідно розробити єдині технічні стандарти, протоколи й інтерфейси, що дозволять безперешкодно та безпечно інтегрувати нові системи. Це уникне появи інформаційних островів в мережі МВС. Крім того, важливо посилювати кадрову складову. Оскільки людський фактор є основною вразливістю, потрібно постійно вдосконалювати кваліфікацію та перепідготовку ІТ-співробітників та користувачів. Вони мають проходити спеціальні тренінги щодо кібергігієни, виявлення соціальної інженерії та використання сучасних засобів криптографічного захисту.

Вдосконалення захисту має бути щоденним процесом. Він має поєднувати високі правові стандарти безпеки з активним використанням сучасних технологій, таких як штучний інтелект та аналітика Big Data, щоб забезпечити найвищий рівень стійкості інформаційно-аналітичних систем МВС до постійно змінних кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.Ua/laws/show/2657-12#Text (дата звернення: 15.05.2022).

2. Про основні засади забезпечення кібербезпеки України: Закон України Документ 2163-VIII, чинний, поточна редакція — Редакція від 19.10.2025, URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення:23.10.2025).

3. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 23.10.2025).

4. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. Відомості Верховної Ради України. 2011. № 32. Ст. 314. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 21.10.2025).

5. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Відомості Верховної Ради України. 1994. № 31. Ст. 286. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 21.10.2025).

6. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Відомості Верховної Ради України. 2010. № 34. Ст. 481 URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 21.10.2025).

7. ВИМОГИ до створення і впровадження єдиної системи електронного документообігу в Міністерстві внутрішніх справ України та центральних органах виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ України URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://mvs.gov.ua/upload/file/vimogi_do_sed_sistemi_mvs_363.pdf (дата звернення: 21.10.2025).

8. Про затвердження Переліку відомостей, що становлять службову інформацію в Міністерстві внутрішніх справ України URL: https://zakon.rada.gov.ua/rada/show/v0573320-23#Text (дата звернення: 21.10.2025).

9. Положення про технічний захист інформації в Україні: Указ Президента від 27.09.1999 № 1229/99. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text (дата звернення: 21.10.2025).

10. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 25.10.2025).

11. Актуальні проблеми управління інформаційною безпекою держави : збірник тез наукових доповідей, (Київ, 4 квіт. 2019 р.). Київ : Національна академія Служби безпеки України, 2019. 384 с.

12. Бєлай С.В., Споришев К.О. Вплив стану системи інформаційно аналітичного забезпечення сил безпеки України на державну безпеку. Наукові інновації та передові технології (Серія "Управління та адміністрування"). 2024. Випуск № 2 (30). С. 29—37.

13. Інформація, комунікація, суспільство 2024: матеріали 13-ї Міжнародної наукової конференції ICS-2024. – Львів: Видавництво Львівської політехніки, 2024. – URL: http://skid.lpnu.ua/wpcontent/ uploads/2024/05/ICS2024_Proceedings.pdf, вільний. С 35, 37 (дата звернення: 25.10.2025).

14. Конституція України: прийнята на 5-й сесії Верховної Ради України 28 червня 1996 р. Відомості Верховної Ради України. 1996. № 30. Ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 25.10.2025).

15. Офіційне інтернет-представництво «Президент України». URL: http://surl.li/uhubf (дата звернення 09.05.2024). 3. Про Національну поліцію: Закон

України від 02.07.2015: № 580-VIII URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення 10.10.2025).

16. Офіційний веб-сайт Президента України. URL: http://www.president.gov.ua/ (дата звернення: 25.10.2025).

17. Офіційний сайт Верховної Ради України. URL: www.rada.gov.ua (дата звернення: 25.10.2025).

18. Урядовий портал. Єдиний вебпортал органів виконавчої влади. URL: http://www.kmu.gov.ua/control/ (дата звернення: 25.10.2025).

19. Офіційний вебпортал Міністерства внутрішніх справ України. URL: http://www.mvs.gov.ua/ (дата звернення: 25.10.2025).

20. Офіційний вебсайт Міністерства юстиції України. URL: http://www.minjust.gov.ua/ (дата звернення: 25.10.2025).

21. Офіційний вебпортал Міністерства освіти та науки України. URL: http://www.mon.gov.ua/ (дата звернення: 25.10.2025).

22. Інформаційно-пошукова правова система «Нормативні акти України (НАУ)». URL: http://www.nau.ua (дата звернення: 25.10.2025).

23. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку пріоритетних електронних інформаційних ресурсів її суб'єктів : постанова Кабінету Міністрів України від 14.11.2018 № 1024, станом на 22.08.2023. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF#Text (дата звернення 08.10.2025).

24. Про затвердження Положення про Департамент інформаційно аналітичної підтримки Національної поліції України : наказ Національної поліції України від 31.01.2020 № 77. URL: https://www.npu.gov.ua/propoliciyu/struktura-nacionalnoyi-policiyi/departament-informacijno-analitichnoyipidtrimki (дата звернення 10.10.2025).

25. Наказ МВС від 21.01.2025 № 34 «Про внесення змін до Переліку відомостей, що становлять службову інформацію в Міністерстві внутрішніх

справ України» URL: https://mvs.gov.ua/normativno-pravovi-akti/nakaz-mvs-vid-21012025-34-pro-vnesennia-zmin-do-pereliku-vidomostei-shho-stanovliat-sluzbovu-informaciiu-v-ministerstvi-vnutrisnix-sprav-ukrayini (дата звернення 09.10.2025).

26. Європейська конвенція з прав людини: ратифіковано Законом України 17.07.1997. URL: https://zakon.rada.gov.ua/ laws/show/995_004#Text (дата звернення 09.10.2025).

27. Конвенція Організації Об'єднаних Націй проти корупції : ратифіковано Законом від 18.10.2006. URL: https://zakon.rada.gov.ua/ laws/show/995_c16#Text (дата звернення 10.10.2025).

28. Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки та оборони України на 2023-2027 роки : затв. Указом Президента України від 11.05.2023 № 273/2023. URL: https://zakon.rada.gov.ua/ laws/show/273/2023#Text (дата звернення 08.10.2025).

29. Регламенти ЄС в галузі кібербезпеки: Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій»

30. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28 груд. 2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text (дата звернення: 25.10.2025).

31. Бандурка О.М., Безпалова О.І., Джафарова О.В. Управління органами Національної поліції України : підручник МВС України, Харків. нац. ун-т внутр. справ. Харків: Стильна типографія, 2017. 580 с.

32. Біленчук П. Д., Борисова Л. В., Неклонський І. М., Собина В. О. Правові засади інформаційної безпеки України : монографія. Харків : 2018. 289 с.

33. Борисов В. І., Карчевський М. В., Шепітько М. В Міжнародні стандарти та національна кримінально-правова політика у сфері охорони

інформаційної безпеки : монографія : електрон. наук. вид. Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. – Харків : Право, 2023. – 152 с.

34. Грицишен Д. О., Дикий А. П., Бутузов В. М., Цимбалюк, В. С. Механізм забезпечення інформаційної безпеки реалізації державної політики запобігання та протидії економічній злочинності. Ефективність державного управління, 2023 № 3, с. 70–76. URL: https://doi.org/10.36930/507611 (дата звернення: 25.10.2025).

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

36. Даніч В.М., Шевченко С.М. Інформаційний простір. Review of transport economics and management. 2022. Iss. 8 (24). С. 120– 140. DOI: https://doi.org/10.15802/ rtem2022/277626 (дата звернення: 25.10.2025).

37. Задорожнюк Н. О. Сучасні технології бізнес-аналітики. Економічна аналітика: сучасні реалії та прогностичні можливості : збірник матеріалів міжнар. наук.-прак. конф.. Київ, 2019. С. 105–107.

38. Колесніков А.П. Обмеження використання штучного інтелекту в правоохоронній діяльності відповідно до AI ACT. Актуальні питання забезпечення безпекового середовища в Україні : зб. тез наук. доп. Всеукр. наук.-практ. конф. (Київ, 19 квітня 2024 р.). Київ : ДНДІ МВС України, 2024 С. 313-315. URL: https://www.researchgate.net/publication/387187888_Obmezenna_vikoristanna_stucnogo_ intelektu_v_pravoohoronnij_dialnosti_vidpovidno_do_AI_ACT (дата звернення: 25.10.2025).

39. Кавин С. Нормативно-правові механізми забезпечення кібербезпеки в нових державах – членах ЄС Вісн. Київ. нац. ун-ту імені Тараса Шевченка. Юридичні науки. – 2021. – № 2 (117). – С. 30–38.

40. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236с.

41. Копійка М. В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки Політичне життя. – 2020. – № 1. – С. 102–109.

42. Концепція розвитку штучного інтелекту в Україні: схвалена розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text(дата звернення: 25.10.2025).

43. Кудінов В. А., Яровий К. В. Інформаційне забезпечення правоохоронної діяльності: навч.-практ. посіб. Київ: Нац. акад. внутр. справ, 2024. 120 с.

44. Куракін О., Скрябін О. Особливості правового регулювання використання штучного інтелекту в Україні. Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право», 2023 №36, с. 36-42. URL: https://doi.org/10.26565/2075-1834-2023-36-04 (дата звернення: 25.10.2025).

45. Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України: матеріали Науково-практичної конференції (Львів, 20 грудня 2024) — ЛьвівЛьвів : ЛьвДУВС, 2025. – 137 с.

46. Комаров М. Ю., Гончар С. Ф., Ониськова А. В. Нормативний аспект побудови та впровадження системи управління інформаційною безпекою на об'єктах критичної інфраструктури. Моделювання та інформаційні технології. № 82. 2018. С. 40–48.

47. Ляпін К. Е. Виклики та можливості сучасності: комплексна система захисту інформації. Збірник матеріалів VI міжнародної науково-практичної конференції «Інформаційна безпека та комп'ютерні технології»: тези доповідей, 20-21 квітня 2023 р. Кропивницький: ЦНТУ, 2023. 96 с.

48. Лубко Д., Мірошниченко М. Механізми безпеки інформації та їх виклики. Науковий вісник Таврійського державного агротехнологічного

університету № 14(2). (2024). URL: https://doi.org/10.32782/2220-8674-2024-24-2-26 (дата звернення: 25.10.2025).

49. Макаренко Є. А., Рижков М. М., Ожеван М. А. Міжнародна інформаційна безпека: теорія і практика: підручник Київ: Центр вільної преси, 2016. – 418 с.

50. Мельнікова О. О. Організаційно-правові основи інформаційно-аналітичного забезпечення діяльності правоохоронних органів Протидія злочинності: проблеми практики та науково-методичне забезпечення № 2 2023

51. Остроухов В.В., Присяжнюк М.М., Фармагей О.І., Чеховська М.М. Інформаційна безпека : підручник Київ : Видавництво Ліра-К, 2021. 412 с.

52. Пересада О.М. Роль Національної поліції України в забезпеченні інформаційної безпеки держави: теоретико-методологічні аспекти. Правовий часопис Донбасу. № 4 (69). 2019. С. 183–189. DOI: https:// doi.org/10.32366/2523-4269-2019-69-4- 183-189 (дата звернення: 25.10.2025).

53. Рижков Е. В., Синиціна Ю. П, Прокопов С. О. Інформаційно-аналітичне забезпечення правоохоронної діяльності: навч. посіб. Дніпро : Дніпров. держ. ун-т внутр. справ, 2024. 180 с.

54. Савіцький Л.М., Безносенко С.Ю., Горбач Р.Я. Сучасні інформаційні технології у сфері безпеки та оборони № 1 (49)/2024

55. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України : дис. д-ра. юрид. наук : 12.00.07. Ужгород. 2019. 487 с. URL: https://uacademic.info/ua/document/0519U000217#google_vignette (дата звернення: 25.10.2025).

56. Ткачук Т.Ю. Інформаційна безпека держави у національному законодавстві європейських країн. Visegrad Journal on Human Rights. 2018 № 1. С. 145–150.

57. Турчак А.В. Механізми забезпечення інформаційної безпеки як складової державної безпеки України: дис. канд.. юрид. наук: 25.00.02. К.: 2020. 229 с.

58. Фролова О. М. Роль ООН в системі міжнародної інформаційної безпеки. Міжнародні відносини. Серія «Політичні науки». 2018. №18-19. URL : http://joumals.iir.kiev.ua/index.php/pol_n/article/view/3468. (дата звернення: 25.10.2025).

59. Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. Комплексні системи захисту інформації: навч. посіб. 63-тє вид. Вінниця: ВНТУ, 2018. 119 с. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://pdf.lib.vntu.edu.ua/books/IRVC/Yaremchuk_2018_118.pdf (дата звернення: 25.10.2025).

60. Harris W., Sadok M. How do professionals assess security risks in practice? An exploratory study. *Security Journal*. 2023. № 37(3). P. 671-685. DOI:10.1057/s41284-023-00389-y (дата звернення: 25.10.2025).

61. State policy of Ukraine in the field of ensuringinformation security of person, society, stateInformation Security of the Person, Society, State. 2022.№ 1–3 (34–36)71rada.gov.ua/laws/show/2163-19#Text (дата звернення: 25.10.2025).

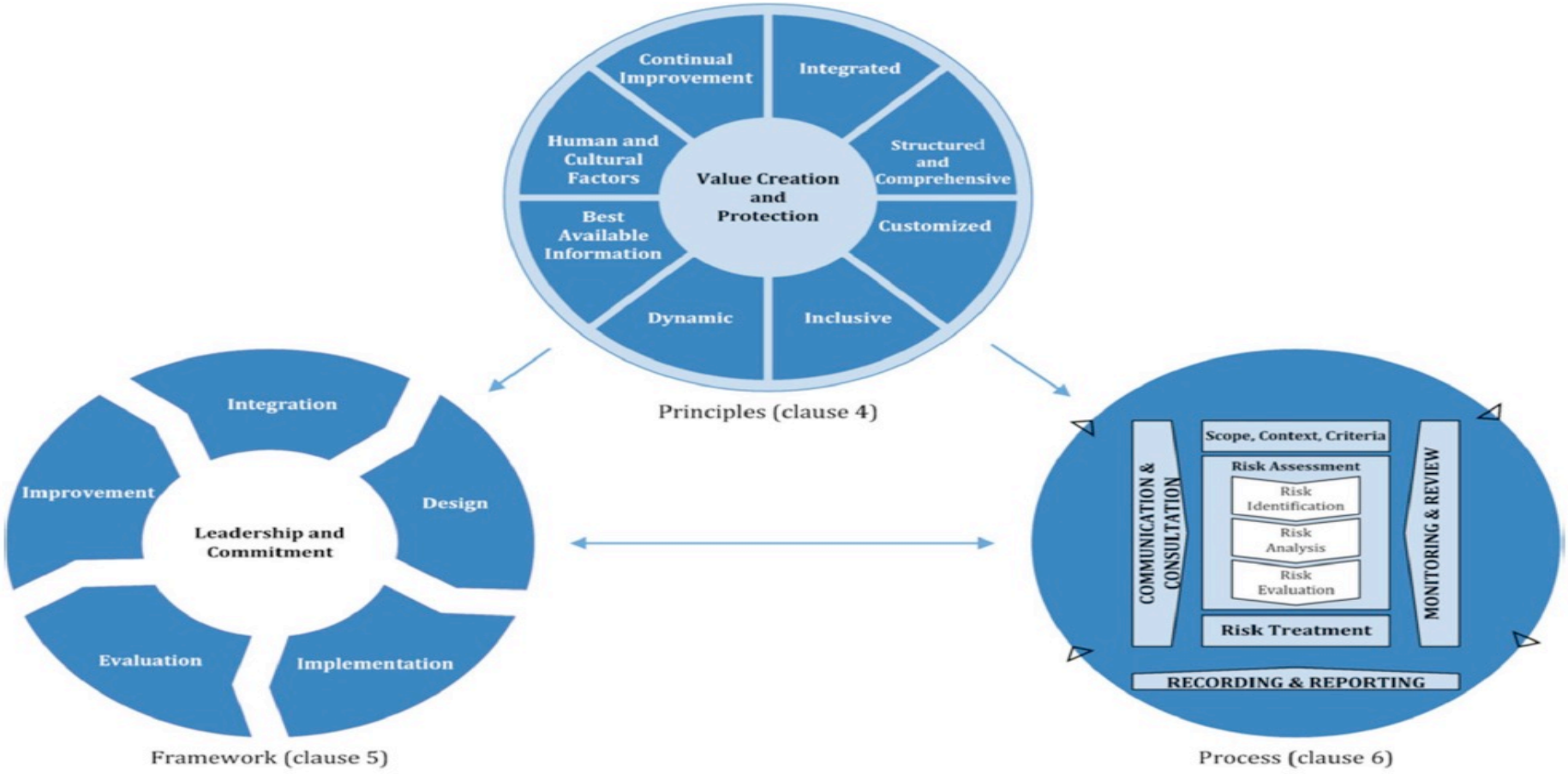
62. Resolution adopted by the General Assembly on 22 December 2018 [on the report of the First Committee (A/73/505)] 73/266. Advancing responsible State behaviour in cyberspace in the context of international security [Electronic resource]. – https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/465/01/PDF/N1846501.pdf.

63. Resolution adopted by the General Assembly on 22 December 2018 [on the report of the First Committee (A/73/505)] 73/266. Advancing responsible State behaviour in cyberspace in the context of international security [Electronic resource]. – https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/465/01/PDF/N1846501.pdf

ДОДАТКИ

Додаток А

Принципи, структура і процес управління безпекою [Harris W., Sadok M. How do professionals assess security risks in practice? An exploratory study. *Security Journal*. 2023. № 37(3). P. 671-685. DOI:10.1057/s41284-023-00389-y]



Додаток Б

Програма інформатизації системи МВС [19]

Додаток В

Список нормативних документів щодо інформаційної безпеки МВС України

1. Конституція України	Право на інформацію, захист персональних даних.	Сайт Верховної Ради України (rada.gov.ua)
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»	Вимоги до створення КСЗІ, правові засади захисту інформації.	Сайт Верховної Ради України (rada.gov.ua)
3. Закон України «Про кібербезпеку»	Організаційно-правові засади захисту критичної інфраструктури, суб'єкти кібербезпеки (включаючи МВС).	Сайт Верховної Ради України (rada.gov.ua)
4. Закон України «Про державну таємницю»	Порядок доступу та захисту секретної інформації.	Сайт Верховної Ради України (rada.gov.ua)
5. Закон України «Про захист персональних даних»	Вимоги до обробки, зберігання та захисту персональних даних громадян в ІАС.	Сайт Верховної Ради України (rada.gov.ua)
6. Постанова КМУ № 373 від 27.05.2020	Деталізація вимог до захисту інформації в державних реєстрах.	Сайт Верховної Ради України (rada.gov.ua)
Накази МВС щодо організації кіберзахисту та Інструкції з діловодства з ДСК	Деталізація відповідальності, порядку дій у разі інцидентів, правил роботи з документами та інформацією "Для службового користування".	Не публікуються. Є документами внутрішнього користування.
Політика інформаційної безпеки МВС	Стратегічний документ, що визначає загальні принципи та цілі захисту інформації в системі Міністерства.	Обмежений доступ.
Нормативні документи технічного захисту інформації (НД ТЗІ)	Стандарти для створення та атестації Комплексних систем захисту інформації (КСЗІ).	Офіційний сайт Держспецзв'язку (cip.gov.ua) у розділі "Нормативна база".

Додаток Г

Основні засади забезпечення інформаційної безпеки у країнах світу

Країна	**Рівень розвитку інформаційно-комунікаційної сфери країни**	**Особливості забезпечення інформаційної безпеки**	**Механізми забезпечення інформаційної безпеки**
США	Дуже високий	Потужна національна стратегія кібербезпеки, активна співпраця між державними і приватними секторами, використання передових технологій для моніторингу та захисту.	Законодавчі акти, такі як Закон про кібербезпеку, створення агентств типу CISA, програми публічно- приватного партнерства, постійне інвестування в технологічні рішення.
Польща	Високий	Зростаючий акцент на кібербезпеці в національній стратегії, посилення законодавчої бази, активне залучення до європейських ініціатив та програм з кібербезпеки.	Створення національного центру кібербезпеки, впровадження рекомендацій ЄС, розвиток законодавства, проведення національних навчань та тренувань.
Великобританія	Дуже високий	Розробка та впровадження Національної стратегії кібербезпеки, створення Національного центру кібербезпеки (NCSC), співпраця з міжнародними партнерами.	Введення в дію Національного центру кібербезпеки, законодавчі ініціативи, міжнародне співробітництво в рамках GCHQ та інших організацій, створення спеціалізованих навчальних програм.

Німеччина	Дуже високий	Створення Федерального відомства з інформаційної безпеки (BSI), активна участь у європейських кібербезпекових ініціативах, суворі вимоги до захисту критичної інфраструктури.	Законодавче регулювання через IT-Sicherheitsgesetz, участь у міжнародних кібербезпекових ініціативах, впровадження стандартів ISO/IEC 27001, розвиток технічних засобів захисту.

Продовження Додаток Г

Франція	Високий	Впровадження національної стратегії кібербезпеки, створення Національного агентства з безпеки інформаційних систем (ANSSI), акцент на захисті державних і приватних інформаційних систем.	Розвиток ANSSI, законодавче регулювання, включення кібербезпеки до національних стратегій, регулярні оцінки та аудити безпеки, участь у міжнародних програмах та ініціативах