УДК 342.7
DOI https://doi.org/10.32782/2524-0374/2024-9/118

КЛАСИФІКАЦІЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

CLASSIFICATION OF THREATS TO INFORMATION SECURITY IN LAW ENFORCEMENT ACTIVITIES

Мазепа С.О., к.ю.н., доцент,
доцент кафедри кримінального права та процесу
Західноукраїнського національного університету,
міжнародний дослідник
Оснабрюцького університету

У статті розглянуто комплекс питань, пов'язаних із забезпеченням інформаційної безпеки в діяльності правоохоронних органів України в умовах цифрової трансформації, гібридної агресії та стрімкого розвитку інформаційних технологій. Проаналізовано ключові джерела загроз, включаючи використання штучного інтелекту злочинцями, кіберзлочини, витоки інформації, дезінформацію, а також технічні та організаційні вразливості систем МВС. Узагальнено положення українського законодавства у сфері інформаційної та кібербезпеки та проведено порівняльний аналіз із відповідними нормами права Європейського Союзу (NIS2, GDPR, Cybersecurity Act). Визначено пріоритетні напрямки нормативного, технічного та організаційного забезпечення інформаційної безпеки, надано рекомендації щодо адаптації європейських практик до української системи МВС. Зроблено висновок про необхідність інтеграції інформаційної безпеки у всі етапи управлінської та оперативної діяльності правоохоронних структур.

Інформаційна безпека в системі МВС має гарантуватися на трьох рівнях: законодавчому – через прийняття чітких нормативно-правових актів, що регулюють обробку, доступ та захист інформації; технічному – шляхом використання сучасних засобів шифрування, сертифікованого програмного забезпечення, контролю доступу, багатофакторної автентифікації; організаційному – через політики кібергігієни, навчання персоналу, моніторинг аномальної активності, внутрішній аудит та інші адміністративні заходи.

Враховуючи досвід ЄС, доцільно адаптувати до українських реалій такі європейські принципи: ризик-орієнтоване управління безпекою; зобов'язання щодо оперативного реагування на інциденти; підвищення обізнаності та сертифікація безпеки IT-рішень; міжвідомчий обмін кіберзагрозами.

Основні загрози, виявлені в контексті практичної діяльності МВС, мають переважно кібернетичний, технічний, соціально-психологічний і внутрішньоорганізаційний характер. Їхня класифікація та превенція повинні бути закріплені в системній стратегії інформаційної безпеки МВС із урахуванням міжнародного досвіду.

Ключові слова: інформаційна безпека, кіберзагрози, правоохоронні органи, штучний інтелект, європейське законодавство.

The article examines a set of challenges related to ensuring information security in the activities of Ukrainian law enforcement agencies amid digital transformation, hybrid aggression, and rapid development of information technologies. It analyzes key sources of threats, including the criminal use of artificial intelligence, cybercrime, data leaks, disinformation, as well as technical and organizational vulnerabilities in the Ministry of Internal Affairs (MIA) systems. The study generalizes the provisions of Ukrainian legislation in the field of information and cybersecurity and provides a comparative analysis with relevant European Union regulations (NIS2, GDPR, Cybersecurity Act). It identifies priority directions for legislative, technical, and organizational support of information security and offers recommendations for adapting European practices to the Ukrainian MIA system. The conclusion emphasizes the necessity of integrating information security into all stages of managerial and operational activities of law enforcement agencies.

Information security in the Ministry of Internal Affairs system must be guaranteed at three levels: legislative – through the adoption of clear regulatory acts governing the processing, access, and protection of information; technical – through the use of modern encryption tools, certified software, access control, and multi-factor authentication; organizational – through cyber hygiene policies, staff training, monitoring of abnormal activity, internal audits, and other administrative measures.

Taking into account the experience of the EU, it is advisable to adapt the following European principles to Ukrainian realities: risk-oriented security management; commitment to respond promptly to incidents; awareness raising and certification of IT security solutions; interagency exchange of cyber threats.

The main threats identified in the context of the practical activities of the Ministry of Internal Affairs are predominantly cybernetic, technical, socio-psychological, and internal organizational in nature. Their classification and prevention should be enshrined in the Ministry of Internal Affairs' systematic information security strategy, taking into account international experience.

Key words: information security, cyber threats, law enforcement agencies, artificial intelligence, European legislation.

Вступ. Пандемія, війна та технологічний прогрес стали основними факторами, які перенесли буденне життя в інформаційний простір та суттєво вплинули на зміни в інформаційному суспільстві. Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України [1]. Досвід провідних країн показує, що для ефективного забезпечення інформаційної безпеки необхідно посилювати ті структури, які відповідають за реалізацію державної політики у ключових технологічних напрямках – захисті інформаційних ресурсів, самої інформації та безпеці інформаційного обміну [2; с. 54].

Роль інформаційної безпеки в правоохоронній діяльності є особливо важливою, оскільки витік або втрата такої важливої інформації, як електронні докази, реєстри злочинців, дані щодо кримінальних справ, правопорушників тощо.....мають надто дорогу ціну.

Виклад основного матеріалу. Інформаційна безпека – це важлива сфера діяльності держави. Інформаційні технології розвиваються з нереальною швидкістю та правове регулювання часто запізнюється з розвитком. Розвиток штучного інтелекту є великим успіхом та допоміжним інструментом для людства. Але використання ШІ в руках злочинців становить суттєву небезпеку. Терабайти інформації збираються щохвилини, такі розробки, як чат GPT, інтернет речей та інше накопичують чимало інформації про людину. Рада Національної безпеки та оборони розглядає

нформаційну безпеку України як складову частину національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом;[4] Змістовну сутність інформаційної безпеки у спрощеному вигляді можна викласти як комплекс превентивних дій, спрямованих на забезпечення права на інформацію і свободу інформаційної діяльності, на захист інформації і права власності на інформацію, на захист від інформації та від інформаційних впливів [3; с. 134].

Особливу увагу слід приділити розкриттю суті інформаційної загрози як потенційно або реально негативного явища, тенденцій і чинників інформаційного впливу на людину [15; с. 111], суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні. Але, перш ніж говорити про загрози інформаційній безпеці, проаналізуємо види інформації, яка використовується МВС у правоохоронній діяльності:

- Докази
- Персональні дані
- Реєстри

Перелік пріоритетних інформаційних ресурсів Єдиної інформаційної системи Міністерства внутрішніх справ міститься у наступних структурах:

1) Націоанльна поліція – 18
2) МВС – 7
3) Державна прикордонна служба – 5
4) Державна міграціна служба – 3
5) Державна служба з надзвичайних ситуацій – 2
6) Державна судова адміністрація – 1
7) Офіс Генерального прокурора – 1 [5].

Треба наголосити, що Закон України «Про інформацію» містить визначення інформації, згідно з яким інформацією є будь-які відомості та / або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. У цьому ж Законі визначені основні види інформації: 1) інформація про фізичну особу; 2) інформація довідково-енциклопедичного характеру; 3) інформація про стан довкілля (екологічна інформація) [6]; 4) інформація про товар (роботу, послугу); 5) науково-технічна інформація; 6) податкова інформація; 7) правова інформація; 8) статистична інформація; 9) соціологічна інформація; 10) інші види інформації. Однією із найважливіших умов підвищення рівня протидії злочинності є широке застосування сучасних досягнень науково-технічного прогресу, а також інформаційних технологій [8; с. 112].

Де може виникати загроза для представника правоохоронних органів:

- Несанкціонований доступ до інформації шляхом зламу через ненадійний пароль або имейл збирач інфо
- Безвідповідальне використання інструментів ШІ
- Витік інформації через месенджери
- Соціальні мережі
- Інтернет речей
- Розголошення інформації підчас бесіди
- Корупційна складова

Інформаційна безпека в правоохоронній діяльності є критично важливою для забезпечення конфіденційності, цілісності та доступності даних. Основні загрози можуть виникати в таких сферах:

1. Кіберзлочини та хакерські атаки
- використання шкідливого програмного забезпечення (віруси, трояни, руткіти).
- атаки на бази даних та сервіси правоохоронних органів (DDoS, SQL-ін’єкції).
- викрадення або модифікація оперативної інформації про кримінальні справи, агентів, свідків тощо.

2. Витік конфіденційної інформації
- нсайдерські загрози (недобросовісні співробітники, шпигунство).
- недостатньо захищені канали передачі інформації (незашифровані повідомлення, слабкі паролі).
- втрата або крадіжка пристроїв із доступом до службових систем.

3. Дезінформація та інформаційні атаки
- поширення фейкових новин для підриву довіри до правоохоронних органів.
- икористання соціальних мереж для дискредитації слідства або маніпуляції громадською думкою.
- підробка доказів чи маніпуляція цифровими даними.

4. Недостатній рівень кібергігієни серед персоналу
- використання ненадійних паролів або їх повторне використання.
- відсутність двофакторної автентифікації.
- перехід за фішинговими посиланнями та відкриття шкідливих вкладень у листах.

5. Слабкі місця у програмному забезпеченні та апаратних системах
- використання застарілих або непатчених систем.
- вразливості у спеціалізованих правоохоронних платформах та базах даних.
- незахищені мобільні пристрої, які використовуються у службових цілях.

6. Загрози з боку організованої злочинності та держав-агресорів
- цілеспрямовані кібератаки на правоохоронні структури з боку ворожих держав.
- підкуп або шантаж співробітників для отримання конфіденційної інформації.
- використання штучного інтелекту для автоматизації атак.

7. Відсутність або неефективність політик інформаційної безпеки
- відсутність чітких правил користування службовими системами.
- недостатній контроль за доступом до критично важливих даних.
- відсутність регулярного навчання персоналу щодо кіберзагроз.

Правоохоронним органам необхідно впроваджувати комплексні заходи кібербезпеки, включаючи шифрування даних, багатофакторну автентифікацію, моніторинг аномальної активності та регулярне навчання співробітників, в тому числі як користуватися інструментами штучного інтелекту та яку інформацію туди заборонено завантажувати.

У законодавстві ЄС поняття інформаційної безпеки визначається насамперед у нормативно-правових актах, що стосуються кібербезпеки, захисту даних та захисту критичної інфраструктури. Основними правовими документами, в яких розглядається цей термін, є Директива NIS2 (Директива (ЄС) 2022/2555), GDPR (Регламент (ЄС) 2016/679) та Закон про кібербезпеку (Регламент (ЄС) 2019/881). Наведемо кілька ключових положень, які можна запозичити з європейських законодавчих ініціатив (NIS2, GDPR, Cybersecurity Act) для підвищення рівня інформаційної безпеки правоохоронних органів:

- ризик-орієнтований підхід до управління безпекою (NIS2) (запровадження системного управління ризиками, що враховує вразливості, загрози та потенційний вплив інцидентів на критичні функції. Правоохоронні органи мають регулярно проводити оцінку ризиків і вживати відповідних технічних і організаційних заходів).
- зобов'язання щодо оперативного реагування та повідомлення про інциденти (NIS2, GDPR) (становлення чітких процедур для виявлення, повідомлення та реагування на інциденти безпеки в стислий термін (наприклад, протягом 24–72 годин). Це дозволяє мінімізувати наслідки атак і координувати дії з іншими структурами).
- зміцнення кібергігієни та навчання персоналу (Cybersecurity Act, NIS2) (постійне підвищення обізнаності співробітників щодо сучасних кіберзагроз, у тому числі через навчання, симуляції фішингових атак та запровадження політик безпечного використання цифрових ресурсів).
- захист персональних даних та мінімізація їх обробки (GDPR) (впровадження принципів «privacy by design» і «data minimization» у процеси обробки персональних даних, зокрема при веденні кримінальних реєстрів або відеоспостереженні).
- сертифікація безпеки IT-рішень (Cybersecurity Act) (використання IT-продуктів і послуг, які мають сертифікацію кібербезпеки відповідно до європейських стандартів (ENISA), для забезпечення довіри до використовуваних технологій).
- міжвідомча співпраця та обмін інформацією (NIS2) (створення умов для безпечного обміну кіберзагрозами між національними і міжнародними структурами, зокрема через CSIRT, правоохоронні мережі та платформи співпраці.

Отже, необхідно також удосконалювати нормативно-правове регулювання у сфері забезпечення безпечного опрацювання інформації (включно з її пошуком, збиранням, аналізом, використанням, збереженням і поширенням) та застосуванням нових технологій, використання, збереження та поширення) і застосування нових технологій, рівень якого має відповідати розвитку цих технологій та інтересам суспільства. Цифрові технології мають сильний вплив на управлінські структури, включно з органами внутрішніх справ.

Органи, підрозділи системи МВС та центральні органи виконавчої влади, які координуються і спрямовуються міністром внутрішніх справ України:

- Національна поліція України
- Державна прикордонна служба України
- Державна служба України з надзвичайних ситуацій
- Національна гвардія України
- Державна міграційна служба України
- Головний сервісний центр МВС України

Інтенсивний розвиток процесу цифровізації спричиняє стрімкі зміни та технологічні інновації, які, у свою чергу, породжують складні юридичні виклики в межах цифрової екосистеми.

Суббот А., аналізуючи практичну діяльність правоохоронних органів, виокремив форми гарантування їхньої інформаційної безпеки на законодавчу (ухвалення нормативноправових актів, які встановлюють правила використання й обробки інформації, доступ до якої обмежено, та визначають ступінь відповідальності за порушення цих правил); та технічну (регулювання доступу до всіх ресурсів інформаційної системи (технічних, програмних, елементів баз даних), регламентація порядку роботи користувачів і персоналу, обмеження права доступу до окремих файлів тощо) [9; с. 22]. Ми, у свою чергу, визачимо організаційну форма, яка включає: розробку та впровадження внутрішніх політик і регламентів з інформаційної безпеки; створення та функціонування підрозділів (або відповідальних осіб) з інформаційної та кібербезпеки;періодичне навчання персоналу з питань кібергігієни, протидії фішингу, роботи з конфіденційною інформацією тощо.

- Встановлено, що загрози інформаційній безпеці поділяються на наявні та потенційно можливі явища і чинники, які можуть створити певну небезпеку інтересам людини, суспільства і держави в інформаційній сфері [10]. Керівникам структурних підрозділів апарату МВС, закладів, установ і підприємств, що належать до сфери управління МВС, було рекоментовано запровадити преведення ряду досліджень у сфері інформаційної безпеки, що свідчить про надзвичайну важливість даного питання [16].

Висновок. У сучасних умовах, коли цифровізація, гібридна війна з боку держави-агресора та стрімкий розвиток інформаційних технологій формують нові виклики у сфері національної безпеки, забезпечення інформаційної безпеки набуває пріоритетного значення в діяльності органів системи МВС України. Аналіз чинного законодавства України, практики правоохоронної діяльності та відповідних положень законодавства Європейського Союзу (зокрема, Директиви NIS2, GDPR та Регламенту про кібербезпеку) дозволяє зробити певні висновки.

Так, інформаційна безпека є складовою частиною національної безпеки України, що підтверджується положеннями РНБО та вимогами законодавства (Закони України «Про національну безпеку», «Про інформацію», «Про основні засади забезпечення кібербезпеки України»). Правоохоронні органи є розпорядниками критичної інформації, такої як персональні дані, кримінальні реєстри, електронні докази, що потребує особливого режиму захисту з урахуванням ризиків, пов'язаних із несанкціонованим доступом, витоком, модифікацією або знищенням даних.

Інформаційна безпека в системі МВС має гарантуватися на трьох рівнях:

законодавчому – через прийняття чітких нормативно-правових актів, що регулюють обробку, доступ та захист інформації;

технічному – шляхом використання сучасних засобів шифрування, сертифікованого програмного забезпечення, контролю доступу, багатофакторної автентифікації;

організаційному – через політики кібергігієни, навчання персоналу, моніторинг аномальної активності, внутрішній аудит та інші адміністративні заходи.

Враховуючи досвід ЄС, доцільно адаптувати до українських реалій такі європейські принципи:

- ризик-орієнтоване управління безпекою;
- зобов'язання щодо оперативного реагування на інциденти;
- підвищення обізнаності та сертифікація безпеки IT-рішень;
- міжвідомчий обмін кіберзагрозами.

Основні загрози, виявлені в контексті практичної діяльності МВС, мають переважно кібернетичний, технічний, соціально-психологічний і внутрішньоорганізаційний характер. Їхня класифікація та превенція повинні бути закріплені в системній стратегії інформаційної безпеки МВС із урахуванням міжнародного досвіду.

ЛІТЕРАТУРА

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України" : Указ Президента України від 25 лют. 2017 р. № 47/2017 // Офіц. вісн. Президента України. 2017. № 6. Ст. 172. URL: https://www.president.gov.ua/documents/472017-21374 (дата звернення: 21.07.2024).

2. Бойченко О. В. Політика інформаційної безпеки в системі інформаційного забезпечення органів внутрішніх справ // *Форум права*. 2009. № 1. С. 50–55.

3. Олійник О. В. Нормативно-правове забезпечення інформаційної безпеки в Україні //*Право і суспільство*. – 2012. – №. 3. – С. 132-137. С.135

4. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки України" : Указ Президента України від 28 груд. 2021 р. № 685/2021 // Офіц. вісн. Президента України. 2022. № 1. Ст. 24. URL: https://www.president.gov.ua/documents/6852021-410694 (дата звернення: 21.07.2024).

5. Кудінов В. А., Яровий К. В. Інформаційне забезпечення правоохоронної діяльності. 2024.

6. Сучасні пріоритети розвитку України: економічна та інформаційна безпека : матеріали Всеукр. наук.-практ. конф., м. Дніпро, 10 жовт. 2023 р. Дніпро : ДДУВС, 2023.

7. Про інформацію : Закон України від 02 жовт. 1992 р. № 2657-XII. URL: http://zakon4.rada.gov.ua/laws/show/1906-15 (дата звернення: 21.07.2024).

8. Банах С. Поняття інформаційної діяльності правоохоронних органів. 2019. Запоріз. обл. прокуратура. URL: https://zap.gp.gov.ua/ua/news.html?_m=publications&_c=view&_t=rec&id=382441 (дата звернення: 21.07.2024).

9. Суббот А. Інформаційна безпека діяльності працівників правоохоронних органів //*Віче*. – 2014. – №. 22. – С. 19-22.

10. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. URL: http://zakon4.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 21.07.2024).

11. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. URL: http://zakon2.rada.gov.ua/laws/show/2341-14 (дата звернення: 21.07.2024).

12. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 9 січ. 2007 р. № 537-V // Відом. Верховної Ради України. 2007. № 12. Ст. 102.

13. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII // Відом. Верховної Ради України. 2018. № 31. Ст. 241. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 21.07.2024).

14. Про рішення Ради національної безпеки і оборони України від 14 трав. 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України від 26 серп. 2021 р. № 447/2021 // Офіц. вісн. Президента України. 2021. № 22. Ст. 123. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 21.07.2024).

15. Новицький В. Я. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах // Інформація і право. 2022. № 1 (40). С. 111–118.

16. Про затвердження тематики наукових досліджень і науково-технічних (експериментальних) розробок на 2025–2029 роки : наказ МВС України від 21 трав. 2024 р. № 326. URL: https://mvs.gov.ua/normativno-pravovi-akti/nakaz-mvs-vid-21052024-326-pro-zatverdzennia-tematiki-naukovix-doslidzen-i-naukovo-texnicnix-eksperimentalnix-rozrobok-na-2025-2029-roki (дата звернення: 21.07.2024).