УДК 351.74:004.9
DOI https://doi.org/10.32782/2524-0374/2024-10/67

ІНФОРМАЦІЙНА КУЛЬТУРА ПРАВООХОРОНЦІВ: ПРОБЛЕМИ ТА ШЛЯХИ УДОСКОНАЛЕННЯ

INFORMATION CULTURE OF LAW ENFORCERS: PROBLEMS AND WAYS TO IMPROVE

Повалена М.В., к.ю.н., доцент,
доцент кафедри теорії права, конституційного та приватного права
Інститут з підготовки фахівців для підрозділів Національної поліції
Львівського державного університету внутрішніх справ,
доцент кафедри адміністративного та інформаційного права
Інститут права, психології та інноваційної освіти Національного університету «Львівська політехніка»

Здреник І.В., к.ю.н., доцент,
доцент кафедри теорії права, конституційного та приватного права
Інститут з підготовки фахівців для підрозділів Національної поліції
Львівського державного університету внутрішніх справ

У статті детально розглядаються основні аспекти інформаційної культури правоохоронців в Україні, акцентуючи увагу на актуальних проблемах, що виникають у зв'язку з недостатнім рівнем інформаційної безпеки. Автори аналізують недосконаліть законодавчої бази, яка не завжди відповідає сучасним викликам інформаційної безпеки. Відсутність єдиних етичних стандартів у роботі з конфіденційною інформацією створює ризики не лише для правоохоронних органів, але й для суспільства в цілому. У статті досліджуються проблеми, що виникають у процесі внутрішньої комунікації між підрозділами правоохоронних органів, що перешкоджає ефективному обміну інформацією та затримує процеси прийняття рішень.

Окрему увагу приділено порівнянню української практики з міжнародними стандартами, що впроваджуються в державах-членах Європейського Союзу та Сполучених Штатах Америки, де чітко визначені норми та процедури забезпечення інформаційної безпеки. Виявлені проблеми дають змогу зробити висновки щодо необхідності розвитку та вдосконалення нормативно-правової бази в Україні.

Запропоновані шляхи вдосконалення інформаційної культури, зокрема, впровадження нових технологій для внутрішньої комунікації, а також рекомендації щодо безпечного використання особистих пристроїв працівниками правоохоронних органів. Підкреслюється, що реалізація запропонованих заходів є необхідною для підвищення загальної ефективності роботи правоохоронних органів і зміцнення довіри суспільства до їхньої діяльності в умовах цифрової трансформації. Висвітлені в статті проблеми та шляхи їх вирішення можуть стати основою для подальших досліджень, що забезпечить захист та надійність правоохоронної системи України.

Ключові слова: інформаційна культура, правоохоронні органи, інформаційна безпека, кібербезпека, етичні стандарти, внутрішня комунікація, особисті пристрої, міжнародні стандарти, захист прав людини, цифрова трансформація.

The article provides an in-depth examination of key aspects of information culture among law enforcement officers in Ukraine, focusing on current issues arising from insufficient levels of information security. A significant issue highlighted is the lack of awareness among law enforcement personnel regarding cyber threats, which, in turn, heightens the risk of cybercrime and the compromise of confidential information.

The authors analyze deficiencies in the legislative framework, which often fails to align with modern information security challenges. The absence of unified ethical standards for handling confidential information creates risks not only for law enforcement agencies but also for society as a whole. The article examines issues in internal communication among law enforcement departments, which hinders effective information exchange and delays decision-making processes.

Special attention is given to comparing Ukrainian practices with international standards implemented in European Union member states and the United States, where clear norms and procedures for ensuring information security are established. Identified issues lead to conclusions on the necessity of developing and improving the regulatory framework in Ukraine.

The article also proposes ways to enhance information culture, including the introduction of new technologies for internal communication and recommendations for the safe use of personal devices by employees. It emphasizes that implementing these measures is essential for increasing the overall efficiency of law enforcement agencies and strengthening public trust in their activities amidst digital transformation. The issues and solutions highlighted in the article may serve as a foundation for further research in this critical area, thereby ensuring the security and reliability of Ukraine's law enforcement system.

Key words: information culture, law enforcement agencies, information security, cybersecurity, ethical standards, internal communication, personal devices, international standards, human rights protection, digital transformation.

В умовах сучасного інформаційного суспільства, коли технології швидко розвиваються, а кіберзагрози стають дедалі частішими, особливо під час війни, яку веде росія проти України, питання забезпечення інформаційної безпеки та дотримання етичних норм у роботі з даними є надзвичайно актуальними для правоохоронних органів та підкреслює необхідність впровадження ефективних заходів захисту інформації та розвитку відповідних етичних стандартів в умовах підвищених ризиків.

Людина повинна володіти не тільки комп'ютерною грамотністю – знаннями про призначення і можливості комп'ютера для обробки інформації, вміннями користуватися поширеними програмами, але й мати високий рівень інформаційно-технологічної культури [1, с. 618]. Ця вимога набуває особливої актуальності для працівників правоохоронних органів у сучасних умовах.

Інформаційна культура правоохоронців, яка охоплює знання, навички та цінності, пов'язані з використанням інформації та інформаційних технологій, є ключовим елементом для ефективного функціонування системи правопорядку. Роль інформаційної культури полягає не лише у здатності попереджати витоки даних і забезпечувати конфіденційність інформації, але й у дотриманні етичних стандартів під час роботи з конфіденційними даними. Це має особливе значення в контексті цифровізації державного управління та правоохоронної діяльності.

Метою цієї статті є аналіз проблем інформаційної культури в правоохоронних органах України та визначення можливих шляхів їх вирішення керуючись національним та міжнародним досвідом. Дослідження охоплює основні виклики, пов'язані з кібербезпекою, етичними аспектами роботи з інформацією, а також нормативно-правовим забезпеченням, що впливають на інформаційну культуру

правоохоронців. У статті розглянуто шляхи підвищення рівня інформаційної безпеки та сформовано пропозиції щодо вдосконалення підготовки працівників правоохоронних органів для роботи в умовах цифрових викликів.

Поняття «інформаційна війна» та «інформаційний тероризм» уже тривалий час використовуються і стали невід'ємною частиною сучасного світу, зокрема враховуючи воєнний стан. Інформаційні атаки стають потужним інструментом впливу, який може використовуватися для дезінформації, поширення тривоги, розколу в суспільстві та послаблення національної безпеки під час збройного протистояння.

Аналіз інформаційної культури в правоохоронних органах вказує на необхідність удосконалення знань та навичок працівників у сфері захисту інформації, що є критично важливим для гарантування національної безпеки та підвищення ефективності правоохоронної діяльності в умовах посилених ризиків.

Формування інформаційної культури майбутніх правоохоронців є першочерговим завданням, що полягає у формуванні їхніх навичок ефективної роботи з інформаційними ресурсами, вміння критично мислити та опановувати новітні інформаційні технології для професійної діяльності. Інформаційна культура включає навички пошуку, аналізу та використання інформації, що важливо як для професійного становлення, так і для загального розвитку курсантів. Важливо поєднувати теоретичну підготовку з практичними завданнями, які сприяють опануванню інформаційних технологій, необхідних для ефективної роботи в правоохоронній сфері.

Значна кількість працівників правоохоронних органів володіють базовими знаннями у сфері інформаційних технологій, але часто стикаються з труднощами в реалізації етичних стандартів у практичній діяльності. Зокрема, недостатня обізнаність у питаннях конфіденційності даних, кіберзахисту та інформаційної етики, може спричинити порушення прав людини та погіршення довіри населення до правоохоронних органів.

В Україні спостерігаються суттєві прогалини в законодавчій базі, які вимагають правового врегулювання, зокрема в контексті кібербезпеки та управління ризиками при обробці інформації в правоохоронних органах.

Аналізуючи існуючу нормативно-правову базу у сфері інформаційної безпеки в України слід зазначити, що основою правового забезпечення інформаційної культури є статті 11, 32, 34 Конституції України, якими визначено інформаційні та культурні права і свободи людини й громадянина. У ст. 34 зазначається, що кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань; кожному надається право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб. Отже, держава є гарантом безперешкодної реалізації та належного захисту прав громадян на інформацію, а відповідно, і є гарантом інформаційної безпеки.

Окрім Основного Закону, правовою основою розвитку інформаційної культури та забезпечення інформаційної безпеки слід зазначити Закони України «Про інформацію» від 02.10.1992, «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007, «Про захист інформації в інформаційно-комунікаційних системах» від 5.07.1994, «Про доступ до публічної інформації» від 13.01.2011, «Про захист персональних даних» від 01.06.2010, «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 та Указ Президента України від 26.08.2021 № 447/2021 яким введено в дію рішення Ради національної безпеки і оборони України від 14.05.2021 «Про Стратегію кібербезпеки України».

Нормативно-правова база, що регулює питання інформаційної безпеки в правоохоронних органах України, включає ряд законодавчих актів, основними з яких є *Закон України «Про захист персональних даних»* від 01.06.2010 – визначає принципи обробки та захисту інформації, а також Закон України «Про доступ до публічної інформації» від 13.01.2011, що забезпечує прозорість діяльності правоохоронних органів, Закон України «Про державну таємницю» від 21.01.1994 – регулює порядок обробки, зберігання та захисту інформації, що становить державну таємницю, Постанова Кабінету Міністрів України «Деякі питання документування управлінської діяльності» від 17.01.2018 – визначає правовий статус електронних документів, що використовуються в правоохоронних органах, Накази та постанови Міністерства внутрішніх справ України та Національної поліції України, що містять вимоги та рекомендації щодо забезпечення інформаційної безпеки в правоохоронних органах.

В умовах сьогодення на законодавчому рівні найбільш детально врегульовані питання інформаційно-аналітичного забезпечення Національної поліції України. Зокрема, ст. 25 Закону України «Про Національну поліцію» від 2.07.2015, визначено повноваження поліції у сфері інформаційно-аналітичного забезпечення. Зазначено, що поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень у таких напрямах: 1) формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; 2) користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади; 3) здійснює інформаційно-пошукову та інформаційно-аналітичну роботу; 4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями; 5) надає до Єдиного державного реєстру призовників, військовозобов'язаних та резервістів. Поліція може створювати власні бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчі інформаційно-аналітичні системи, необхідні для виконання покладених на неї повноважень [2].

Прикладом законного закріплення обов'язковості володіння певними елементами інформаційної культури є положення, викладені у ст. 25–27 Закону України «Про Національну поліцію», низки вимог щодо здійснення працівниками поліції окремих видів інформаційної діяльності, пов'язаних з оволодінням як інструментальними та комунікативними, так і ціннісними елементами інформаційної культури. Це охоплює питання щодо використання інформаційних ресурсів поліцейськими в цілях здійснення інформаційно-пошукової та інформаційно-аналітичної діяльності.

Для забезпечення ефективної роботи правоохоронних органів необхідно переглянути та вдосконалити існуючу нормативну базу щодо інформаційної безпеки. Рекомендується провести аналіз міжнародного досвіду, щоб визначити кращі практики, які можна адаптувати до української системи.

У міжнародній практиці, зокрема у Сполучених Штатах Америки (США) та державах-членах Європейського Союзу (ЄС), питання інформаційної безпеки та культури в правоохоронних органах регулюються через впровадження чітко визначених стандартів і нормативно-правових актів. У США, наприклад, існують комплексні програми підготовки, які передбачають не лише технічні аспекти, а й етичні норми, що регулюють обробку інформації.

У ЄС розроблено ряд директив і регламентів, що стосуються захисту особистих даних (GDPR) [3], які зобов'язують правоохоронні органи дотримуватися високих стандартів інформаційної безпеки. Ці практики можуть слугувати прикладом для України, адже їхній

досвід показує, що ефективна інформаційна культура формує довіру суспільства до правоохоронних органів та забезпечує більшу захищеність громадян.

У Європейському кодексі поліцейської етики 2001 р. (п. 42) вказано, що збирання, зберігання і використання персональних даних поліцією має здійснюватися відповідно до міжнародних принципів захисту даних і, зокрема, повинно бути обмежене в обсязі, необхідному для досягнення правових, легітимних і конкретних цілей. Однак неконтрольоване використання особистих даних може становити порушення прав відповідних осіб на повагу їхнього приватного життя. Задля уникнення зловживань під час збору, зберігання та використання особистих даних, ця діяльність поліції має регулюватися спеціальними принципами по захисту даних. Слід зазначити, що на рівні Ради Європи ці відносини регулюються Рекомендацію № R(87)15 Комітету Міністрів державам-членам, що визначає використання персональних даних у секторі поліції. Вказана Рекомендація щодо використання персональних даних поліцією містить напрями введення в дію принципів Конвенції Ради Європи № 108 в контексті обробки персональних даних поліцейськими органами. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 ратифікована Україною 06.07.2010.

Створення та впровадження етичних стандартів і кодексів поведінки для правоохоронців є важливим кроком у підвищенні інформаційної культури. Ці документи повинні чітко визначати, як працівники повинні обробляти конфіденційну інформацію, спілкуватися з громадськістю і співпрацювати один з одним. Впровадження етичних норм допоможе запобігти порушенням прав людини та зміцнити довіру суспільства до правоохоронних органів.

Отже, для забезпечення ефективності правоохоронної діяльності в Україні в умовах сучасних викликів необхідно вдосконалити інформаційну культуру правоохоронців через навчання, впровадження міжнародних стандартів та удосконалення нормативно-правової бази.

У процесі аналізу інформаційної культури правоохоронців в Україні було виявлено кілька ключових проблем, які негативно впливають на ефективність роботи правоохоронних органів, затримують прогрес у забезпеченні інформаційної безпеки та ускладнюють виконання службових обов'язків. Однією з найактуальніших проблем інформаційної культури правоохоронців є недостатня обізнаність щодо кіберзлочинності. Кіберзагрози, такі як фішинг, шкідливе програмне забезпечення та атаки на інформаційні системи, стають дедалі більш поширеними. Відсутність знань і навичок у сфері кібербезпеки серед працівників правоохоронних органів може спричинити атаки на їхні системи, а також до зниження довіри суспільства до здатності правоохоронців захистити інформацію громадян. Правоохоронці часто стикаються з етичними дилемами під час обробки особистих даних громадян. Відсутність чітких керівних принципів призводить до різноманітних підходів у трактуванні та дотриманні норм інформаційної етики, що може спричинити порушення прав людини та негативно впливає на довіру населення до правоохоронних органів. Етичні питання, пов'язані з використанням конфіденційної інформації, вимагають належного обговорення та визначення, щоб забезпечити відповідальність і прозорість у діяльності правоохоронців.

Внутрішня комунікація в правоохоронних органах також є важливою складовою інформаційної культури. Труднощі в обміні інформацією між різними підрозділами можуть призвести до затримок у прийнятті рішень та зниження оперативності реагування на загрози. Внутрішня комунікація часто обмежується формальними каналами, що ускладнює обмін важливою інформацією. Відсутність сучасних комунікаційних платформ є перешкодою на шляху до створення ефективної системи управління інформацією. Важливим аспектом інформаційної безпеки є регулювання використання особистих гаджетів працівниками правоохоронних органів. Розробка чітких політик використання особистих пристроїв для зменшення ризиків витоків даних. Слід визначити, які види інформації можуть зберігатися на особистих пристроях, а також які заходи безпеки повинні бути впроваджені. Наприклад, можна рекомендувати використання шифрування даних, встановлення антивірусного програмного забезпечення та обмеження доступу до конфіденційної інформації.

Зокрема, 19 вересня 2024 року Національний координаційний центр кібербезпеки ухвалив рішення обмежити використання Telegram в органах державної влади, військових формуваннях і на об'єктах критичної інфраструктури, що свідчить про усвідомлення необхідності посилення заходів безпеки в умовах сучасних викликів [4].

Для покращення внутрішньої комунікації в правоохоронних органах слід впроваджувати нові технології. Створення платформ для безпечного обміну інформацією дозволить забезпечити конфіденційність даних і зменшити ризик витоків інформації. Такі платформи можуть включати системи миттєвого обміну повідомленнями, закриті групи для обговорення важливих питань, а також інструменти для спільної роботи, для оперативного обміну інформацією що сприятиме підвищенню ефективності роботи.

Важливим аспектом інформаційної безпеки є регулювання використання особистих гаджетів працівниками правоохоронних органів. Розробка чітких політик використання особистих пристроїв для зменшення ризиків витоків даних. Слід визначити, які види інформації можуть зберігатися на особистих пристроях, а також які заходи безпеки повинні бути впроваджені. Наприклад, можна рекомендувати використання шифрування даних, встановлення антивірусного програмного забезпечення та обмеження доступу до конфіденційної інформації.

Недостатній рівень підготовки кадрів з питань інформаційної безпеки є однією з головних перешкод для розвитку інформаційної культури в правоохоронних органах. Системи навчання часто не охоплюють сучасні загрози та виклики, а також не забезпечують належного рівня практичної підготовки. Необхідно удосконалювати програми підвищення кваліфікації, які включатимуть новітні технології, етичні аспекти роботи з інформацією та кібербезпеку. Залучення експертів з міжнародного досвіду може значно покращити якість навчання. Одним із ключових шляхів покращення інформаційної культури серед правоохоронців є впровадження регулярних тренінгів та навчальних програм з основ кіберзахисту, виявлення загроз, реагування на інциденти та захист конфіденційної інформації. Важливо, щоб навчання проводилось не лише на початковому етапі роботи, але й на регулярній основі, з урахуванням нових загроз і технологій. Це дозволить відслідкувати за розвитком останніх змін у сфері інформаційної безпеки та покращить здатність реагувати на кіберзагрози. Систематичне підвищення кваліфікації працівників правоохоронних органів є невід'ємною частиною вдосконалення інформаційної культури. Впровадження програм сертифікації та акредитації з питань інформаційної безпеки допоможе забезпечити високий рівень професійної підготовки. Регулярне оновлення знань і навичок допоможе правоохоронцям ефективніше реагувати на сучасні виклики в сфері інформаційної безпеки.

Висновки. У сучасному інформаційному суспільстві, де швидкий розвиток технологій і зростаючі кіберзагрози стають реальністю, інформаційна культура правоохоронців відіграє вирішальну роль у забезпеченні національної безпеки та довіри населення. Дослідження показало, що недостатня обізнаність щодо кіберзлочинності, відсутність єдиних етичних стандартів та недостатня комуніка-

ція між різними підрозділами є основними проблемами, які перешкоджають ефективному функціонуванню правоохоронних органів.

Важливість формування високої інформаційної культури не можна переоцінити. Вона включає в себе не лише знання та навички, необхідні для роботи з інформаційними технологіями, але й дотримання етичних норм при обробці конфіденційних даних. В умовах війни та інформаційних атак, які веде агресор, працівники правоохоронних органів повинні бути готовими до швидкої реакції на нові виклики, що вимагає постійного вдосконалення їхніх знань і навичок.

Запропоновані в статті шляхи удосконалення інформаційної культури правоохоронців включають інтеграцію міжнародних стандартів, розробку чітких етичних норм та регулярне навчання з кібербезпеки. Окрім цього, необхідно зміцнити законодавчу базу, яка регулює питання інформаційної безпеки, щоб забезпечити правову основу для ефективного використання інформації в правоохоронній діяльності.

Таким чином, покращення інформаційної культури правоохоронців є невідкладним завданням, яке вимагатиме зусиль з боку держави, навчальних закладів та самих працівників правоохоронних органів для створення безпечнішого та ефективнішого середовища для захисту прав і свобод громадян. Тільки за умови системного підходу та активного впровадження нових стандартів можна досягти значних успіхів у зміцненні інформаційної безпеки та довіри суспільства до правоохоронних органів.

Подальші дослідження в цій сфері мають зосередитися на розвитку адаптивних підходів до інформаційної культури в умовах цифрової трансформації. Важливо вивчити нові виклики та можливості, які виникають у зв'язку з швидкими технологічними змінами і забезпечити готовність правоохоронців до реагування на ці виклики. Необхідність постійного вдосконалення підходів до інформаційної культури, відповідно до міжнародних стандартів і практик, стає ще більш актуальною в умовах глобалізації та інтеграції України у світове співтовариство.

ЛІТЕРАТУРА

1. Баландіна Н.М., Слатвінська В.М. Інформаційна культура інформатизованого суспільства. *Міжнародна науково-практична конференція «Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру» (з нагоди 30-річчя проголошення незалежності України та 25-річчя прийняття Конституції України)* : у 2 т. : (м. Одеса, 21 травня 2021). 2021. Т. 1. С. 616–618.
2. Закон України «Про Національну поліцію». *Відомості Верховної Ради*. 2015. № 40–41. Ст. 379.
3. Загальний регламент про захист даних (General Data Protection Regulation) 2016/679 URL: https://gdpr-text.com/uk/
4. НКЦК прийняв рішення обмежити використання Telegram в органах державної влади, військових формуваннях, на об'єктах критичної інфраструктури. Рада національної безпеки і оборони України. https://www.rnbo.gov.ua/ua/Diialnist/6994.html