ТАВОЛЖАНСЬКИЙ
ОЛЕКСІЙ ВОЛОДИМИРОВИЧ
кандидат юридичних наук, доцент кафедри кримінально-правової політики Національного юридичного університету імені Ярослава Мудрого
ORCID 0000-0001-8798-4820,

ДЕМИДОВА ЄВГЕНІЯ ЄВГЕНІЇВНА
кандидатка юридичних наук, доцентка, доцентка кафедри криміналістики Національного юридичного університету імені Ярослава Мудрого
ORCID 0000-0002-5049-7946
e-mail ye.ye.demydova@nlu.edu.ua8

УДК 348.8:004.056
DOI 10.37772/2518-1718-2026-1(53)-7

ДО ПИТАННЯ ІНФОРМАЦІЙНОЇ І КІБЕРБЕЗПЕКИ В ДІЯЛЬНОСТІ ОРГАНІВ ПРОБАЦІЇ

У статті здійснено комплексний аналіз проблем інформаційної та кібербезпеки в діяльності органів пробації України в умовах активної цифровізації державного управління та трансформації кримінально-виконавчої системи. Дослідження проведено крізь призму чинного нормативно-правового регулювання та практики діяльності уповноважених органів з питань пробації з урахуванням сучасних викликів і загроз у сфері захисту інформації.

Особливу увагу приділено труднощам забезпечення належного контролю та здійснення соціально-виховної роботи щодо суб'єктів пробації, зокрема в процесі збору, обробки, зберігання та передачі персональних даних. Наголошено, що впровадження інформаційно-комунікаційних технологій, електронних реєстрів і дистанційних форм взаємодії з особами, які перебувають на обліку пробації, одночасно підвищує ефективність роботи служби та створює додаткові ризики порушення інформаційної і кібербезпеки.

Встановлено, що досягнення високого рівня ефективності виконання завдань пробації потребує подальшого реформування форм і методів діяльності, впровадження інноваційних рішень, використання мобільних інструментів взаємодії, а також запозичення кращих міжнародних практик. Обґрунтовано необхідність формування комплексної системи забезпечення інформаційної та кібербезпеки, яка ґрунтується на поєднанні організаційних, технологічних і кадрових підходів.

Окремо підкреслено значення належного кадрового забезпечення, підвищення рівня цифрової компетентності персоналу органів пробації та вироблення узгодженої державної політики у сфері запобігання повторним кримінальним правопорушенням. За результатами дослідження сформульовано пропозиції щодо вдосконалення правового регулювання та посилення інституційної спроможності служби пробації з метою підвищення рівня інформаційної та кібербезпеки.

Ключові слова: пробація; органи пробації; суб'єкти пробації; нагляд; соціально-виховна робота; дистанційні форми контролю; мобільні додатки; кадрове забезпечення; воєнний стан; ресоціалізація.

Постановка проблеми. Забезпечення справедливого та безпечного суспільства, орієнтованого на мінімізацію правопорушень, визначається однією з ключових цілей інституту пробації. Пробація функціонує як система наглядових і соціально-виховних заходів, що застосовуються на підставі судового рішення та відповідно до вимог законодавства до осіб, засуджених до кримінальних покарань, не пов'язаних з позбавленням волі, а також у межах підготовки та надання суду інформації, необхідної для індивідуалізації кримінально-правового впливу. Серед базових цінностей діяльності органів пробації поряд із професіоналізмом, партнерською взаємодією та повагою особливе місце відводиться інноваційності, що передбачає безперервне підвищення кваліфікації персоналу, впровадження сучасних і ефективних інструментів роботи, а також адаптацію та інтеграцію кращих міжнародних практик.

Водночас реалізація інноваційного підходу в діяльності органів пробації супроводжується низкою нормативно-правових та організаційних проблем, які негативно впливають на ефективність здійснення як

наглядових, так і соціально-виховних функцій щодо осіб, до яких застосовано покарання, не пов'язані з позбавленням волі. Практика діяльності органів пробації свідчить про наявність прогалин у національному законодавстві щодо правового регулювання дистанційних форм контролю, диспропорцій у кадровому забезпеченні відповідних підрозділів, а також ускладнення взаємодії з суб'єктами пробації в умовах воєнного стану. Окремої уваги потребує відсутність комплексної та узгодженої державної політики у сфері запобігання повторним кримінальним правопорушенням, зокрема стосовно осіб, які перебувають на тимчасово окупованих територіях або мають статус внутрішньо переміщених осіб, що обумовлює необхідність наукового осмислення та вироблення системних підходів до вдосконалення діяльності органів пробації.

Метою дослідження є окреслення основних проблем забезпечення інформаційної та кібербезпеки в роботі органів пробації в Україні, а також встановлення ключових напрямів удосконалення нормативно-правового регулювання і організаційних механізмів діяльності уповноважених органів з питань пробації в кіберсфері.

Аналіз останніх досліджень і публікацій. У зв'язку із високою актуальністю забезпечення інформаційної та кібербезпеки державних органів України, особливо в умовах воєнного стану та посиленої цифрової трансформації суспільства, значна увага вітчизняних дослідників спрямована на дослідження та осмислення теоретико-методологічних, правових, організаційних і технологічних аспектів цього феномену.

Так, питанням впровадження інновацій в органи державної влади та правового регулювання інформаційної безпеки та кібербезпеки в них займалися Д. О. Красіков, А. М. Любчич, І. Кульчій, О. Ж. Скибун та інші. В свою чергу загалом питанням формування та реалізації державної політики у сфері інформаційної та кібербезпеки займалися, зокрема, О. В. Таволжанський, О. Ю. Горун, Л. Веселова, І. В. Діордіца, Р. В. Шаповал, В. О. Клочко, К. Захаренко.

Однак, наразі у науковому дискурсі наразі відсутні дослідження предметом яких є питання забезпечення інформаційної та кібербезпеки в органах пробації, що також підтверджує актуальність даної праці.

Виклад основного матеріалу. Завдяки прогресивному розвитку інформаційних технологій вочевидь відбувається й стрімка цифровізація державного управління, впровадження нових механізмів, використання різних інформаційних, інформаційно-комунікаційних систем, перехід до електронної форми документообігу шляхом створення відповідних електронних реєстрів, систем, мереж, які безперечно суттєво полегшують реалізацію органами державної влади, місцевого самоврядування покладених на них повноважень, проте водночас створюють нові ризики для інформаційного середовища публічної адміністрації.

Цікаво, що поступова цифровізація державного апарату в Україні, активний розвиток інформаційних технологій та перші законодавчі спроби регулювання безпеки у віртуальному просторі (кіберпросторі) - хронологічно збіглися з етапом становлення та активного впровадження національного інституту пробації, що зумовлює необхідність розкриття основних положень організаційного та правового забезпечення інформаційної та кібербезпеки органів пробації в Україні, оскільки інформаційна складова в роботі відносно нового та надзвичайно важливого органу виконавчої влади є визначальною, фактично вона забезпечує прийняття раціональних та своєчасних управлінських рішень у сфері нагляду за засудженими, соціально-виховної роботи, ефективної взаємодії з правоохоронними органами та судом, зокрема з використанням спеціально створених інформаційно-комунікаційних та інших систем.

Важливо також зазначити, що створення нового органу виконавчої влади, разом із стрімким розвитком інформаційних технологій вочевидь закономірно створило площину для розвитку нових суспільних відносин, у зв'язку з чим -одночасно збільшився діапазон ризиків і загроз для учасників цих суспільних відносин [1, с. 146-149].

Відтак, розбудова дієвих правових механізмів захисту цього простору є першочерговим і фундаментальним кроком на шляху до забезпечення виконання покарання у цілому і безпосередньо загальної безпеки функціонування інституту пробації в Україні.

Відповідно до ч. 1 ст. 4 Закону України «Про пробацію» (далі Закон) від 05.02.2015, метою пробації є забезпечення безпеки суспільства шляхом виправлення засуджених, запобігання вчиненню ними повторних кримінальних правопорушень та забезпечення суду інформацією, що характеризує обвинувачених, з метою прийняття судом рішення про міру їхньої відповідальності [2]. У свою чергу, відповідно до ст. 2 цього Закону під органом пробації розуміється центральний орган виконавчої влади, що реалізує державну політику у сфері пробації. Загалом аналіз положень вищезазначеного нормативно-правового акту свідчить, що інформаційний та кіберпростір охоплює діяльність органів пробації на всіх рівнях реалізації покладених на них завдань і повноважень.

Так, завдання пробації, визначені ст. 6 Закону України «Про пробацію» включають підготовку досудових доповідей щодо обвинувачених, здійснення

нагляду за засудженими до різних видів покарань, виконання покарань, не пов'язаних із позбавленням волі, направлення засуджених до виправних центрів, реалізацію пробаційних програм, проведення соціально-виховної роботи та підготовку осіб до звільнення. Реалізація цих завдань вочевидь передбачає збір, обробку, зберігання інформаційних баз та обмін великими обсягами персональних даних і службової інформації між органами пробації, судами, правоохоронними органами та іншими державними установами, що здійснюють нагляд або соціально-виховну роботу з засудженими. Сьогодні за підтримки проєктів ЄС "Pravo-Justice" та EDGE в Україні запущено та функціонує Єдиний реєстр засуджених та осіб, узятих під варту. Розпорядженням Кабінету Міністрів України від 06 вересня 2017 року № 608-р «Деякі питання обліку засуджених та осіб, узятих під варту» затверджено "Порядок формування та ведення Єдиного реєстру засуджених та осіб, узятих під варту" [3]. Зазначений документ багато в чому полегшує роботу персоналу пробації, але в той же час потребує додаткових знань, умінь і навичок для повноцінного та безпечного користування електронним реєстром.

Так, наприклад, ключовими елементами соціально-виховної роботи є залучення до суспільно корисної діяльності та освіта. Для належного забезпечення реалізації зазначених елементів соціально-виховної роботи безперечно необхідним є забезпечення можливості користування засудженими та працівниками органів пробації мережею Інтернет і сучасними інформаційними технологіями, оскільки саме вони створюють умови для доступу до освітніх ресурсів, дистанційних програм навчання, інформації про можливості працевлаштування, соціальні сервіси та державні електронні послуги тощо [4, с. 113-118].

Підготовка досудових доповідей (ст. 9 Закону) також потребує об'єднання інформації та документів із різних державних реєстрів, забезпечення їх достовірності та конфіденційності для прийняття об'єктивного судового рішення. Водночас, нагляд за засудженими та реалізація пробаційних програм ґрунтується на постійному моніторингу, веденні електронних обліків і використанні спеціалізованих інформаційних систем.

Відповідно, ефективне функціонування органів пробації неможливе без належного рівня інформаційної та кібербезпеки, оскільки будь-яке порушення цілісності, конфіденційності чи доступності даних може призвести до порушення прав громадян, збоїв у виконанні нагляду та пробаційних заходів і загрози громадській безпеці. Слушною є думка авторів які наголошують, що саме формування віктимологічного портрета потерпілих може стати основою для розробки ефективних заходів попередження кіберзлочинів [5, с. 464-488].

Варто звернути увагу на думку Д. О. Красікова, який зазначає, що інформаційна безпека - це стан захищеності прав та інтересів держави, суспільства та окремих осіб щодо збору, обробки, зберігання, розповсюдження та доступу до інформації, причому вона є складовою національної безпеки України [6, с. 173]. Теж саме стосується і кібербезпеки легальне визначення якої наведене у п. 5 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», відповідно до якого кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1].

Тобто фактично, забезпечення інформаційної та кібербезпеки повинно бути однією з провідних функцій органів пробації, оскільки це питання напряму корелюється з питанням забезпечення національної та громадської безпеки.

Наразі, питання правового регулювання забезпечення інформаційної безпеки та кібербезпеки в органах пробації здійснюється, або повинно б було здійснюватися – Законами України «Про інформацію», «Про захист персональних даних», «Про доступ до публічної інформації», «Про основні засади забезпечення кібербезпеки України», «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», Стратегією кібербезпеки затвердженої Указом Президента України від 26 серпня 2021 року №447/2021, Постановою КМУ від 16 листопада 2002 р. №1772 Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах, Постановою КМУ від 23 грудня 2020 р. №1295 Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, Наказом ДУ «Центра пробації» від 03.04.2023 №145/ОД-23 (далі Наказ).

Проте на практиці, аналіз вищезгаданого Наказу [8], дозволяє зробити висновок, що наразі органи з питань пробації у своїй діяльності задля забезпечення інформаційної та кібербезпеки вживають лише наступні заходи: забезпечення в установленому порядку розгляду звернень громадян, запитів на отримання публічної інформації та інших запитів і звернень згідно з чинним законодавством; забезпечення належного оформлення, повноти та достовірності даних; здійснення обробки та забезпечення захисту

персональних даних у випадках та в порядку встановленому законодавством. Зазначений перелік заходів містить лише мінімальні дії щодо забезпечення інформаційної безпеки, в свою чергу будь-які заходи задля забезпечення кібербезпеки взагалі відсутні.

Водночас, відповідно до вищезазначених нормативно-правових актів ефективне забезпечення інформаційної безпеки та кібербезпеки в органах пробації може бути досягнуто шляхом: забезпечення захисту персональних даних шляхом встановлення внутрішніх процедур обробки, контролю доступу, шифрування та моніторингу несанкціонованих спроб доступу; організацію контролю доступу та аутентифікації користувачів інформаційних систем із веденням журналів дій; ідентифікацію та управління ризиками кібербезпеки через періодичні аудити, тестування на вразливості та розробку планів реагування на кіберінциденти; захист критичних інформаційних ресурсів та систем шляхом резервного копіювання, встановлення засобів захисту від шкідливого ПЗ та забезпечення безперебійного функціонування систем; впровадження моніторингу, виявлення кіберзагроз і реагування на інциденти, а також обміну інформацією про загрози з іншими державними органами; підготовку та навчання персоналу з питань інформаційної та кібербезпеки, проведення інструктажів та тренінгів; розробку внутрішніх політик, регламентів і стандартів з інформаційної та кібербезпеки; забезпечення міжвідомчої взаємодії та координації з іншими державними органами у сфері кіберзахисту [9; 10; 11].

Окрему увагу також варто приділити Постанові Кабінету Міністрів України «Деякі питання реагування на кіберінциденти, кібератаки, кіберзагрози» від 26 листопада 2025 р. № 1533, якою закріплено єдині організаційні та процедурні засади реагування суб'єктів забезпечення кібербезпеки на кіберінциденти та кібератаки. Зазначений нормативно-правовий акт передбачає обов'язок державних органів впроваджувати внутрішні механізми виявлення, фіксації, аналізу та повідомлення про кіберінциденти, а також налагоджувати взаємодію з національною системою реагування, зокрема з CERT-UA та іншими уповноваженими суб'єктами. Наразі, положення даної Постанови також є необхідними до впровадження в діяльність органів пробації [12].

Висновок. Вочевидь, реалізація зазначених заходів є обов'язковою умовою належного функціонування органів пробації та напряму залежать від вмілого та професійного використання необхідних для цього технологій [13, с. 60-65], а їх ігнорування може призвести до низки негативних наслідків, серед яких: порушення конфіденційності та цілісності персональних даних засуджених і інших учасників процесу, несанкціонований доступ до службової інформації, підвищення ризику кібератак на інформаційні системи органів пробації, збої у функціонуванні електронних реєстрів та систем моніторингу, що у підсумку може спричинити неправомірні рішення суду, порушення прав людини, зниження ефективності соціально-виховної та наглядової роботи, а також загрозу громадській безпеці і національному інформаційному суверенітету.

Також, наразі у ДУ «Центр пробації» відсутній спеціальний структурний підрозділ до компетенції якого б належало забезпечення інформаційної безпеки та кібербезпеки, лише деякі формальні завдання закріплені за відділом цифровізації в пробації та відділом внутрішньої безпеки, що напряму пов'язано з одним із внутрішньополітичних детермінантів кіберзлочинності - відсутністю підготовки кваліфікованих фахівців, недостатній рівень міжнародної співпраці та фінансування, повільне впровадження інновацій в діяльність органів виконавчої влади [14, с. 158-164]. Загалом, вітчизняне законодавство у сфері інновацій має надто вузьке коло впливу на реальні економічні, соціально-економічні відносини. Ряд пільг, впроваджених задля стимулювання інноваційної діяльності було скасовано, а державні гарантії мають декларативний характер, у той час як національна інноваційна система (НІС) України потребує комплексного застосування усіх можливих засобів стимулювання [15, с. 25].

З метою підвищення рівня інформаційної та кібербезпеки в органах пробації необхідно сформувати комплексну систему заходів, що базується на організаційних, технологічних та організаційно-кадрових підходах. Серед ключових організаційних кроків можна виділити зокрема створення спеціалізованого підрозділу або сектора, відповідального за забезпечення інформаційної безпеки та захист державних інформаційних ресурсів, що має створити умови для централізованого координування політики безпеки та контролювати її виконання на всіх рівнях системи пробації. Цей підрозділ повинен реалізовувати внутрішні політики та регламенти щодо обробки, зберігання та передачі персональних і службових даних, включаючи шифрування інформації, управління доступом користувачів, ведення журналів дій та резервне копіювання критично важливих даних.

Також, важливо забезпечити системний підхід до управління ризиками кібербезпеки, що передбачає регулярне тестування інформаційних систем на вразливості, проведення аудитів, оцінку загроз та розробку планів реагування на кіберінциденти, що дозволить мінімізувати потенційні негативні наслідки порушень цілісності, конфіденційності та доступності даних. Не менш значущою є кадрова складова - підготовка та регулярне навчання персоналу з питань інформаційної та кібербезпеки, проведення інструк-

тажів та тренінгів щодо виявлення загроз і попередження несанкціонованого доступу.

Ключовим елементом ефективності системи може стати міжвідомча взаємодія, що передбачає обмін інформацією про кіберзагрози з іншими державними органами, правоохоронними структурами та органами судової влади, що дозволяє своєчасно виявляти та нейтралізувати потенційні ризики.

ЛІТЕРАТУРА

1. Таволжанський О. В. Деякі актуальні аспекти сучасної кримінально-правової політики в сфері забезпечення кібербезпеки України. *Актуальні проблеми протидії злочинності та корупції: збірник тез Всеукраїнської науково-практичної конференції.* Харків: Юрайт. 2023. С. 145–150. URL: https://surl.lt/risnvm (дата звернення 28.01.2026 р.).
2. Про пробацію: Закон України від 05.02.2015 №160-VIII URL: https://zakon.rada.gov.ua/laws/show/160-19#Text (дата звернення 28.01.2026 р.).
3. Про затвердження Порядку формування та ведення Єдиного реєстру засуджених та осіб, узятих під варту: Наказ Міністерства юстиції України від 26.06.2018 №2023/5 URL: https://zakon.rada.gov.ua/laws/show/z0762-18#Text (дата звернення 28.01.2026 р.).
4. Таволожанський О. В., Проценко О. А. Гуманізація системи виконання покарань як запорука виправлення засуджених. *Право та інноваційне суспільство*. 2021. № 1 (16). С. 113–118. DOI: 10.37772/2309-9275-2021-1(16)-16 (дата звернення 28.01.2026 р.).
5. Holovkin B., Cherniavskyi S., Tavolzhansky O. Factors of Cybercrime in Ukraine. *Relações Internacionais no Mundo Atual*. 2022. Vol. 3, No 41. C. 464-488 https://doi.org/10.21902/Revrima.v3i41.6401 (дата звернення 28.01.2026 р.)
6. Красіков Д. О. Правове забезпечення інформаційної безпеки в діяльності органів внутрішніх справ України: автореф. дис. ... канд. юрид. наук: 12.00.07. Київ. 2012. 220с. (дата звернення 28.01.2026 р.).
7. 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 28.01.2026 р.).
8. Наказ ДУ «Центра пробації» від 03.04.2023 №145/ОД-23 URL: https://drive.google.com/file/d/1rPPBO3barSfeK0Jo4hV3pAwuQcxhjetT/view?usp=sharing (дата звернення 28.01.2026 р.).
9. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: Постанова КМУ від 23 грудня 2020 р. №1295. URL: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text (дата звернення 28.01.2026 р.).
10. Стратегія кібербезпеки затверджена Указом Президента України від 26 серпня 2021 р. №447/2021 URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення 28.01.2026 р.).
11. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах: Постанова КМУ від 16 листопада 2002 р. №1772. URL: https://zakon.rada.gov.ua/laws/show/1772-2002-%25D0%25BF#Text (дата звернення 28.01.2026 р.).
12. Деякі питання реагування на кіберінциденти, кібератаки, кіберзагрози: Постанова КМУ від 26 листопада 2025 р. №1533 URL: https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#Text (дата звернення 28.01.2026 р.).
13. Демидова Є. Є. Цифрові технології в кримінальному провадженні: сучасні підходи й тенденції застосування. *Слідча та детективна діяльність: виклики і перспективи*. Харків, 2023. С. 60–65. URL: https://ivpz.kh.ua/wp-content/uploads/2023/10/Збірник-Слідча-та-детективна-діяльність_25.05.23.pdf (дата звернення 28.01.2026 р.).
14. Таволжанський, О. В. Основи державної кіберполітики України: формування та реалізація. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького*. Серія: Право, 2017, 4. С. 158-164 Режим доступу: http://nbuv.gov.ua/UJRN/Nivif_2017_4_27 (дата звернення 28.01.2026 р.).
15. Любчич А. М. Стимулювання інновацій в державному секторі: зарубіжний досвід. *Право та інновації*. № 1 (29) 2020. С.22-27 URL: http://openarchive.nure.ua/handle/document/14766 (дата звернення 26.01.2026 р.).

REFERENCES

1. Tavolzhansky, O. V. (2023). Some current aspects of modern criminal-legal policy in the field of ensuring cybersecurity in Ukraine. Actual Problems of Combating Crime and Corruption: Collection of Abstracts of the All-Ukrainian Scientific and Practical Conference, 145–150. Retrieved from https://surl.lt/risnvm [in Ukrainian].
2. Verkhovna Rada of Ukraine. (2015). On Probation: Law of Ukraine No. 160-VIII of 05.02.2015. Retrieved from https://zakon.rada.gov.ua/laws/show/160-19#Text [in Ukrainian].

3. Ministry of Justice of Ukraine. (2018). On Approval of the Procedure for Formation and Maintenance of the Unified Register of Convicts and Persons Taken into Custody: Order No. 2023/5 of 26.06.2018. Retrieved from https://zakon.rada.gov.ua/laws/show/z0762-18#Text [in Ukrainian].
4. Tavolzhansky, O. V., & Protsenko, O. A. (2021). Humanization of the penal system as a guarantee of the correction of convicts. Law and Innovative Society, (1(16)), 113–118. https://doi.org/10.37772/2309-9275-2021-1(16)-16 [in Ukrainian].
5. Holovkin, B., Cherniavskyi, S., & Tavolzhansky, O. (2022). Factors of cybercrime in Ukraine. Relações Internacionais no Mundo Atual, 3(41), 464–488. https://doi.org/10.21902/Revrima.v3i41.6401 [in English].
6. Krasikov, D. O. (2012). Legal support of information security in the activities of internal affairs bodies of Ukraine: Candidate of Law dissertation abstract (12.00.07). Kyiv, Ukraine. [in Ukrainian].
7. Verkhovna Rada of Ukraine. (2017). On the Main Principles of Ensuring Cybersecurity of Ukraine: Law of Ukraine No. 2163-VIII of 05.10.2017. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].
8. State Institution "Probation Center". (2023). Order No. 145/OD-23 of 03.04.2023. Retrieved from https://drive.google.com/file/d/1rPPBO3barSfeK0Jo4hV3pAwuQcxhjetT/view?usp=sharing [in Ukrainian].
9. Cabinet of Ministers of Ukraine. (2020). On Certain Issues of the Functioning of the System for Vulnerability Detection and Response to Cyber Incidents and Cyber Attacks: Resolution No. 1295 of 23.12.2020. Retrieved from https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text [in Ukrainian].
10. President of Ukraine. (2021). Cybersecurity Strategy of Ukraine: Decree No. 447/2021 of 26.08.2021. Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#Text [in Ukrainian].
11. Cabinet of Ministers of Ukraine. (2002). On Approval of the Procedure for Interaction of Executive Authorities in the Protection of State Information Resources in Information and Electronic Communication Systems: Resolution No. 1772 of 16.11.2002. Retrieved from https://zakon.rada.gov.ua/laws/show/1772-2002-%25D0%25BF#Text [in Ukrainian].
12. Cabinet of Ministers of Ukraine. (2025). On Certain Issues of Response to Cyber Incidents, Cyber Attacks, and Cyber Threats: Resolution No. 1533 of 26.11.2025. Retrieved from https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#Text [in Ukrainian].
13. Demydova, Ye. Ye. (2023). Digital technologies in criminal proceedings: Modern approaches and application trends. Investigative and Detective Activity: Challenges and Prospects, 60–65. Retrieved from https://ivpz.kh.ua/wp-content/uploads/2023/10/Збірник-Слідча-та-детективна-діяльність_25.05.23.pdf [in Ukrainian].
14. Tavolzhansky, O. V. (2017). Basics of state cyberpolicy of Ukraine: Formation and implementation. Scientific and Informational Bulletin of Ivano-Frankivsk University of Law named after King Danylo Halytskyi. Series: Law, 4, 158–164. Retrieved from http://nbuv.gov.ua/UJRN/Nivif_2017_4_27 [in Ukrainian].
15. Liubchych, A. M. (2020). Stimulating innovation in the public sector: International experience. Law and Innovation, (1(29)), 22–27. Retrieved from http://openarchive.nure.ua/handle/document/14766 [in Ukrainian].

TAVOLZHANSKY OLEKSII

Candidate of juridical sciences (PhD in Law), Associate professor, Associate professor of the Department of Criminal Law Policy, Yaroslav Mudryi National Law University,

DEMYDOVA YEVHENIIA

Candidate of juridical sciences (PhD in Law), Associate professor, Associate Professor of the Department of Criminalistics, Yaroslav Mudryi National Law University

ON THE ISSUE OF INFORMATION AND CYBERSECURITY IN THE ACTIVITIES OF PROBATION AUTHORITIES

Background. The rapid development of information technologies and the intensive digitalization of public administration significantly affect the functioning of the probation system in Ukraine. Along with positive effects related to efficiency, accessibility, and optimization of control and supervisory measures, these processes generate new risks in the field of information and cybersecurity, particularly in relation to the processing and protection of personal data of probation subjects.

Purpose. The purpose of the article is to analyze the current state of information and cybersecurity in the activities of probation authorities in Ukraine through the prism of regulatory and legal regulation and practical implementation, as well as to identify key problems and outline priority directions for improving institutional capacity in this area under modern conditions.

Methods. The study is based on a set of general scientific and special legal research methods, including analysis and synthesis, formal-legal, comparative-legal, systemic and structural-functional methods. Normative legal acts regulating probation activities, information protection and personal data processing were analyzed, along with practical aspects of the functioning of authorized probation bodies.

Results. The article identifies significant difficulties in ensuring effective control and social-educational work with probation subjects in the context of digital interaction and remote forms of influence. Particular attention is paid to risks related to the collection, storage, processing and transmission of personal data, as well as vulnerabilities caused by insufficient technical protection, fragmented legal regulation and limited digital competencies of personnel. It is established that achieving high efficiency in probation tasks requires reforming traditional forms and methods of work, implementing innovative digital solutions, mobile communication tools, and adopting best international practices. The necessity of forming an integrated system of information and cybersecurity based on organizational, technological and human resource approaches is substantiated.

Conclusions. The study concludes that strengthening information and cybersecurity in the activities of probation authorities is a prerequisite for effective prevention of repeated criminal offenses and sustainable development of the probation system. The article emphasizes the need to eliminate gaps in legal regulation, enhance interagency coordination, improve personnel training, and develop a coherent state policy in the field of information protection. The proposed measures are aimed at increasing the institutional resilience of probation authorities and ensuring a balance between digital innovation and the protection of fundamental rights.

Keywords: probation; probation authorities; probation subjects; supervision; social and educational work; remote forms of control; mobile applications; staffing; martial law; resocialization.

За ДСТУ 8302:2015 цю статтю слід цитувати:

Таволжанський О. В., Демидова Є. Є. До питання інформаційної і кібербезпеки в діяльності органів пробації. *Право та інновації*. 2026. № 1 (53). С. 63–69. https://doi.org/10.37772/2518-1718-2026-1(53)-7.

Дата подання автором: 28.01.2026
Дата прийняття після рецензування: 20.02.2026
Дата опублікування: 29.04.2026