Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

УДК 343.13 (477)

DOI https://doi.org/**10.5281/zenodo.15186978**

Інноваційні підходи до забезпечення безпеки учасників кримінального судочинства: методологічні засади та перспективи розвитку

Гриньків Олександра Олексіївна

доктор юридичних наук, старший викладач кафедри спеціальних дисциплін, Національна академія Державної прикордонної служби України імені Богдана Хмельницького, Україна, м. Хмельницький, alexandra.pravo@gmail.com, https://orcid.org/0000-0003-1002-7955

Прийнято: 14.03.2025| Опубліковано: 29.03.2025

Анотація. *У статті розглянуто проблеми забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві, з урахуванням сучасних викликів та розвитку технологій. За результатами аналізу нормативно-правового регулювання захисту таких осіб, вказано на відсутність єдиної концепції оцінки загроз та уніфікованих підходів до управління ризиками.*

Запропоновано використання евристичних моделей для оперативного оцінювання загроз, а також інтегрування кількісних методів аналізу, зокрема багатофакторного регресійного аналізу, теорії ігор та імітаційного моделювання. Визначено перспективність застосування штучного інтелекту та машинного навчання для прогнозування ризиків, виявлення латентних загроз та персоналізації заходів захисту.

Окрему увагу приділено питанням забезпечення конфіденційності даних у межах реалізації Програм захисту, обґрунтовано необхідність впровадження

криптографічних технологій, блокчейн-рішень та ступенів багаторівневого контролю доступу до конфіденційних даних.

Результати дослідження вказують на необхідність розробки та впровадження певних моделей оцінки загроз, що здатні враховувати динамічні зміни у суспільстві, розвиток технологій та міждисциплінарний підхід до формування стратегії захисту учасників кримінального судочинства.

Ключові слова: *забезпечення безпеки, захист, учасник кримінального судочинства, Програма захисту, оцінка загроз, управління ризиками, штучний інтелект, конфіденційність.*

Innovative Approaches to Ensuring the Security of Criminal Justice Participants: Methodological Foundations and Development Prospects

Hrynkiv Oleksandra Oleksiivna

Doctor of Law, Senior lecturer at the Department of Special disciplines Bohdan Khmelnytskyi National Academy of the State Border Service of Ukraine, Khmelnytskyi, Ukraine, alexandra.pravo@gmail.com, https://orcid.org/0000-0003-1002-7955

Abstract. *The article examines the challenges of ensuring the security of individuals involved in criminal proceedings, considering modern threats and technological advancements. The shortcomings of the current regulatory framework for the protection of witnesses and victims are analyzed, particularly the lack of a unified threat assessment concept and standardized risk management approaches.*

The study proposes the use of heuristic models for rapid threat assessment, as well as the integration of quantitative analysis methods, including multifactor regression analysis, game theory, and simulation modeling. The prospects of applying artificial intelligence and machine learning for risk forecasting, latent threat detection, and the personalization of protection measures are identified.

Special attention is given to data confidentiality within protection programs, where the necessity of implementing cryptographic technologies, blockchain solutions, and multi-level access control policies is substantiated.

The research results indicate the need to develop adaptive threat assessment models capable of considering the dynamic changes in the security environment and applying an interdisciplinary approach to forming strategies for protecting witnesses and victims.

Keywords: *security provision, protection, participant in criminal proceedings, Protection Program, threat assessment, risk management, artificial intelligence, confidentiality.*

Постановка проблеми. Забезпечення безпеки учасників кримінального судочинства залишається тим питанням, яке завжди є актуальним як в теорії, так і на практиці.

Безумовно, забезпечення захисту таких осіб є доволі складною діяльністю на практиці, оскільки вимагає застосування не лише системного підходу, а й високого рівня професійної компетентності суб'єктів, відповідальних за його реалізацію. Зауважимо, що ефективність такого процесу безпосередньо залежить від якості ухвалених управлінських рішень, ступеня їхньої обґрунтованості та своєчасності, а також від рівня впровадження інтегрованих підходів до безпекових заходів, що поєднують правові, організаційні, технічні та психологічні аспекти. При цьому надзвичайно важливим є врахування високого рівня суб'єктивності під час оцінювання загроз, а також значної невизначеності динаміки безпекових процесів, що можуть безпосередньо впливати на фізичний і психологічний стан учасників кримінального судочинства. Це вимагає розроблення інноваційних методологічних підходів до керування ризиками, які поєднуватимуть використання методів прогнозування на підставі аналізу великих масивів даних, осмислення різних сценаріїв загроз та запровадження відповідних стратегій реагування.

На нашу думку, впровадження механізмів оперативного моніторингу загроз (що можуть мати місце для учасників кримінального судочинства), зокрема із залученням інтелектуальних систем аналізу даних, дозволить створити гнучку та ефективну систему безпеки, яка здатна своєчасно пристосовуватися до умов, що змінюються, та швидко реагувати на нові виклики.

Аналіз останніх досліджень і публікацій. В Україні дослідження проблеми забезпечення безпеки учасників кримінального судочинства започаткували В.С. Зеленецький та М.В. Куркін. В подальшому окремі питання вивчали: В.П. Бахін, В.І. Бояров, В.К. Весельський, В.В. Войніков, В.І. Галаган, В.В. Гевко, Г.І. Глобенко, О.В. Гогусь, О.В. Ільченко, Н.С. Карпов, В.В. Касько, Б.М. Качмар, С.В. Ковмир, Є.Є. Кондратьєв, О.Д. Котова, В.С. Кузьмічов, Є.Д. Лук'янчиков, А.О. Ляш, І.А. Малютін, В.Т. Маляренко, А.М. Орлеан, Т.І. Панасюк, Н.В. Пелипенко, М.А. Погорецький, К.О. Ромодановський, О.І. Ромців, С.М. Стахівський, Р.В. Тарасенко, А.А. Тимошенко, Р.Р. Трагнюк, В.М. Тертишник, О.В. Усенко, К.Д. Шевченко, Л.М. Шестопалова, Т.В. Шимко, А.А. Юнусов та ін.

Як бачимо, проблема забезпечення безпеки учасників кримінального процесу привертала увагу не лише вчених, а й практиків, оскільки є саме тим важелем, який передбачає створення належних умов для всебічного, повного та об'єктивного встановлення всіх обставин під час розслідування кримінального провадження [1, с. 4].

В.С. Зеленецький та М.В. Куркін свого часу наголошували, що будь-яка небезпека викликає у людини потребу в захисті [2, с. 85], що є особливо актуальним в умовах сьогодення [3] та потребує інноваційних підходів до його негайного забезпечення.

Впровадження інноваційних підходів щодо забезпечення безпеки зазначених суб'єктів наразі залишається відкритим, тому питання розвитку такої діяльності залежить від подальшого удосконалення методології захисту в повному обсязі.

Формулювання цілей статті (постановка завдання).

Метою статті є дослідження особливостей новітніх підходів до забезпечення безпеки учасників кримінального судочинства в сучасних умовах.

Завдання:

1. Розглянути проблемні питання щодо забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві, з урахуванням сучасних викликів.

2. Проаналізувати методологію прийняття рішень щодо захисту таких суб'єктів.

3. Окреслити окремі питання забезпечення конфіденційності даних у межах реалізації Програм захисту.

4. Сформулювати пропозиції для належного рівня захисту учасників кримінального процесу.

Викладення основного матеріалу дослідження. Раніше ми вже детально розглядали сутність забезпечення безпеки [4, с. 106 – 109], тому не зупинятимось на цьому.

Разом з тим, проведений нами тоді аналіз норм чинного кримінального процесуального законодавства України свідчив про те, що вітчизняне нормативно-правове регулювання забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві, потребує удосконалення. При цьому, нами вказано на головний недолік – відсутність єдиної концепції. Сформульовані в подальшому у дисертації та монографії висновки і пропозиції за результатами наукової діяльності й практичного досвіду роботи [1; 4] мали би призвести до покращення напряму цієї діяльності. Однак, враховуючи тривалий період часу, події сьогодення, розвиток інформаційних технологій тощо, варто зазначити, що забезпечення безпеки суб'єктів кримінального процесу потребує нових підходів задля вирішення проблеми захисту.

Зауважимо, що відсутність в національній системі кримінального судочинства уніфікованих процедур оцінки загроз впливає на прийняття управлінських рішень та значною мірою знижує ефективність функціонування Програм захисту, створюючи умови для використання шаблонних підходів, які

не враховують унікальні особливості кожного випадку. Така ситуація обумовлює недостатню адаптивність безпекових заходів до динамічно змінюваного середовища загроз, що, у свою чергу, може призвести до неадекватного реагування на нові виклики. Крім того, відсутність систематизованих алгоритмів оцінювання ризиків ускладнює процес прийняття обґрунтованих рішень щодо застосування конкретних заходів захисту, збільшуючи рівень суб'єктивності та ймовірність помилкових оцінок тощо [5, с. 198; 6, с. 137].

Основними методологічними засадами прийняття рішень у сфері забезпечення безпеки учасників кримінального судочинства є застосування евристичних моделей, що дозволяють здійснювати оперативну оцінку загроз шляхом використання експертних методів та якісного аналізу ризиків, які забезпечують можливість врахування широкого спектру факторів, що впливають на безпекову ситуацію.

Евристичні підходи, будучи пристосованими до змінного середовища, сприяють оперативному прийняттю рішень, зокрема в умовах високої невизначеності та фрагментарності безпекової інформації. Вони дозволяють враховувати нелінійність загрозливих факторів, взаємозалежність різноманітних ризиків і специфіку психологічного стану захищених осіб. Водночас евристичні моделі можуть ефективно доповнюватися методами кількісного аналізу, такими як багатофакторний регресійний аналіз та методи нечіткої логіки, що дозволяє підвищити точність прогнозування потенційних ризиків та формування персоналізованих заходів безпеки. Вчені обґрунтовують, що використання евристичних моделей у поєднанні з аналітичними підходами дозволяє досягти оптимального балансу між швидкістю та точністю прийняття рішень, що дуже важливо у контексті мінливих загрозливих ситуацій [7; 8; 9].

Результати останніх наукових досліджень у сфері захисту свідків і потерпілих свідчать, що недостатня аналітична підтримка управлінських рішень може призвести до неефективних або суперечливих заходів, знижуючи загальну результативність Програм захисту та створюючи ризики для їхньої реалізації. Це зумовлює необхідність вдосконалення методологічних підходів до аналізу

ризиків, які б враховували не лише кількісні, але й якісні аспекти загроз, забезпечуючи комплексний підхід до управління ризиками. Складність реалізації Програм захисту вимагає розробки адаптивних моделей оцінки ризиків, здатних своєчасно реагувати на сучасні виклики та використовувати інноваційні підходи до управління інформацією, зокрема методи штучного інтелекту та алгоритми машинного навчання (підгалузь штучного інтелекту, яка спеціалізується на аналізі даних і самонавчанні систем [10]). Удосконалення процесів прийняття рішень в межах Програм захисту потребує активного залучення міждисциплінарних підходів та використання сучасних технологій аналізу великих масивів даних для підвищення точності прогнозів і ефективності заходів захисту тощо.

Серед формальних методів аналізу ризиків, що застосовуються в керуванні безпековими програмами, виділяють методи лінійної регресії, імітаційного моделювання та теорії ігор, які забезпечують можливість кількісної оцінки ризиків шляхом математичного моделювання та прогнозування наслідків реалізації різних стратегій. Лінійна регресія дозволяє ідентифікувати залежності між змінними та здійснювати прогнозування на основі історичних даних, тоді як імітаційне моделювання надає змогу відтворювати можливі сценарії розвитку ситуації з урахуванням випадкових факторів. Теорія ігор, у свою чергу, є потужним інструментом для прийняття стратегічних рішень у конфліктних ситуаціях, що передбачають взаємодію між кількома зацікавленими сторонами. Проте ефективність цих методів значною мірою детермінується якістю вхідних даних, що включає не лише їхню точність і повноту, а й релевантність до актуальної безпекової ситуації. Адекватність обраної моделі визначається її здатністю до адаптації в умовах мінливої загрозливої обстановки, а також відповідністю специфіці кримінального провадження. Коректність інтерпретації отриманих результатів безпосередньо впливає на прийняття обґрунтованих управлінських рішень, що вимагає високого рівня кваліфікації аналітиків та застосування комплексного підходу до оцінки результатів, зокрема шляхом

порівняльного аналізу кількох моделей та інтеграції різних джерел інформації [11].

Крім того, використання методів валідації моделей та їхнього постійного оновлення на основі нових безпекових даних є доволі важливим для забезпечення актуальності оцінок та підвищення ефективності Програм захисту. Для підвищення надійності оцінок важливим фактором є інтеграція формальних методів з експертними оцінками, що дозволяє враховувати як явні, так і латентні фактори, що важко піддаються кількісному вимірюванню за допомогою стандартних статистичних інструментів. Залучення експертного середовища дозволяє використовувати накопичений професійний досвід і суб'єктивні знання для уточнення параметрів формальних моделей, підвищення їхньої адаптації до конкретних умов кримінального провадження.

Поза тим, застосування методів багатокритеріального аналізу та когнітивного моделювання дозволяє синтезувати об'єктивні дані з якісними характеристиками безпекової ситуації, забезпечуючи таким чином комплексну оцінку ризиків. Водночас важливим в цьому сенсі є використання міждисциплінарного підходу, який передбачає залучення фахівців з різних галузей – криміналістики, психології, соціології та інформаційної безпеки задля створення більш повної картини загроз та вироблення дієвих стратегій реагування на небезпеку.

Процес прийняття рішень щодо унікальних випадків загроз у межах Програм захисту вимагає багаторівневого аналізу, що охоплює використання гіпотетичних припущень, аналіз ретроспективних даних та прогнозування на основі сучасних методів аналітики. Такий підхід обумовлює значні виклики для керівників підрозділів захисту, оскільки він передбачає необхідність одночасного врахування великої кількості змінних, включаючи правові, соціальні, технічні та психологічні аспекти [11].

Крім зазначеного, оптимальний вибір стратегій безпеки потребує очевидної інтеграції аналітичних підходів, таких як багатофакторний аналіз ризиків, із практичним досвідом фахівців та інтуїтивними судженнями, які базуються на

багаторічній практиці і здатності оперативного реагування на нестандартні ситуації. Використання методологій аналізу сценаріїв, оцінки чутливості та системного підходу до управління ризиками дозволяє створювати динамічні безпекові моделі, здатні адаптуватися до швидкозмінного середовища загроз та забезпечити високий рівень захисту учасникам кримінального судочинства.

Наголосимо, що в умовах сьогодення ми маємо справу з штучним *інтелектом, який є* надзвичайно потужним інструментом, що *дозволяє не лише* автоматизувати процес завчасного *виявлення загроз,* але й дозволяє оцінювати та пом'якшувати потенційні *загрози [12; 10]*.

Інтеграція штучного інтелекту в систему оцінювання загроз є важливим етапом у вдосконаленні Програм захисту, оскільки вона дозволяє не лише підвищити точність прогнозування ризиків, а й забезпечити оперативне виявлення нових загрозливих факторів.

Використання методів машинного навчання, включаючи глибокі нейронні мережі, алгоритми кластерного аналізу та обробку природної мови (NLP), дозволяє аналізувати великі обсяги різнорідних даних з відкритих та закритих джерел. Це сприяє ідентифікації латентних загроз, оцінці поведінки потенційних зловмисників і передбаченню можливих сценаріїв розвитку ситуації. Водночас, поєднання регресійного аналізу, методів сучасної оцінки ризиків, дозволяє підвищити надійність прогнозів і мінімізувати похибки, що є властивими окремим підходам. Також важливим стає використання алгоритмів адаптивного навчання, які здатні самостійно коригувати параметри оцінювання ризиків після надходження нових даних, що забезпечує постійну актуальність безпекових стратегій [13].

Відзначимо, що вагомим аспектом реалізації Програм захисту є забезпечення конфіденційності персональних даних учасників кримінального судочинства, що безперечно є необхідною умовою ефективного функціонування всієї системи безпеки. Використання сучасних методів криптографічного захисту, зокрема шифрування даних на всіх етапах їх обробки та зберігання, а також впровадження протоколів аутентифікації та авторизації, є ключовими

факторами, що забезпечують захист від несанкціонованого доступу. Окрім цього, важливим є впровадження багаторівневого контролю доступу користувачів, що дозволяє мінімізувати ризики витоку інформації. Використання блокчейн-технологій [14 – 16] для забезпечення цілісності та незмінності критично важливих даних також є перспективним напрямом, що сприяє підвищенню довіри до механізмів захисту. Важливим елементом є розробка та імплементація процедур регулярного аудиту безпеки, які дозволяють своєчасно виявляти потенційні вразливості та вдосконалювати механізми захисту інформації. Зауважимо, комплексний підхід до забезпечення конфіденційності включає не лише технічні заходи, але й нормативно-правові механізми, що регламентують обробку, зберігання та передачу даних, а також підвищення рівня обізнаності персоналу щодо ризиків та методів захисту конфіденційної інформації.

Висновки. Таким чином, процес прийняття управлінських рішень у сфері захисту учасників кримінального судочинства потребує системного та інтегрованого підходу, який базується на поєднанні сучасних технологій, аналітичних методів, експертних оцінок та нормативно-правового регулювання. Впровадження комплексної системи моніторингу загроз, що ґрунтується на аналізі великих масивів даних, прогнозуванні за допомогою штучного інтелекту та машинного навчання, дозволить забезпечити своєчасне реагування на потенційні ризики. Адаптивні моделі безпеки, які використовують сценарне планування та методи імовірнісного аналізу, сприятимуть підвищенню ефективності реалізації Програм захисту, враховуючи динаміку загрозливого середовища.

Крім того, важливим компонентом ефективного управління безпековими процесами є міжвідомча взаємодія та обмін інформацією між правоохоронними органами, що дозволяє створити єдину платформу для координації заходів захисту та забезпечення оперативного реагування.

Таким чином, реалізація зазначених заходів сприятиме не лише забезпеченню належного рівня захисту учасників кримінального процесу, але й підвищенню довіри суспільства до механізмів правосуддя. Впровадження єдиних

методичних стандартів, що засновані на передових практиках міжнародного досвіду, дозволить створити ефективну систему виявлення загроз на початкових стадіях, сприятиме диференційованому підходу до розробки стратегій захисту та підвищить загальну ефективність Програм захисту тощо.

Список використаних джерел

1. Гриньків О.О. Застосування заходів безпеки учасників кримінального судочинства: вітчизняна практика та світовий досвід : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ. нац. ун-т внутр. справ. Київ, 2010. 20 с.

2. Зеленецький В. С. Поняття безпеки та її забезпечення суб'єктам кримінального процесу. *Вісник ун-ту внутр. справ МВС України.* Харків, 1997. Вип. 2. С. 84 – 88.

3. Гриньків О.О. Окремі аспекти забезпечення конфіденційності персональних даних учасників кримінального судочинства. *Міхновські юридичні читання*. URL: https://nadpsu.edu.ua/nauka/naukovi-konferencziyi/#

4. Гриньків О.О., Ляш А.О. Заходи забезпечення безпеки у кримінальному судочинстві: [монографія]. Тернопіль: Астон, 2012. 260 с.

5. Ковмир С.В. Захист учасників кримінального судочинства: управлінські аспекти. *Науковий журнал Київський часопис права*. 2023. № 4. С. 132 – 138.

6. Ковмир С.В. Керування ризиками під час реалізації програм захисту учасників кримінального судочинства. *Юридичний вісник Law Herald*. 2023. № 4. С. 192–202. URL: http://yurvisnyk.in.ua/v4_2023/25.pdf

7. Вітлінський В.В., Наконечний С.І. Ризик у менеджменті. К.: ТОВ «Борисфен-М», 1996. 336 с.

8. Вітлінський В.В. Аналіз, оцінка і моделювання ризику. К.: ДЕМІУРГ, 1996. 212 с.

9. Вітлінський В. В. Аналіз ризиків. Київ: КНЕУ, 2002. 198 с.

10. Огляд новітніх технологій у сфері Інтернет-безпеки: як захистити дані. URL: https://homenet.online/oglyad-novitnih-tehnologiy-u-sferi-internet-bezpeki/

11. Дес Дерлоу. Ключові управлінські рішення. Технологія прийняття рішень. Київ: Всесвито, Наукова думка, 2001. 242 с.

12. Два обличчя штучного інтелекту: Generative AI vs Predictive AI. URL: https://careers.epam.ua/blog/generative-ai-vs-predictive-ai

13. Borum, Randy, Fein, Robert, Vossekuil, Bryan, and John Berglund. 1999. Threat assessment: defining an approach for evaluating risk of targeted violence. Behavioural Sciences and the Law, 17: C. 323 – 337.

14. Soni N. Evolution of Blockchain. 2020. URL: https://medium.com/@nehasoni1812/evolution-of-blockchain-f243f7509fe6#:~:text=Stefan%20Konst%20published%20his%20theory,linked%20together%20using%20cryptographic%20methods.

15. Conway L. Blockchain Explained. *Investopedia*. 2020. URL: https://www.investopedia.com/terms/b/blockchain.asp#:~:text=By%20spreading%20its%20operations%20across,the%20processing%20and%20transaction%20fees.

16. Clavin J., Duan S., Zhang H. Blockchains for Government: Use Cases and Challenges/ DGOV, 2020. URL: https://dl.acm.org/doi/fullHtml/10.1145/3427097.