УДК 343.3/.7:004(477)
DOI https://doi.org/10.32850/sulj.2023.3.10

НАЦІОНАЛЬНІ РЕАЛІЇ АНАЛІЗУ КІБЕРЗЛОЧИННОСТІ ЗА МЕТОДОЛОГІЄЮ ЄВРОПОЛУ IOCTA

Користін О. Є., Демедюк С. В., Панченко Є. В., Користін О. О.

У статті зосереджено увагу на концептуальних питаннях кібербезпеки в Україні. Наголошено як на глобальних трендах кіберзлочинності, так і на важливості врахування у цьому контексті воєнної агресії проти України й особливостях кіберзагроз, що активізуються і у зв'язку з війною.

Відзначено, що в умовах формування сучасних технологічних викликів, зокрема і в кіберпросторі, у суспільстві значно зросли вимоги щодо підвищення ефективності та результативності діяльності органів правопорядку, що передбачає, зокрема упровадження стратегічного менеджменту на основі розвитку сучасних методологій інформаційно-аналітичного забезпечення та осмислення реальних тенденцій в кримінальному середовищі. Акцентовано на тому, що розуміння реального стану та упровадження адекватної державної політики у сфері кібербезпеки потребує компетентного розвідувального аналітичного процесу, усвідомлення сучасних трендів й реального пізнання ключових кіберзагроз, а також розробки сучасної методології аналізу кіберзлочинності.

У статті висвітлено ключові підходи дослідницького проєкту щодо упровадження методології Європолу Оцінки загроз організованої злочинності в мережі Інтернет (Internet Organised Crime Threat Assessment – IOCTA), яку доповнено оцінюванням ризиків поширення кіберзагроз, спроможностей та вразливостей щодо протидії загрозам.

Увагу зосереджено на сучасному етапі правового регулювання у сфері кібербезпеки та вимогах аналітичного супроводження проблем кіберзлочинності з метою підвищення обізнаності та формування ефективної протидії на основі підвищення спроможності органів правопорядку. Враховуючи зазначені вимоги, спираючись на методологічні засади Європолу IOCTA, розширено перелік завдань, який передбачає: здійснення огляду національних та міжнародних нормативно-правових актів щодо забезпечення кібербезпеки; вивчення зарубіжного досвіду аналізу кіберзлочинності на прикладі методології Європолу IOCTA; ідентифікація загроз та оцінювання ризиків поширення кіберзлочинності в Україні; оцінювання спроможностей протидії кіберзлочинам та визначення вразливостей; аналіз тенденцій у сфері кіберзлочинності в Україні; побудова прогнозних моделей управління ризиками у сфері протидії кіберзлочинності.

Ключовим завданням у дослідженні обрано формування надійної експертної вибірки, на основі використання фільтрів логічної помилки, для забезпечення подальшого репрезентативного аналізу та висновків.

Ключові слова: *кібербезпека, кіберзлочинність, аналіз загроз, оцінка ризиків, IOCTA.*

Korystin O. Ye., Demediuk S. V., Panchenko Ye. V., Korystin O. O. National realities of cybercrime analysis according to Europol IOCTA methodology

The article focuses on conceptual issues of cyber security in Ukraine. Both the global trends of cybercrime and the importance of taking into account in this context the military aggression against Ukraine and the features of cyberthreats that are becoming more active due to the war are emphasized.

It was noted that in the conditions of the formation of modern technological challenges, in particular in cyberspace, the requirements for increasing the efficiency and effectiveness of the activities of law enforcement agencies have significantly increased in society, which includes, in particular, the introduction of strategic management based on the development of modern methodologies of information and analytical support and the understanding of real trends in criminal environment. It is emphasized that understanding the real situation and implementing an adequate state policy in the field of cyber security requires a competent intelligence analytical process, awareness of modern trends and real knowledge of key cyber threats, as well as the development of modern cybercrime analysis methodology.

The article highlights the key approaches of the research project on the implementation of Europol's Internet Organized Crime Threat Assessment (IOCTA) methodology, which is complemented by risk assessment of cyber threats, capabilities and vulnerabilities to counter threats.

Attention is focused on the current stage of legal regulation in the field of cyber security and the requirements for analytical monitoring of cybercrime problems with the aim of raising awareness and forming effective countermeasures based on increasing the capacity of law enforcement agencies. Taking into account the specified

requirements, based on the methodological principles of Europol IOCTA, the list of tasks has been expanded, which includes: conducting a review of national and international normative legal acts on ensuring cyber security; study of foreign experience in cybercrime analysis using the Europol IOCTA methodology as an example; identification of threats and risk assessment of the spread of cybercrime in Ukraine; assessment of cybercrime countermeasures and identification of vulnerabilities; analysis of trends in cybercrime in Ukraine; construction of predictive risk management models in the field of combating cybercrime.

The key task in the study was the formation of a reliable expert sample, based on the use of logical error filters, to ensure further representative analysis and conclusions.

***Key words:** cyber security, cyber crime, threat analysis, risk assessment, IOCTA.*

Постановка проблеми. Розвиток цифрових технологій формує новітні виклики глобальному світу та національним економікам, суттєво впливає на формування базових засад кібербезпеки. Сучасні національні інтереси пріоритетно зосереджуються на формуванні кіберстійкості країни, ключовими напрямами якої є захист критичної інфраструктури, зниження рівня кіберзлочинності, підвищення обізнаності та дотримання інтересів національної безпеки [1].

Тривала гібридна війна та широкомасштабна воєнна агресія рф особливо актуалізує проблеми кібербезпеки, що потребує об'єктивного розуміння її стану в Україні та реалізації відповідної державної політики, а також адекватної відповіді агресору. Саме тому «*Україна створить та забезпечить розвиток підрозділів із повноваженнями ведення збройного протиборства в кіберпросторі, … оцінку спроможностей та ефективності підрозділів, розроблення та імплементацію індикаторів оцінки їх діяльності*» [2].

Протидія кіберзлочинності сьогодні є невід'ємною частиною протиборства в кіберпросторі. Водночас, в умовах формування сучасних технологічних викликів, що сприяють поширенню новітніх загроз, зокрема і в кіберпросторі, у суспільстві значно зросли вимоги щодо підвищення ефективності та результативності діяльності органів правопорядку. Саме тому трендом правоохоронної діяльності сьогодні є упровадження стратегічного менеджменту на основі розвитку сучасних методологій інформаційно-аналітичного забезпечення та осмислення реальних тенденцій в кримінальному середовищі.

Метою статті є розвідки у сфері кібербезпеки з акцентуванням уваги на досліджені особливостей аналізу та напрацюванні системи знань щодо кіберзлочинності. Усвідомлення сучасних трендів та реального пізнання ключових кіберзагроз, на основі оцінювання ризиків їх поширення, оцінювання спроможностей та вразливостей щодо протидії кіберзагрозам, дасть можливість охарактеризувати напрями для формування реально дієвих механізмів ризик-орієнтованого підходу [3] щодо забезпечення кібербезпеки сучасного українського суспільства, що, у свою чергу, сформує достатній масив знань для формування обґрунтованих пропозицій щодо протидії кіберзлочинності.

В останні роки, у дослідженнях багатьох відомих вітчизняних дослідників, значна увага приділяється різним проблемам, пов'язаним з розробкою напрямів щодо кібербезпеки, зокрема протидії кіберзлочинності: Баранова О.А. [4], Бєлякова К.І. [5], Бірюкова Д.С., Бутузова В.М., Гнатюка С.О. [6], Горбуліна В., Довганя О.Д. [7], Дубова Д.В., Кормича Б.А., Корченка О.Г. [8], Лісовської Ю.П., Марущака А.І. [9], Пилипчука В.Г., Тихомирова О.О., Хахановського В.Г., Цимбалюка В.С., Швеця М.Я. та інших. Разом з тим, розуміння реального стану та упровадження адекватної державної політики у цій сфері потребує компетентного розвідувального аналітичного процесу, усвідомлення сучасних трендів й реального пізнання ключових кіберзагроз, а також розробки сучасної методології аналізу кіберзлочинності, яку сьогодні запропоновано Європолом під назвою «Оцінка загроз організованої злочинності в мережі Інтернет» (*Internet Organised Crime Threat Assessment – IOCTA*) (*далі IOCTA*) й на цій основі формування стратегії адекватної протидії. Важливе місце у цій системі займає оцінювання ризиків поширення кіберзагроз, оцінювання спроможностей та вразливостей щодо протидії загрозам, формуючи при цьому реально дієвий механізм ризик-орієнтованого підходу по забезпеченню кібербезпеки [10].

Виклад основного матеріалу. Небезпечні високотехнологічні загрози глобального характеру, що мають високий потенційний вплив та руйнівні наслідки для життєдіяльності будь-якого суспільства, є невід'ємним наслідком розвитку новітніх технологій. І охорона суспільних відносин, інтересів людини, суспільства та держави в сфері кіберпростору займає одне з пріоритетних місць в системі національної безпеки. Сучасний світ, враховуючи такі зміни намагається враховувати загальні тенденції та впроваджувати механізми забезпечення кібербезпеки [11].

Сучасні розвинені безпекові системи, зокрема й у сфері кібербезпеки, характеризуються

новаціями загальнонаукового та спеціального змісту, які створюють можливості передбачення із врахуванням взаємопов'язаних елементів, серед яких одним із основних інструментів є управління ризиками. Наразі, із врахуванням Резолюції генеральної асамблеї ООН та у межах розвитку глобальної культури кібербезпеки, упроваджуються механізми, серед яких одне з ключових місць займає ризик-орієнтований підхід – *учасники повинні здійснювати періодичну оцінку ризиків з метою виявлення загроз та факторів уразливості, мати належні технології та інструменти контролю для цього з урахуванням значущості інформації і її захисту* [12].

Тож, очевидно, реалізуючи державну політику із врахуванням міжнародних стандартів, Україна активно розвивається і в цьому напрямі. Зокрема, у Стратегії національної безпеки України, введеної в дію Указом Президента України від 14 вересня 2020 року № 392/2020 [13], зазначено, що Україна *запровадить національну систему стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на широкий спектр загроз, що передбачатиме оцінку ризиків, своєчасну ідентифікацію загроз і визначення вразливостей, а також поширення необхідних знань і навичок у цій сфері*. Про ризик-орієнтований підхід щодо забезпечення кібербезпеки зазначається і в Стратегії кібербезпеки України на період 2021–2025 років [14], а у Плані реалізації Стратегії кібербезпеки [15] (далі *План реалізації Стратегії*) чітко визначено завдання: «*Впровадити ризик-орієнтований підхід у частині заходів забезпечення кібербезпеки … розробити методики ідентифікації та оцінки кіберризиків …, забезпечити нормативне врегулювання питань щодо впровадження обов'язковості здійснення періодичної оцінки кіберризиків на підставі розроблених методик*».

Вочевидь, упровадження сучасних методологій потребує відповідного наукового супроводження, більше того, аналіз стратегічного характеру, що базується на емпіричній базі, сформованій широкою експертною думкою, реалізується безпосередньо в межах не лише кримінології, а й соціології, статистики та науки про дані (*Data Science*), що вимагає дотримання методологічних вимог. Саме тому, на нашу думку, є усі підстави стверджувати, що такі завдання вирішуються переважно в межах прикладного наукового дослідження, із врахуванням дослідницького досвіду та напрацюванням відповідної методології й інструментарію обробки та аналізу великих даних (Big Data).

Науковці ДНДІ МВС України вже не один рік використовують ризик-орієнтований підхід щодо аналізу проблем у сфері безпеки [16, 17, 18, 19]. Водночас, у 2021 році у складі експертної групи РНБО України реалізовано проєкт, предметом якого був стратегічний аналіз у сфері кібербезпеки в Україні [20]. Науковий інтерес завжди викликають зарубіжні новації, упровадження яких в Україні є не лише можливим, а й необхідним процесом. Зокрема, фахівці з кібербезпеки, особливо у сфері правоохоронної діяльності, неодноразово висказувалися щодо методології Європолу IOCTA, яка є головним стратегічним продуктом Європолу, що забезпечує орієнтовану на правоохоронні органи оцінку нових загроз і ключових подій у сфері кіберзлочинності. В аналітичних висновках, окрім загальних характеристик кіберзлочинів, висвітлюються тенденції щодо її поширення, нові форми та напрями, про що свідчать кібератаки. Також зазначається про зростаюче зближення кіберпростору та організованої злочинності тощо.

У передмові доповіді IOCTA-2021 виконавчий директор Європолу Кетрін де Болле (Catherine De Bolle) зазначила, що «*життєво важливо продовжувати вдосконалювати нашу колективну інформаційно-технологічну (IT) грамотність та обізнаність, оскільки кіберзлочинність укорінилася в нашому суспільстві*» [21]. Саме тому, розвиваючи науковий пошук та у співпраці з Департаментом кіберполіції НПУ, було започатковано науково-дослідну роботу за темою «Аналіз кіберзлочинності в Україні з використанням методології Європолу IOCTA».

Наразі, завдання, які було визначено такою співпрацею, повністю корелюються не тільки з відомчими програмами. Планом реалізації Стратегії в п. 20 визначено: «*Розробити методику проведення щорічних соціологічних досліджень щодо кіберзагроз, … з оцінками ефективності діяльності державних органів у протидії їм і забезпечити проведення таких досліджень*». Тобто вітчизняні реалії та чинні правові норми вже сьогодні вказують на більш широку постановку завдань. Також, у пункті 7 Плану реалізації Стратегії зазначається: «*Забезпечити оцінку спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони …*», а, визначаючи ціль щодо ефективної протидії кіберзлочинності, закріплено «*Україна забезпечить набуття правоохоронними органами … спроможностей для мінімізації загроз кіберзлочинності, посилення їх технологічного*

і кадрового потенціалу для проведення превентивних заходів та розслідування кіберзлочинів» і з цією метою необхідно *«Запровадити скоординоване виявлення та розкриття вразливостей інформаційно-комунікаційних систем»*.

Враховуючи зазначені вимоги, спираючись на методологічні засади Європолу IOCTA, було розширено перелік завдань, який передбачає:

здійснення огляду національних та міжнародних нормативно-правових актів щодо забезпечення кібербезпеки;

вивчення зарубіжного досвіду аналізу кіберзлочинності на прикладі методології Європолу «Internet Organised Crime Threat Assessment» (IOCTA);

ідентифікація загроз та оцінювання ризиків поширення кіберзлочинності в Україні;

оцінювання спроможностей протидії кіберзлочинам та визначення вразливостей;

аналіз тенденцій у сфері кіберзлочинності в Україні;

побудова прогнозних моделей управління ризиками у сфері протидії кіберзлочинності.

Для проведення дослідження обрано ризик-орієнтований підхід у якості базового, який, на нашу думку, став основою для дослідження за обраним напрямом. Базовими засадами для реалізації визначених завдань оцінювання ризиків є міжнародний стандарт, імплементований до вітчизняного законодавства, так як у 2018 році прийнятий як національний стандарт, – ДСТУ ISO 31000:2018 [22].

Експертною групою, що була сформована з представників кіберполіції та науковців ДНДІ, опрацьовано опитувальник Європолу щодо IOCTA та додатково визначено індикатори більш широкого спектру, забезпечуючи виконання визначених дослідницьких завдань. Під час проведення стратегічних сесій використовувались методи фасилітації та мозкового штурму на предмет ідентифікації загроз у сфері кібербезпеки, вразливостей системи кібербезпеки та спроможностей кіберполіції. На цій основі розроблено відповідний опитувальник, відповіді на запитання якого були конфіденційними і не потребували розкриття особистих даних експертів. Опитування проводилось в режимі ON-LINE шляхом заповнення анкет, в яких кожен індикатор оцінювався за двома характеристиками: «Ймовірність (Рівень оцінювання)» та «Можливі наслідки (Вплив)» за 3-4-5-бальною шкалою. При оцінюванні важливим вбачалося відображення специфіки регіону мешкання, власного досвіду та обізнаності респондентів щодо сфери кібербезпеки України.

Водночас, враховуючи значний обсяг опитувальника (1025 індикаторів), напруженість при його осмисленні та заповненні, а також припускаючи можливість помилкових тверджень респондентів, було запроваджено фільтри логічної помилки у різних розділах опитувальника, що забезпечило певну надійність даних для подальшого аналізу.

Важливим є зазначити про те, що IOCTA використовує широкий спектр інформаційних джерел, серед яких важливе місце займає саме експертна думка, а не лише матеріали кримінальних проваджень, які потенційно обмежують перспективи аналітичних висновків. А тому сформований

Рис. 1. Джерела інформації за надійною експертною вибіркою

масив надійних даних забезпечено використанням наступних джерел (Рис. 1): кримінальні провадження – 86,3 %; оперативно-розшукові справи – 3,4 %; довідково-аналітичні матеріали – 10,3 %.

За категорією посад експертів, які взяли участь в опитуванні та пройшли фільтри надійності, дані наступні (Табл. 1):

Зазначена експертна вибірка забезпечила формування базової сукупності даних, отриманих від лише тих експертів, які надавали логічно узгоджені відповіді. Незважаючи на те, що після фільтрування даних залишилося 45,81 % початкової вибірки, якість результатів суттєво зросла. Це можна бачити на прикладі оцінювання індикаторів за експертними вибірками щодо надійності (Табл. 2).

Порівнюючи розподіл оцінювання за групами експертів, що були відібрані за фільтром відсутності логічних помилок, у порівнянні з тими, хто цей фільтр не пройшов, можна бачити, різниця в розподілах є значною, зокрема:

щодо активності в Даркнет по відмиванню коштів – 60,3 % ненадійних експертів вказали на таку ймовірність, в той час як надійні обрали цей варіант лише у 38,9 % випадків. Ця різниця є не тільки статистично значущою (критерій $x^2 = 29.314$, $p < 0.000$), але й величина ефекту є дуже значною (V Крамера = 0.214, $p < 0.000$), а результати, за своєю суттю, були прямо протилежні.

щодо технологічної відсталості України в сучасних ІКТ – 10,4 % ненадійних експертів вказали на низький рівень, в той час як надійні обрали цей варіант у 15,5 % випадків. Варіант «дуже високий» був обраний ними лише у 8,3 % випадків. Ця різниця є не тільки статистично значущою (критерій $x^2 = 30.118$, $p < 0.000$), але й величина ефекту є дуже значною (V Крамера = 0.217, $p < 0.000$). Аналогічні тенденції спостерігаються і по інших важливих питаннях анкети.

Таким чином, обмеження вибірки на основі перевірки на логічну помилку є статистично значущим та забезпечує надійність експертної вибірки для подальшого репрезентативного аналізу.

Висновки. Таким чином, використовуючи методологію Європолу IOCTA та застосовуючи ризик-орієнтований підхід, започатковано упровадження сучасних підходів стратегічного аналізу у сфері протидії кіберзлочинності. Достатньо показовими є використані у дослідженні матеріали опитування експертів, а також проведена вибірка на основі логічної помилки, що дозволило підійти до наступного усвідомлення сучасних трендів та реального пізнання ключових кіберзагроз, оцінювання ризиків їх поширення, оцінювання спроможностей та вразливостей щодо протидії кіберзагрозам. Проведений у статті аналіз є лише початковим етапом спільного дослідницького проєкту

Таблиця 1

Категорії посад респондентів

Категорія посади	Відсоток у загальній кількості надійної вибірки
оперативний працівник	17.7
керівник оперативного підрозділу	4.6
аналітик	1.4
керівник аналітичного підрозділу	0.3
інспектор (старший інспектор)	76.0

Таблиця 2

Аналіз за фільтром логічної помилки

НАЗВА ІНДИКАТОРА	ОЦІНКА	Вибірка		Статистична значущість	Pearson Chi-Square	Cramer's V
		Ненадійна частина	Надійна частина			
11.7. Активність в Даркнет: відмивання коштів	*так*	60,3%	38,9%	0,000	29.314	.214
	ні	39,7%	61,1%	0,000		
1.1. Технологічна відсталість в Україні щодо сучасних ІКТ (рівень)	*нульовий*	7.3%	3.4%	0,000	30.118	.217
	низький	10.4%	15.5%	0,000		
	середній	43.1%	58.7%	0,000		
	високий	25.0%	14.0%	0,000		
	дуже високий	14.2%	8.3%	0,000		

кіберполіції та науковців, який закладає суттєву методологічну базу сучасного стратегічного менеджменту в правоохоронній діяльності та потребує більш глибокого подальшого дослідження усього масиву даних, застосування сучасних методів та інструментів аналізу щодо визначення пріоритетів та побудови прогнозних моделей.

Література

1. Roger Hurwitz. Keeping Cool: Steps for Avoiding Conflict and Escalation in Cyberspace. *Georgetown Journal of International Affairs*: Georgetown University. 2014.

2. Про План реалізації Стратегії кібербезпеки України: Рішення Ради національної безпеки і оборони України від 30 грудня 2021 року. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text

3. Користін О.Є., Свиридюк Н.П. Методологічні засади оцінювання ризиків в правоохоронній діяльності. *Наука і правоохоронна*. № 3. 2020. С. 191-197.

4. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи. Київ: Видавничий дім «СофтПрес», 2005. 316 с.

5. Бєляков К.І. Інформація в праві: теорія і практика: монографія. Київ: Видавництво "КВІЦ", 2006. 116 с.

6. Гнатюк С.О. Методологія формування та забезпечення державної системи кібербезпеки в галузі цивільної авіаціїю. *Актуальні питання забезпечення кібербезпеки та захисту інформації*: тези доп. III міжнар. наук.-практ. конф., 22-25 лютого 2017 р. Київ, 2017. С. 65-67.

7. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. Київ: Видавничий дім «АртЕк», 2017. 107 с.

8. Корченко О., Казмірчук С., Ахметов Б. Прикладні системи оцінювання ризиків інформаційної безпеки: монографія, Київ: ЦП Компринт, 2017. 435 с.

9. Марущак А.І. Інформаційні ресурси держави: зміст та проблема захисту. *Правова інформатика*. 2009. № 1(21). С. 65-71.

10. Користін О.Є., Веселова Л.Ю. Ризикорієнтованість кібербезпеки. *Наука і правоохоронна*. 2021. № 3. С. 16–23.

11. Директива Європейського Парламенту І Ради (ЄС) 2016/1148 від 6 липн. 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_013-16/find?text=%F0%E8%E7%E8%EA (дата звернення: 11.08.2023)

12. Резолюція Генеральної Асамблеї ООН 57/329, ухвалена на 78 пленарному засіданні 57-ї сесії. 20 грудня 2002 року. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement (дата звернення: 11.08.2023)

13. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України"»: Указ Президента України від 14 вересня 2020 року № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 11.08.2023)

14. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013(дата звернення: 11.08.2023)

15. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про План реалізації Стратегії кібербезпеки України"»: Указ Президента України від 01 лютого 2022 року № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/37/2022#Text (дата звернення: 11.08.2023)

16. Kovalchuk T.I., Korystin O. Y., Sviridyuk N. P. Hybrid threats in the civil security sector in Ukraine. *Problems of Legality*. 2019. № 147. 163–175. DOI: https://doi.org/10.21564/2414-990x.147.180550

17. Oleksandr Korystin, Nataliia Svyrydiuk, Volodymyr Tkachenko. Fiscal Security of the State Considering Threats of Macroeconomic Nature. *Proceedings of the International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research* (BAMBEL2021). Series: Advances in Economics, Business and Management Research. 27 August 2021. Vol. 188. Pp. 65-69. DOI: 10.2991/AEBMR.K.210826.012

18. Користін О.Є., Цюприк І.В., Свиридюк Н.П., Прокоф'єфа-Янчиленко Д.М. Оцінювання ризиків розвитку системи кримінальної юстиції України. *Наука і правоохорона*. 2021. № 2. С. 108-116. DOI: https://doi.org/10.36486/np.2021.2(52)

19. Користін О.Є., Свиридюк Н.П. Оцінювання загроз у сфері лісового господарства України. *Наука і правоохорона*. 2023. № 1. С. 145-153. DOI (Issue): https: //doi.org/10.36486/np.2023.1(59)

20. Користін О.Є., Користін О.О. Загрози у сфері кібербезпеки в Україні. *Наука і правоохоронна*. 2022. № 1 (55). С. 119-126. DOI: https: //doi.org/10.36486/np.2022.1(55)

21. Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021. Publications Office of the European Union. Luxembourg. 2021.

22. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT). URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_31000_2018.pdf (дата звернення: 11.08.2023)

Демедюк С. В.,
кандидат юридичних наук,
заступник Секретаря Ради національної
безпеки і оборони України

Панченко Є. В.,
начальник 4-го управління
(оперативно-аналітичного
забезпечення та аналізу відкритих джерел)
Департаменту кіберполіції
Національної поліції України

Користін О. Є.,
доктор юридичних наук, професор,
заслужений діяч науки і техніки України,
головний науковий співробітник НДЛ
кримінологічних досліджень
Державного науково-дослідного інституту
Міністерства внутрішніх справ України

Користін О. О.,
магістрант
Національного авіаційного університету