DOI (Issue): https: //doi.org/10.36486/np.2022.1(55) Issue 1(55) 2022

УДК 004.056

Користін Олександр Євгенійович,
доктор юридичних наук, професор, заслужений діяч
науки і техніки України, головний науковий співробітник
ДНДІ МВС України, м. Київ, Україна
ORCID ID 0000-0001-9056-5475
Користін Олександр Олександрович,
студент IV курсу, Національний авіаційний університет, м. Київ, Україна

ЗАГРОЗИ У СФЕРІ КІБЕРБЕЗПЕКИ В УКРАЇНІ

У статті зосереджується увага на дослідженні загроз у сфері кібербезпеки в Україні. Дослідження проводилось на основі отриманих емпіричних даних – результатів анкетування фахівців НСКБ щодо ідентифікації та оцінювання ймовірності й впливу загроз у сфері кібербезпеки. Обґрунтовується достовірність отриманої експертної вибірки.

На основі оцінювання ризиків здійснено рейтингування загроз у сфері кібербезпеки в Україні. Особливий акцент зроблено на найзначніших загрозах у сфері кібербезпеки, які потребують невідкладного реагування та формування відповідної державної політики протидії та зниження ризику їх прояву.

***Ключові слова**: кібербезпека, загроза, ризик, ризик-орієнтований підхід, ідентифікація, експертне середовище.*

Питання протидії загрозам у сфері кібербезпеки займає провідне місце у системі національної безпеки України. Особливої актуальності проблема кібербезпеки набула за сучасних обставин, що повністю формується під впливом тривалої гібридної війни та відкритого воєнного вторгнення РФ на територію нашої держави. Такий стан національної безпеки потребує адекватного підходу до вирішення проблем безпеки, зокрема і щодо об'єктивного розуміння стану кібербезпеки в Україні та реалізації відповідної державної політики, спрямованої на ефективну протидію загрозам у сфері кібербезпеки.

Метою цієї статті є дослідження проблематики загроз у сфері кібербезпеки, особливостей їх ідентифікації та рейтингування з акцентом на визначенні найзначніших, що потребують невідкладної уваги.

Останніми роками у багатьох наукових роботах значна увага приділяється різним проблемам протидії кіберзагрозам в Україні. Зокрема питання, пов'язані з розробкою напрямів щодо протидії кіберзагрозам, ставали предметом досліджень багатьох відомих учених: Баранова О.А. [1], Бєлякова К.І. [2], Бірюкова Д.С., Бутузова В.М., Гнатюка С.О. [3], Горбуліна В., Довганя О.Д. [4], Дубова Д.В., Кормича Б.А., Корченка О.Г. [5], Лісовської Ю.П., Марущака А.І. [6], Пилипчука В.Г., Тихомирова О.О., Хахановського В.Г., Цимбалюка В.С., Швеця М.Я. та інших. Водночас розуміння реального стану та упровадження адекватної державної політики у цій сфері потребує постійного аналітичного процесу, усвідомлення

DOI (Article): https: //doi.org/10.36486/np.2022.1(55).12

сучасних трендів та реального пізнання ключових кіберзагроз та напрямів й інструментів розбудови НСКБ.

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 [7].

Розвиток нових технологій в інформаційній сфері, кіберпросторі, разом із розвитком соціальних комунікацій у сіспільстві, несе надзвичайно небезпечні загрози високотехнологічного та глобального характеру. Вирішення комплексних та багатоманітних проблем кібербезпеки, пов'язаних із інформаційними мережами та відкритими системами, може бути відносно складним, а потенційні наслідки та вплив на діяльність суб'єкта та країни можуть бути руйнівним. Фактори, що є ключовими для суспільного успіху, можуть залежати від здатності забезпечувати безпеку інформації, процесів, систем та інфраструктури у кіберпросторі.

Сучасний світ, зважаючи на такі зміни, намагається враховувати загальні тенденції та впроваджувати механізми забезпечення кібербезпеки [8]. Охорона суспільних відносин, інтересів людини, суспільства та держави в сфері кіберпростору є пріоритетним питанням системи національної безпеки. Країни світу демонструють спільну позицію щодо кібербезпеки та стандартів захисту прав людини в кіберпросторі, яка є динамічною і розвивається на основі переосмислення підходів.

Сучасні світові погляди щодо протидії загрозам у сфері кібербезпеки мають різноманітні засади формування. Зокрема, змістовними та новаційними є ініціативи, пов'язані з протидією гібридним загрозам, серед яких кіберзагрози – ключові. Глобальна культура кібербезпеки передбачає врахування взаємопов'язаних елементів, серед яких виділяється й оцінка ризиків – учасники мають 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 [9].

Україна активно розвивається і в цьому напрямі. Зокрема, у Стратегії національної безпеки України, уведеної в дію Указом Президента України від 14 вересня 2020 року № 392/2020 [10], 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 до забезпечення кібербезпеки зазначається і в Стратегії кібербезпеки України на період 2021–2025 років [11, 12, 13].

Саме таке завдання було визначено групою експертів РНБО України, до складу якої увійшли представники суб'єктів НСКБ та профільних закладів вищої освіти, яка під час проведення стратегічних сесій, активно впроваджуючи методи фасилітації й мозкового штурму на предмет ідентифікації загроз у сфері кібербезпеки, методологічною базою для проведення подальшого дослідження обрала саме ризик-орієнтований підхід у якості базового. На нашу думку, такий

DOI (Article): https: //doi.org/10.36486/np.2022.1(55).12

інструмент став початком для досліджень за напрямом і основою для оцінки кіберзагроз та подальшого стратегічного планування у зазначеній сфері.

З цією метою було розроблено відповідний опитувальник (рис. 1).

№ З/П	**КІБЕРЗАГРОЗИ** - *наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.*	ЙМОВІРНІСТЬ			МОЖЛИВІ НАСЛІДКИ			
		висока	середня	низька	катастрофа	критичний стан	тяжкий стан	незначні наслідки
1.	**Кібератаки** - спрямовані (навмисні) дії в кіберпросторі проти суб'єктів та/або об'єктів в Україні							
	за секторами поширення (можливим є вибір одного або декількох секторів одночасно):	X	X	X	X	X	X	X
1.1	*індивідуальний (громадяни)*							
1.2.	*багатогалузевий характер поширення*							
1.3.	*управління (адміністрування)*							
1.4.	*економіка*							
1.5.	*фінанси / банки / страхування*							
1.6.	*інфраструктура*							
1.7.	*виробництво*							
1.8.	*оборона*							
1.9.	*безпека*							
1.10.	*охорона здоров'я / медицина*							
1.11.	*освіта*							
1.12.	*інформація та комунікації*							
1.13.	*професійний / цифрові послуги*							
1.14.	*соціальні послуги*							
1.15.	*культура, розваги та ігри.*							
2.	**Шкідливе програмне забезпечення** (Malware)							
2.1.	Вірус ("virus")							
2.1.1.	*Хробак ("worm")*							

Рис. 1. Анкета щодо експертного опитування на предмет гібридних загроз у секторі цивільної безпеки

Опитування проводилось онлайн, шляхом заповнення анкет із дотриманням режиму конфіденційності та без розкриття індивідуальних даних опитуваних. Зазначене експертне оцінювання відображає власний досвід респондентів та обізнаність щодо визначеного предмета опитування. Упроваджена вибірка забезпечила одержання 798 анкет. Загальна сукупність даних, окрім іншого, передбачає також виділення окремих груп респондентів за ознаками належності до суб'єкта, сфери суспільних відносин, віку, статі тощо. Кожен індикатор оцінювався за двома характеристиками: "Ймовірність (Рівень оцінювання)" та "Можливі наслідки (Вплив)" за 3–4–5-бальною шкалою.

Передбачалося, що через значний обсяг анкети, складність питань і короткий час їх осмислення експерти могли припускатися помилки у відповідях. Тому для подальшого дослідження необхідним вбачалося обмеження вибірки найбільш якісними та надійними даними, тобто перевірити респондентів на предмет їх логічної помилки. З цією метою при розробленні анкети у різні розділи були внесені запитання, логічно обґрунтованою відповіддю на які було їх оцінювання

DOI (Issue): https: //doi.org/10.36486/np.2022.1(55) Issue 1(55) 2022

у характеристиці *"ймовірність"* як *"висока" або "середня"*, але не *"низька"* в умовах війни. Наприклад, *"Кібератаки як елемент гібридної війни"* тощо.

Таким чином, у базовій сукупності подальшого аналізу залишилось 508 анкет лише тих експертів, які надавали логічно узгоджені відповіді, що становить 63,66 %. Незважаючи на те, що після фільтрування даних залишилося 63,66 % початкової вибірки, *якість результатів суттєво зросла*. Це можна бачити на прикладі оцінювання індикатора під питанням 1.8 "Кібератаки у сфері оборони" (Розділ 1 "Загрози") та розподілу у групі тих, хто був відібраний за фільтром відсутності логічних помилок, у порівнянні з тими, хто цей фільтр не пройшов (*табл. 1*).

Як можна побачити, різниця в розподілах є кричущою: 34,4 % ненадійних експертів указали на низьку ймовірність прояву загрози, тоді як надійні обрали цей варіант лише у 8,0 % випадків. Варіант "висока ймовірність" був обраний ними у 64,1 % випадків. Ця різниця є не тільки статистично значущою (критерій $\chi^2 = 25.102$, $p < 0.000$), а й величина ефекту є дуже значною (V Крамера = 0.298, $p < 0.000$). Аналогічні тенденції спостерігаються і за іншими важливими питаннями анкети.

Таким чином, обмеження вибірки на основі перевірки логічної помилки є статистично значущим, надійним та репрезентативним.

Таблиця 1

Аналіз за фільтром логічної помилки

		Вибірка		Разом
		Ненадійна частина	Надійна частина	
1.8. Кібератаки у сфері оборони	низька	34,4 %	8,0 %	11,0 %
	середня	37,5 %	27,9 %	29,0 %
	висока	28,1 %	64,1 %	60,1 %
Разом		100,0 %	100,0 %	100,0 %

Відповідно до попереднього аналізу, проведеного експертною групою РНБО, ідентифіковано 83 загрози у сфері кібербезпеки, а, враховуючи оцінювання експертним середовищем, базова вибірка сформувала можливості для визначення на основі ризику поширення рейтингу кожної з ідентифікованих кіберзагроз (рис. 2).

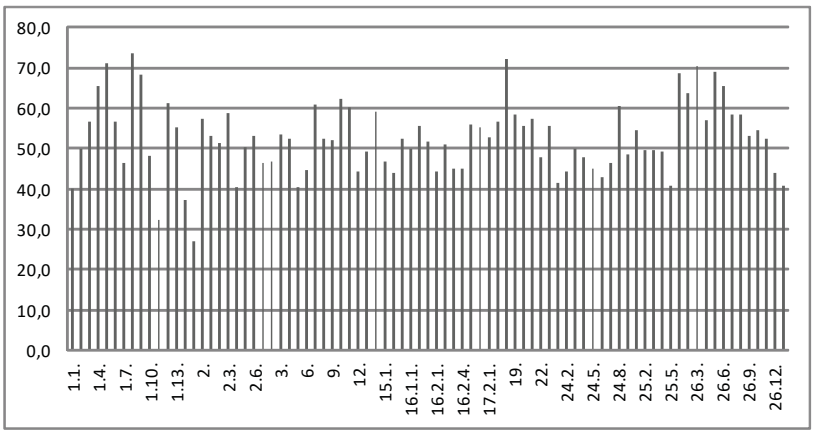

Рис. 2. Загальний рейтинг загроз у сфері кібербезпеки, (%)

DOI (Article): https: //doi.org/10.36486/np.2022.1(55).12

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 [14].

Загальна картина оцінювання ризику поширення ідентифікованих загроз достатньо варіативна, що сприймається також як рівень достатності щодо репрезентативності результатів.

Реалізована методологія передбачає оцінювання ризиків поширення загроз за шкалою від 0 % до 100 % та передбачає такі граничні рівні:

– рівень ризику у зоні вище 60 % – найзначніші загрози (потребують застосування невідкладних заходів щодо зменшення ризику їх поширення);

– рівень ризику у зоні 50–60 % – значні загрози (потребують контролю найвищого керівництва);

– рівень ризику у зоні 40–50 % – загрози, що потребують уваги, але не першорядні;

– рівень ризику у зоні нижче 40 % – незначний рівень.

Таким чином, до найзначніших загроз у сфері кібербезпеки в Україні належить 15 ідентифікованих загроз:

– кібератаки у сфері оборони – 73,76 %;
– кібератаки як елемент гібридної війни проти України – 72,22 %;
– кібератаки у сферах: фінанси / банки / страхування – 70,97 %;
– кібератаки у сфері безпеки – 68,45 %;
– кібератаки у сфері економіки – 65,36 %;
– витік інформації (Information leakage) – 62,33 %;
– кібератаки у сферах інформація та комунікацій – 61,28;
– злом (порушення) даних (Data breaches) – 60,73 %;
– кіберзагрози, пов'язані із упровадженням новітніх технологій: поширення кіберзлочинності – 60,52 %;
– крадіжка особистих даних (Identity theft) – 60,06 %.

Згідно із рекомендаціями ризик-менеджменту, зазначені загрози потребують застосування невідкладних заходів щодо зменшення ризику їх поширення. Друга група – значні загрози, що потребують контролю найвищого керівництва, характеризується 33 індикаторами кіберзагроз.

Проведений аналіз загроз у сфері кібербезпеки не є остаточним та потребує більш глибокого дослідження з використанням більш широкого масиву даних та інформації, застосування сучасних методів та інструментів аналізу. Водночас достатньо показовими є використані у дослідженні статистичні дані та матеріали опитування експертів НСКБ, що дозволило ідентифікувати загрози у сфері кібербезпеки та на основі оцінювання експертним середовищем здійснити їх рейтингування за рівнем ризику, визначивши найважливіші, що потребують невідкладного впровадження заходів щодо зниження ризику їх поширення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Баранов О.А.* Інформаційне право України: стан, проблеми, перспективи. Київ: Видавничий дім "СофтПрес", 2005. 316 с.

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

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

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

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

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

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

8. Директива Європейського Парламенту І Ради (ЄС) 2016/1148 від 6 липня 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

9. Резолюция Генеральной Ассамблеи ООН 57/329, принятая на 78 пленарном заседании 57-й сессии. 20 декабря 2002 года. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement (дата звернення: 06.04.2022).

10. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України". URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 06.04.2022).

11. Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny: Zakon Ukrayiny № 720-IX vid 17.06.2020, VVR, 2020, № 47, st. 408. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 06.04.2022).

12. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про План реалізації Стратегії кібербезпеки України". URL: https://zakon.rada.gov.ua/laws/show/37/2022#Text (дата звернення: 06.04.2022).

13. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні. Матеріал для обговорення. URL: https://parlament.org.ua/wp-content/uploads/2017/12/au_White-book-on-cybersecurity-draft_5.pdf (дата звернення: 06.04.2022).

14. 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: 06.04.2022).

REFERENCES

1. *Baranov O.A.* (2005) Informatsiine pravo Ukrainy: stan, problemy, perspektyvy. "Information law of Ukraine: state, problems, prospects". Kyiv: Vydavnychyi dim "SoftPres", 316 p. [in Ukrainian].

2. *Bieliakov K.I.* (2006). Informatsiia v pravi: teoriia i praktyka. "Information in law: theory and practice": monograph. Kyiv: Publ. "KVITS", 116 p. [in Ukrainian].

3. *Hnatiuk S.O.* (2017) Metodolohiia formuvannia ta zabezpechennia derzhavnoi systemy kiberbezpeky v haluzi tsyvilnoi aviatsiiu. Aktualni pytannia zabezpechennia kiberbezpeky ta zakhystu informatsii. "Methodology of formation and maintenance of the state cybersecurity system in the field of civil aviation. Current issues of cybersecurity and information protection": thesis add. III International scientific-practical Conf., February 22–25, 2017. Kyiv. P. 65–67 [in Ukrainian].

4. *Dovhan O.D., Doronin I.M.* (2017) Eskalatsiia kiberzahroz natsionalnym interesam Ukrainy ta pravovi aspekty kiberzakhystu. "Escalation of cyber threats to the national interests of Ukraine and legal aspects of cyber defense: monograph". Kyiv: ArtEk Publishing House. 107 p. [in Ukrainian].

5. *Korchenko O., Kazmirchu S., Akhmetov B.* (2017) Prykladni systemy otsinyuvannya ryzykiv informatsiynoyi bezpeky. "Applied systems for assessing the risks of information security: a monograph". Kyiv: CP Comprint. 435 p. [in Ukrainian].

6. *Marushchak A.I.* (2009) Informatsiini resursy derzhavy: zmist ta problema zakhystu. "State information resources: content and problem of protection". Legal informatics. No. 1 (21). P. 65–71 [in Ukrainian].

7. *Korystin O.Ye., Veselova L.Yu.* (2021) Ryzykoriyentovanist kiberbezpeky. "Cybersecurity risk orientation". Nauka i Pravookhorona. No. 3. P. 16–23 [Ii Ukrainian].

8. Dyrektyva Yevropeiskoho Parlamentu i Rady (YES) 2016/1148 vid 6 lypn. 2016 roku pro zakhody dlia vysokoho spilnoho rivnyia bezpeky merezhevykh ta informatsiynykh system na terytorii Soiuzu. "Directive of the European Parliament and of the Council (EU) 2016/1148 of 6 July 2016 on measures for a high common level of security of network and information systems in the Union". URL: https://zakon.rada.gov.ua/laws/show/984_013-16/find?text=%F0%E8%E7%E8%EA (Date of Application: 06.04.2022) [in Ukrainian].

9. Rezoliutsiia Heneralnoi Assamblei OON 57/329, pryniataia na 78 plenarnom zasedanii 57-y sessii. "UN General Assembly resolution 57/329, adopted at the 78th plenary session of the 57th session". December 20, 2002. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement (Date of Application: 06.04.2022) [in Russian].

10. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku "Pro Stratehiiu natsionalnoi bezpeky Ukrainy". "On the decision of the National Security and Defense Council of Ukraine of September 14, 2020 "On the National Security Strategy of Ukraine"". URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (Date of Application: 06.04.2022) [in Ukrainian].

11. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy № 720-IX vid 17.06.2020, VVR, 2020, № 47, st. 408. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (Date of Application: 06.04.2022) [in Ukrainian].

12. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 30 hrudnia 2021 roku "Pro Plan realizatsii Stratehii kiberbezpeky Ukrainy". "On the decision of the National Security and Defense Council of Ukraine of December 30, 2021 "On the Implementation Plan of the Cyber Security Strategy of Ukraine"". URL: https://zakon.rada.gov.ua/laws/show/37/2022#Text (Date of Application: 06.04.2022) [in Ukrainian].

13. Propozytsii do polityky shchodo reformuvannyia sfery kiberbezpeky v Ukraini. "Proposals for policy on cybersecurity reform in Ukraine". Material for discussion. URL: https://parlament.org.ua/wp-content/uploads/2017/12/au_White-book-on-cybersecurity-draft_5.pdf (Date of Application: 06.04.2022) [in Ukrainian].

14. DSTU ISO 31000:2018 Menedzhment ryzykiv. Pryntsypy ta nastanovy. "DSTU ISO 31000: 2018 Risk management. Principles and guidelines (ISO 31000: 2018, IDT)". URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_31000_2018.pdf (Date of Application: 06.04.2022) [in Ukrainian].

UDC 004.056

Korystin Oleksandr Ye.,
Doctor of Juridical Sciences, Professor, Honored Academic of Science and Technology of Ukraine, Chief Researcher, State Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID 0000-0001-9056-5475
Korystin Oleksandr O.,
4th year student of the National Aviation University, Kyiv, Ukraine

CYBERSECURITY THREATS IN UKRAINE

The article focuses on the study of cybersecurity threats in Ukraine. The research carried out on the basis of obtained empirical data – the results of the survey of NSCB experts on the identification and assessment of the probability and impact of threats in the sphere of cybersecurity. Reliability of the obtained expert sample is substantiated by using a logical error filter.

DOI (Article): https: //doi.org/10.36486/np.2022.1(55).12

This article substantiates the importance of a risk-based approach to cybersecurity. Authors draw attention to adequate changes in Ukraine of risk-oriented approach development. Basing on risk assessment the rating of cybersecurity threats in Ukraine was carried out. Particular emphasis is placed on the most significant threats in the sphere of cybersecurity, requiring an urgent response and the formation of appropriate state policy to counteract and reduce the risk of their occurrence, in particular: cyber attacks in defense – 73.76 %; cyber attacks as an element of hybrid war against Ukraine – 72.22 %; cyber attacks in the areas: finance / banking / insurance – 70.97 %; cyber attacks in security – 68.45 %; cyber attacks in the economy – 65.36 %.

With these matters cleared away, there is a high level of risk of cybercrime – 60.52 % – due to the introduction of the latest technology. Among different subjects of encroachment, first of all, the highest level of risk concerns state security bodies – 70.52 %; institutions of defense-industrial complex – 69.03 %; state bodies – 68.76 %; objects of critical information infrastructure – 65.40 %; law enforcement bodies – 63.64 %.

Keywords: cybersecurity, threat, risk, risk-based approach, identification, expert environment.

Отримано 11.04.2022