Ефективність державного управління
Efficiency of public administration
ISSN 2070-4011 (print)
ISSN 2786-6580 (online)
https://doi.org/10.36930/507611
Article received 25.11.2023
Article accepted 17.12.2023
УДК 358:343.37
Correspondence author: D. O. Grycyshen, grytsyshen-do@ztu.edu.ua

Д. О. Грицишен, А. П. Дикий, В. М. Бутузов, В.С. Цимбалюк
Державний університет "Житомирська політехніка", м. Житомир, Україна

МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАПОБІГАННЯ ТА ПРОТИДІЇ ЕКОНОМІЧНІЙ ЗЛОЧИННОСТІ

Визначено поняття кіберпростір, кібербезпека, кіберзлочини. Здійснено статистичний аналіз кількості правопорушень та досліджено динаміку вчинених злочинів у сфері використання комп'ютерів та комп'ютерних мереж за період з 2013 по 2022 рр. Наведено інформацію щодо основних секторів хакерських атак та визначено перелік найпоширеніших методів кібератак. Визначено суб'єкти та об'єкти інформаційного захисту державної політики і перелік принципів, якими повинна керуватись система інформаційного захисту, описано етапи формування механізму забезпечення інформаційної безпеки та необхідні види забезпечення (фінансові, інформаційні, правові, кадрові). Зазначені етапи включають оцінення кібербезпеки, встановлення вимог до технологій, впровадження заходів забезпечення інформаційної безпеки та системи моніторингу за кібербезпекою. Запропоновано перелік складових механізму забезпечення інформаційної безпеки, серед яких: 1) забезпечення системи захисту інформації на усіх етапах реалізації державної політики; 2) інформаційна гігієна; 3) впровадження санкцій; 5) розроблення системи оцінювання кіберзагроз; 6) забезпечення кібербезпеки єдиної інформаційної системи МВС України; 7) розроблення системи моніторингу. Визначено методи вирішення проблем інформаційної безпеки (організаційні, правові, психологічні, технічні, технологічні). Встановлено, що зазначені методи мають відповідати запропонованим етапам формування і реалізації механізму, до яких віднесено: 1) оцінення кібербезпеки та кіберзахисту; 2) оцінення потенційних кіберзагроз на майбутні періоди; 3) встановлення вимог до інформаційно-комп'ютерних технологій; 4) впровадження заходів забезпечення інформаційної безпеки; 5) впровадження системи заходів інформаційної безпеки суб'єктів реалізації; 6) впровадження інформаційного забезпечення інформаційно-комунікаційної системи; 7) впровадження системи постійного моніторингу за кібербезпекою.

Ключові слова: державна політика; економічна злочинність; інформаційна безпека.

Вступ

Актуальність дослідження. У процесі розвитку інформаційного суспільства та безмежного доступу до інформаційних джерел – як фізичних, так і віртуальних, особливо актуалізується потреба в якісній комунікації, що передбачає, насамперед, отримання достовірної інформації. Особливо актуальним це питання є для органів правоохоронної діяльності та системи державного управління. Окрім отримання достовірної інформації з метою прийняття ефективних рішень, постає питання щодо її збереження. Усе це актуалізує дослідження, пов'язані з удосконаленням забезпечення інформаційної безпеки реалізації державної політики запобігання та протидії економічній злочинності в системі гарантування економічної безпеки держави. Адже, дедалі частіше, питання інформаційних загроз та кібератак стосується саме правоохоронної системи держави, що унеможливлює здійснення ефективних заходів та забезпечення ефективного управління економічною безпекою держави. "Кіберзагрози для держави загалом та правоохоронної системи можуть проявлятися різними наслідками: соціальні, політичні, економічні, матеріальні, людські жертви, психологічні та інші. Кіберзлочини чинять вплив як на соціально-економічні відносини в певній державі, так і на світову економіку" [7].

Постановка проблеми. Попри це, сьогодні залишається відкритим питанням оновлення та вдосконалення діючих механізмів боротьби з економічною злочинністю у сфері інформаційної та громадської безпеки.

Мета дослідження та основні завдання для її досягнення. Метою є дослідження механізму реалізації державної політики запобігання та протидії економічній

Інформація про авторів:
Грицишен Димитрій Олександрович, д-р екон. наук, д-р наук з держ. управління, професор, проректор з науково-педагогічної роботи та інноваційного розвитку. **Email:** grytsyshen-do@ztu.edu.ua; https://orcid.org/0000-0001- 5484-6421
Дикий Анатолій Петрович, д-р екон. наук, доцент, кафедра теорії та історії держави і права. **Email:** anatoliy@ztu.edu.ua; https://orcid.org/0000-0002-5819-0236
Бутузов Віталій Миколайович, д-р юр. наук, професор, кафедра права і правоохоронної діяльності. **Email:** kppd_bvm@ztu.edu.ua; https://orcid.org/0000-0003-1096-6178
Цимбалюк Віталій Степанович, д-р юр. наук, ст. наук. співробітник, професор, кафедра права і правоохоронної діяльності. **Email:** kppd_tsvs@ztu.edu.ua; https://orcid.org/0009-0009-6458-6227
Цитування за ДСТУ: Грицишен Д. О., Дикий А. П., Бутузов В. М., Цимбалюк В.С. Механізм забезпечення інформаційної безпеки реалізації державної політики запобігання та протидії економічній злочинності. *Ефективність державного управління* : зб. наук. пр. Вип. 3/4(76/77). Львів: НЛТУ України, 2023. С. 70–76.
Citation APA: Grytsyshen, D. O., Dykyi, A. P., Butuzov, V. M., & Tsymbaliuk, V. S. (2023). The mechanism for ensuring information security for the implementation of the state policy of preventing and combating economic crime. *Efficiency of public administration, 3/4*(76/77), 70–76. https://doi.org/10.36930/507611

злочинності.

Предмет дослідження. Предметом дослідження є особливості механізму реалізації державної політики запобігання та протидії економічній злочинності.

Аналіз останніх досліджень та публікацій. Окремі аспекти питання реалізації державної політики запобігання та протидії економічній злочинності розглянуто в працях В.Т. Білоус, З.С. Варналії, Д.О. Грицишена, Д.В. Дубова, В.В. Євдокимова, О.М. Литвака, К.В. Малишева, Г.А. Матусовського, В.В. Ноніка, І.В. Супрунової та ін. Проте, ми вбачаємо за необхідне зосередити увагу саме на інформаційному забезпеченні механізму реалізації державної політики запобігання та протидії економічній злочинності.

Методи та інформаційна база дослідження. Проаналізовано показники кількості правопорушень та досліджено динаміку вчинених злочинів у сфері використання комп'ютерів та комп'ютерних мереж, динаміку кібератак за допомогою методу аналізу та статистичних порівнянь.

Методи абстрагування та узагальнення використано для визначення якісних характеристик механізму забезпечення інформаційної безпеки реалізації державної політики запобігання та протидії економічній злочинності і формулювання висновків дослідження.

Інформаційну базу дослідження становлять наукові публікації вітчизняних учених, статистичні матеріали реєстру кримінальних правопорушень та результати досудового розслідування Генеральної прокуратури України за період 2013-2022 рр., а також особисті наукові розробки та напрацювання авторів цієї публікації.

Виклад основного матеріалу дослідження з обґрунтуванням одержаних результатів

"У сучасних умовах інформаційного світу особливе місце в наукових дослідженнях, які активізуються з кожним роком, посідає кібербезпека. Останнім часом кібербезпека і її окремі аспекти стали предметом численних робіт дослідників. Однак, проблема усвідомлення цього явища залишається відкритою, що є логічним і необхідним, враховуючи надвисокі темпи розвитку суспільних відносин в електронній сфері. Це пояснюється, в першу чергу, розширенням можливостей інформаційного впливу на суспільні відносини, що спричиняє виникнення нових загроз громадської безпеки та викликає необхідність оновлення та вдосконалення системи її забезпечення. Крім того, саме поняття кібербезпеки вимагає якісного переосмислення, викликаного швидкими сутнісними змінами феномена інформації і домінуючими тенденціями розвитку світового співтовариства, яке значною мірою отримує "інформаційний" вимір" [10].

"В епоху інформаційних технологій неможливо почуватися захищеним у кіберпросторі. З розвитком технологій стрімко зростає кількість злочинів у цій сфері, а тому з впевненістю можна стверджувати, що саме "кіберзлочини" у XXI ст. будуть одними з найчисельніших. Виникнення нових сфер суспільного життя породжує й нові загрози. Державна влада, в особі правоохоронних органів, повинна реагувати на суспільно небезпечні та протиправні дії. Тому необхідність в забезпеченні безпеки інтересів людини і громадянина, суспільства та держави, національних інтересів в кіберпросторі поступово набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки держави. Кіберпростір – безмежний, а досвідчені хакери мають всі необхідні навички та засоби, щоб залишатися в ньому інкогніто. Сьогодні кібератаки шкодять не лише фізичним та юридичним особам, але й державам. Кібербезпека – один із ключових аспектів життя в інформаційну добу. Наші смартфони, соцмережі й інші онлайн-відбитки особи містять про користувачів інформації більше, ніж вони самі знають про себе. При тому, вони можуть бути значно більш вразливими для атак зловмисників, ніж людина в реальному житті" [8].

Дубов Д.В. у своєму монографічному дослідженні, присвяченому питанням кіберзлочинності зосереджує увагу на тому, що: "Кіберзагрози Український державі та суспільству умовно можна розділити на два ключових рівні. Перший – "класичні" кіберзлочини – як абсолютно оригінальні, так і вже звичні для нас, для своєї реалізації вони потребують лише сучасних інформаційних технологій. Другий – злочини, характерні для геополітичної боротьби (або такі злочини на місцевому рівні, які мають потенціал вплинути на політичне становище держави): хактивізм, кібершпигунство та кібердиверсії. Водночас техніки здійснення атак в обох випадках демонструють чимало спільного. Наприклад, фішингові техніки можуть бути використані як для заволодінням коштами громадян, так і з кібершпигунською метою. Хоча, звичайно, ціла низка кіберзлочинів має на меті й може скоюватися виключно для збагачення злочинців" [6; с. 210].

Проаналізувавши кількість правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку згідно з даними, наведеними у реєстрі кримінальних правопорушень та результати їх досудового розслідування Генеральної прокуратури України за період 2013-2022 рр. (табл. 1) можна простежити таку динаміку, яка вказує на те, що з 2013 р. до 2018 р. їх кількість збільшується або ж зменшується. Починаючи з 2019 р. до 2022 р. загальна кількість цих правопорушень має тенденцію до постійного зростання. Так, згідно з даними реєстру, загальна кількість таких правопорушень у 2019 р. становила 2204 випадки, а у 2022 р. зросла до 3415 випадків. Окрім того, в табл. 1 наведено кількість правопорушень у розрізі статей Кримінального кодексу України, що дає змогу детальніше зрозуміти наміри зловмисників у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Чинним законодавством передбачено відповідальність за скоєння кіберзлочину в межах статей Кримінального кодексу зазначених в табл. 1.

Водночас, для об'єктивного розгляду питань, пов'язаних зі стороннім впливом на інтернет-ресурси різних органів державної влади та місцевого самоврядування, фінансово-кредитних установ, засобів масової інформації, закладів освіти та інших державних ресурсів, вважаємо за необхідне більш детальне вивчення цього питання.

"У 2021 році в Україні зафіксовано 41 мільйон підозрілих подій інформаційної безпеки, опрацьовано 160 тис. критичних подій, зареєстровано 147 кіберінцидентів", – повідомляє Держспецзв'язку з посиланням на перший щорічний звіт Оперативного центру реагування на кіберінциденти Державного центру кіберзахисту (ДЦКЗ) за результатами виявлення вразливостей і реагування на кіберінциденти та кібератаки.

Табл. 1. Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку за 2013-2022 рр. (на основі [11])

Стаття Кримінального кодексу України	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, ст. 361	408	344	432	494	1795	1023	1183	1187	1679	1403
Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут, ст. 361-1	12	10	21	15	35	134	191	114	35	280
Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, ст. 361-2	20	11	59	28	64	52	57	131	141	60
Несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, ст. 362	152	73	75	311	670	1070	762	1047	1440	1664
Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється, ст. 363	2	4	9	15	6	12	7	16	12	3
Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку, ст. 363-1	1	1	2	2	3	10	4	3	3	5
Всього	*595*	*443*	*598*	*865*	*2573*	*2301*	*2204*	*2498*	*3310*	*3415*

Найчастіше кіберінциденти стосувалися:

- шкідливого програмного коду (28 %);
- збирання інформації зловмисниками (18 %);
- шахрайства (6 %) [5].

Своєю чергою у "Звіті роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки", який розміщено на офіційному сайті Оперативного центру реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації, наведено дані про кількість вчинених кібератак на сайти державних установ у 2021 р. Кількість зібраних та опрацьованих даних для виявлення підозрілих подій на об'єктах кіберзахисту, які спричинили певні кіберінциденти, наведено на рис. 1. Всього за звітний період підсистемою оперативного центру реагування на кіберінциденти виявлено близько 41 млн підозрілих подій інформаційної безпеки на об'єктах кіберзахисту.

Для ефективного реагування на ці загрози усю сукупність підозрілих подій розподілено за трьома пріоритетами: високий (58 %), середній (19 %) та низький (23 %). Відповідно, із загальної кількості виокремлено близько 160000 критичних подій інформаційної безпеки об'єктів кіберзахисту, в загальній сукупності яких найбільша частка критичних подій припадає на організації та підприємства (65 %), дещо менше здійснювався сторонній вплив на інтернет-ресурси Обласних державних адміністрацій (33 %) та міністерств (1 %). Отже, протягом 2021 р. Оперативного центру реагування на кіберінциденти зареєстровано 147 кіберінцидентів.

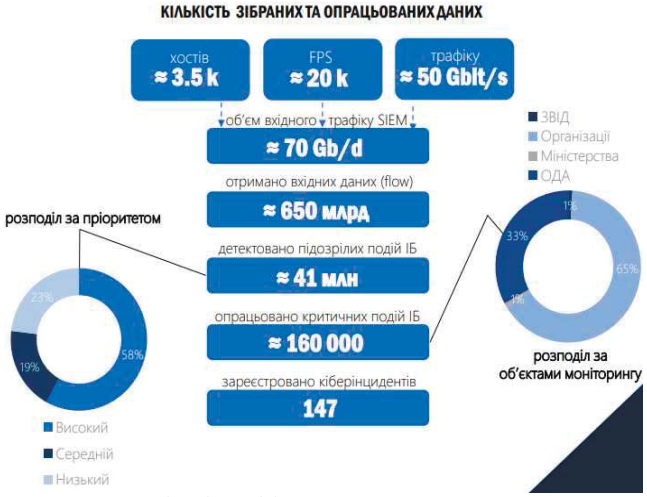

Рис. 1. Кількість зібраних та опрацьованих даних для виявлення кіберінцидентів у 2021 р. [5]

На рис. 2 та рис. 3 представлено інформацію про категорії та типи подій під час вчинення кібератак та кіберінцидентів.

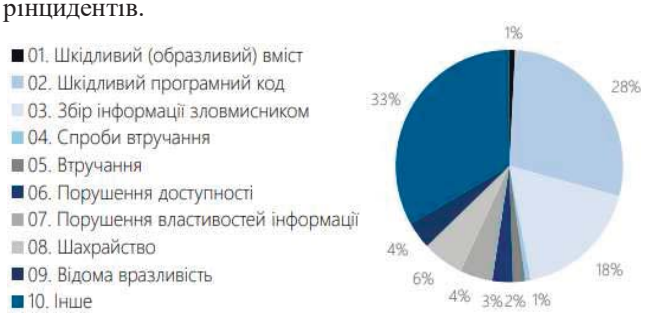

Рис. 2. Категорії подій кібератак та кіберінцидентів у 2021 р. [1]

На рис. 2 відображено усю сукупність критичних подій інформаційній безпеці у розрізі категорій, за якими вчинявся вплив на об'єкти кіберзахисту, згідно з Переліком категорій кіберінцидентів [1]. Отже, найбільший відсоток припадає на категорію 10. Інші невизначені інциденти (33 %), наступні категорії: 02 Шкідливий програмний код (28 %), 03 Збір інформації зловмисником (18 %). Незначний відсоток від загальної кількості припадає на такі категорії подій кібератак як: 08 Шахрайство (6 %), 07 Порушення властивостей інформації (4 %), 09 Відома вразливість (4 %), 06 Порушення доступності (3 %), 05 Втручання (2 %), 01 Шкідливий (образливий) вміст (1 %) та 04 Спроби втручання (1 %).

Також доречним є виокремлення типів подій кібератак та кіберінцидентів за якими зацікавлені особи здійснювали вплив на інтернет-ресурси об'єктів кіберзахисту (рис. 3).

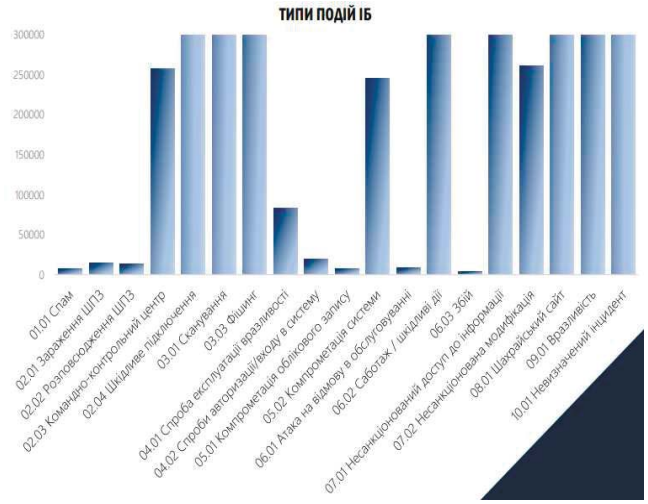

Рис. 3. Типи подій кібератак та кіберінцидентів у 2021 р. [1]

За даними рис. 3 спостерігається така динаміка прояву кібератак та кіберзлочинів у 2021 р. у розрізі їх типів. Так, згідно з Переліком категорій кіберінцидентів [1], найчастіше із загальної кількості інцидентів вчиняються такі, показник яких зафіксовано на рівні 300000: 02.04 Шкідливе підключення; 03.01 Сканування; 03.03 Фішинг; 06.02 Саботаж/шкідливі дії; 07.01 Несанкціонований доступ до інформації; 08.01 Шахрайський сайт; 09.01 Вразливість; 10.01 Невизначений інцидент. Наступними за рівнем прояву (близько 250000) були інциденти: 07.02 Несанкціонована модифікація; 02.03 Командно-контрольний центр; 05.02. Компроментація системи. Майже 10000 інцидентів зафіксовано за типом 04.01 Спроба експлуатації вразливості. Незначна кількість інцидентів, в межах до 2000 проявів, фіксувалася також за такими типами: 04.01 Спроба експлуатації вразливості; 02.01 Зараження шкідливим програмним забезпеченням; 02.02 Поширення ШПЗ; 01.01 Спам; 05.01 Компрометація облікового запису; 06.01 Атака на відмову в обслуговуванні; 06.03 Збій.

За даними, опублікованими у "Звіті роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки", який розміщено на офіційному сайті Оперативного центру реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації, можемо спостерігати ситуацію, що у 2021 р. виявлено та оброблено 1164 випадки кібератак на об'єктах кіберзахисту, які представлено у розрізі типів індикаторів та різновиду шкідливого програмного забезпечення (рис. 4).

Рис. 4. Прояви кібератак у розрізі індикаторів [1]

За типом індикаторів найбільша частка з кількості випадків, вказаної на рис. 4, припадає на кібератаки, вчинені через ip-з'єднання (89 %). Значно менше випадків кібератак зафіксовано через domain та url-з'єднання – 7 % та 4 % відповідно. Якщо розглядати ці випадки з погляду типу, до якого відноситься шкідливе програмне забезпечення – переважають кібератаки, вчинені за допомогою шкідливого мережевого програмного забезпечення, на зразок як Conficker та Trickbot, таких проявів зафіксовано до 500 випадків за кожним типом.

Як зазначає Н. Курочко: "За останній рік кількість кібератак у світі зросла в середньому на 50 %. Перша половина 2022 р. демонструє значне зростання атак проти всіх галузей економіки – у середньому 605 на день. Найчастіше цілями хакерів ставали державний, фінансовий сектори та медіа – близько 2600 атак щотижня, що на 44 % більше, ніж у 2021 р." [9].

Так, у "Аналітичному довіднику "Війна у цифровому вимірі та права людини, – аналітичний звіт за період із 24 лютого по 30 квітня 2022 р.", який підготовлено ГО "Платформа прав людини", зазначено такі дані про кібератаки: "Всього за період із 24 лютого по 30 квітня 2022 р. зафіксовано 32 повідомлення про кібератаки на вебсайти державних органів, установ, організацій та ЗМІ. Серед них: 7 повідомлень стосувалося кібератак на офіційні вебсайти органів державної влади та органів місцевого самоврядування, 23 – на сайти ЗМІ та на соціальні мережі, 2 – на вебсайти ГО." [3, с. 7].

Окрім кібератак досить поширеними є також фішинг-атаки, за допомогою яких зацікавлені особи намагаються заволодіти особистою інформацією населення. Як зазначають О. Вдовенко, Є. Воробйов, Л. Опришко: "Всього за період із 24 лютого по 30 квітня 2022 р. зафіксовано 15 повідомлень про фішинг-атаки, які було націлено на широке коло осіб, зокрема й на органи державної влади, їхніх посадових і службових осіб" [3, с. 10].

Як зазначено в "Аналітичному документі Державної служби спеціального зв'язку та захисту інформації України: "Найбільше атак припало на початок року, ще до повномасштабного вторгнення, а протягом першого місяця війни Україна зазнала втричі більше кібератак, ніж рік тому у відповідний період". Кібератаки тривають і сьогодні, хоча їхня інтенсивність трохи знизилась. З 24.02.2022 по 24.08.2022 було здійснено 1123 кібератаки.

Основні сектори, які атакують хакери: уряд і місцеві органи влади – 260; сектор безпеки та оборони – 154; комерційні організації – 83; фінансовий сектор – 72; інше – 554.

Найпоширеніші методи кібератак: збір інформації зловмисником – 306; шкідливий програмний код – 267; втручання – 149; відома вразливість – 100; інше – 301" [4].

Також за даними ГО "Платформа прав людини", які базуються на отриманій на запит від Держспецзв'язку статистичній інформації, можна спостерігати таку ситуацію щодо кількості кібератак на державний сектор: "Якщо в лютому (з 1 по 23 лютого) на державний сектор здійснили близько 143 тисяч атак, то в наступні місяці ця цифра стрімко зросла: 3,2 мільйона атак за дві декади квітня, 42,7 мільйона у травні, 27,7 мільйона – в червні, 32,3 мільйона атак у липні, 28,7 мільйона атак у серпні, 25,1 мільйона у вересні" [2].

Останнім часом почастішали випадки прояву стороннього впливу на кіберпростір України, значною мірою це пов'язано із повномасштабним вторгненням російської федерації. Такі дії спрямовані на виведення з ладу електронних ресурсів органів державної влади та критичної інфраструктури з метою дестабілізації військово-політичної ситуації в Україні.

Відповідно до зазначеного, механізми забезпечення інформаційної безпеки процесів формування та реалізації державної політики запобігання та протидії економічній злочинності в системі гарантування економічної безпеки держави, мають ґрунтуватися на сукупності складників, до яких віднесемо такі:

- по-перше, забезпечення системи захисту інформації на усіх етапах реалізації державної політики та реалізації правоохоронної функції держави в сфері економічної злочинності. Воно полягає в тому, що інформаційних захист має бути побудований так, щоби врахувати специфіку діяльності кожного суб'єкта реалізації досліджуваної державної політики, а також встановити рівні безпеки для каналів передачі інформації між ним. Система захисту інформації повинна відповідати основним вимогам Конституції України та забезпечувати дотримання прав та свобод громадян і осіб без громадянства;
- по-друге, формування заходів з інформаційної гігієни усіх учасників реалізації державної політики та правоохоронної функції. Як показує практика, більшість інформаційних загроз пов'язані із необережністю учасників реалізації державної політики. Відповідно, є потреба у здійсненні навчальних заходів із кібергігієни серед осіб, що задіяні в досліджуваних процесах;
- по-третє, впровадження системи запобігання та протидії кіберзлочинам та особливих санкцій за злочини, здійснені в сфері реалізації правоохоронної функції;
- по-четверте, розроблення системи оцінки кіберзагроз для державної політики запобігання та протидії економічній злочинності в системі гарантування економічної безпеки держави. Така система оцінення дасть змогу визначити критичні точки та сформувати таку систему захисту, яка буде протидіяти сучасним кіберзагрозам;
- по-п'яте, забезпечення кібербезпеки єдиної інформаційної системи Міністерства внутрішніх справ України;
- по-шосте, розроблення системи моніторингу за кіберзагрозами в системі запобігання та протидії економічній злочинності. Система моніторингу має функціонувати на постійній основі як для попередження загроз, так і для усунення їх наслідків.

Усі зазначенні положення мають стати складниками комплексної системи забезпечення інформаційної безпеки процесу формування та реалізації державної політики запобігання та протидії економічній злочинності в системі гарантування економічної безпеки держави. Комплексність такої системи можлива за умови врахування властивостей усіх складників процесу реалізації державної політики (рис. 2).

Вихідними положеннями механізму забезпечення інформаційної безпеки процесу реалізації державної політики запобігання та протидії економічній злочинності в системі гарантування економічної безпеки держави є такі:

- принципи розроблення та функціонування механізму: законності; приватності; незалежності; динамічності; ієрархічності; захисту даних; керованості; професійності; конфіденційності; комплексності; комунікативності; систематичності;
- завдання, які потрібно досягти через впровадження механізму: 1) протидія інформаційній злочинності; 2) забезпечення обмеженого доступу до даних; 3) забезпечення безпеки даних суб'єктів реалізації державної політики; 4) забезпечення безпеки особистих даних учасників реалізації державної політики; 5) формування системи моніторингу за системою захисту інформації; 6) формування забезпечення реалізації механізму; 7) здійснення оцінки ефективності системи інформаційного захисту;
- методи забезпечення інформаційної безпеки процесу реалізації державної політики запобігання та протидії економічній злочинності: психологічні методи, спрямовані на психологічну оцінку учасників забезпечення інформаційної безпеки для визначення можливості виконання ними завдань, а також попередня оцінка впливу заходів інформаційної безпеки та психологічний стан учасників правоохоронних операцій та реалізації державної політики загалом; правові – формування правового поля забезпечення інформаційної безпеки, що враховує: режим доступу до інформації, порядок обміну інформацією, особливості зберігання та використання інформації, відповідальність за порушення процедур забезпечення інформаційної безпеки та інше; організаційні – розроблення та реалізація заходів із забезпечення інформаційної безпеки; технологічні – впровадження інформаційних технологій та формування вимог до програмних продуктів; технічні – технічне забезпечення процесів зберігання, обміну, збирання й використання інформації та налагодження комунікації між суб'єктами реалізації державної політики.

Висновки та перспективи подальших розвідок

Вважаємо, що механізм забезпечення інформаційної безпеки процесів реалізації досліджуваної політики має ґрунтуватися на системному підході в класичному розумінні змісту системи як впливу суб'єкта на об'єкт. Відповідно, суб'єктами системи інформаційного захисту державної політики є: Міністерство цифрової трансформації України; Міністерство внутрішніх справ; Міністерство оборони України та Генеральний штаб ЗСУ; Служба безпеки України; Кіберполіція; Держслужба спеціального зв'язку та захисту інформації України. Своєю чергою, об'єктом забезпечення інформаційного захисту державної політики є: витік інформації, кіберзлочини та інформаційна безпека учасників реалізації державної політики та правоохоронних процесів.

Власне процес формування системи інформаційного захисту державної політики забезпечення та протидії економічній злочинності має складатися із таких послідовних етапів: 1) оцінення кібербезпеки та кіберзахисту; 2) оцінення потенційних кіберзагроз на майбутні періоди; 3) встановлення вимог до інформаційно-комп'ютерних технологій; 4) впровадження заходів забезпечення інформаційної безпеки; 5) впровадження системи заходів інформаційної безпеки суб'єктів реалізації; 6) впровадження інформаційного забезпечення інформаційно-комунікаційної системи; 7) впровадження системи постійного моніторингу за кібербезпекою. Реалізація зазначених етапів потребує таких видів забезпечення: фінансове, інформаційне, правове, кадрове.

Отже, розроблено механізм забезпечення інформаційної безпеки процесів запобігання та протидії економічній злочинності. Цей механізм включає вихідні положення, зокрема: встановлено суб'єкти забезпечення інформаційного захисту та виявлено властивості об'єктів. Визначено принципи, яким має відповідати система інформаційного захисту процесів реалізації державної політики. У контексті назрілих проблем інформаційного характеру запропоновано сукупність завдань механізму, а їх вирішення можливе через організаційні, правові, психологічні, технічні та технологічні методи. Встановлено, що зазначені методи мають відповідати запропонованим етапам формування і реалізації цього механізму, до яких віднесено: 1) оцінення кібербезпеки та кіберзахисту; 2) оцінення потенційних кіберзагроз на майбутні періоди; 3) встановлення вимог до інформаційно-комп'ютерних технологій; 4) впровадження заходів забезпечення інформаційної безпеки; 5) впровадження системи заходів інформаційної безпеки суб'єктів реалізації; 6) впровадження інформаційного забезпечення інформаційно-комунікаційної системи; 7) впровадження системи постійного моніторингу за кібербезпекою.

Список використаної літератури

1. Cert-Ua (2023). Перелік категорій кіберінцидентів, схвалений Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України (Протокол № 18 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 25.10.2021 (від 28.10.2021 № 16/320/21дск)). URL: https://cert.gov.ua/recommendation/16904
2. Вдовенко, О. (2022). 25 мільйонів кібератак щомісяця. Як Росія намагається зашкодити Україні в цифровому просторі. *Детектор Медіа*. URL: https://detector.media/ infospace/article/204308/2022-10-29-25-milyoniv-kiberatak-shchomisyatsya-yak-rosiya-namagaietsya-zashkodyty-ukraini-v-tsyfrovomu-prostori/
3. Вдовенко, О., Воробйов, Є., & Опришко, Л. (2022). Аналітичний звіт "Війна у цифровому вимірі і права людини". Київ, 68.
4. Державна служба спеціального звязку та захисту інформації України (2022). Війна в Україні. Пульс кібер захисту. Аналітичний документ, 2022. URL: https://www.ppl.org.ua/wp-content/uploads/2022/09/1662392024242416.pdf
5. Дзеркало тижня (2021). Держспецзв'язку назвало кількість зафіксованих у 2021 році кіберзлочинів. URL: https://zn.ua/ukr/TECHNOLOGIES/derzhspetszvjazku-nazvalo-kilkist-zafiksovanikh-u-2021-rotsi-kiberzlochiniv.html
6. Дубов, Д. В. (2014). Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 328. URL: https://niss.gov.ua/sites/default/files/2015-02/Dubov_mon-89e8e.pdf
7. Євдокимов, В. & Грицишен, Д. (Ed) (2023). Криза правоохоронної системи України: монографія. Житомир: Книжковий дім "Бук-друк", 584 с.
8. Капля, А. В. (2021). Кібербезпека як важливий аспект сьогодення. *Конференції Державного університету "Житомирська політехніка"*. URL: https://conf.ztu.edu.ua/wp-content/uploads/2021/01/29-2.pdf
9. Курочко, Н. (2022). Як росія та Україна воюють на кіберфронті. *Економічна правда*. URL: https://www.epravda.com.ua/columns/2022/09/28/691925/
10. Лісовська, Ю. П. (2019). Кібербезпека: ризики та заходи. Київ: Видавничий дім "Кондор", 272.
11. Офіс Генерального прокурора (2023). Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2

D. O. Grytsyshen, A. P. Dykyi, V. M. Butuzov, V. S. Tsymbaliuk

State University "Zhytomyr Polytechnic", Zhytomyr, Uktaine

THE MECHANISM FOR ENSURING INFORMATION SECURITY FOR THE IMPLEMENTATION OF THE STATE POLICY OF PREVENTING AND COMBATING ECONOMIC CRIME

Introduction. In the process of development of the information society and unlimited access to information sources – both physical and virtual, the need for quality communication is especially relevant, which involves, first of all, obtaining reliable information. This issue is especially relevant for law enforcement agencies and the state administration system. In addition to obtaining reliable information for the purpose of making effective decisions, the question of its preservation arises. The above actualizes research related to the improvement of information security in the implementation of the state policy of preventing and combating economic crime in the system of guaranteeing the economic security of the state. After all, the issue of informational threats and cyberattacks is increasingly related to the law enforcement system of the state, which makes it impossible to implement effective measures and ensure effective management of the economic security of the state. "Cyber threats to the state as a whole and the law enforcement system can be manifested by a preponderance of consequences: social, political, economic, material, human victims, psychological and others. Cybercrimes affect both socio-economic relations in a certain state and have an impact on the world economy" [7]

Analysis of Literary Sources. Separate aspects of the implementation of the state policy of prevention and counteraction of economic crime were considered in the works of V.T. Bilous, Z.S. Varnalii, D.O. Grytsyshena, D.V. Dubova, V.V. Evdokymova, O.M. Litvak, K.V. Malysheva, G.A. Matusovsky, V.V. Nonika, I.V. Suprunova et al. However, we consider it necessary to focus attention precisely on the information provision of the mechanism of implementation of the state policy of prevention and counteraction of economic crime.

Results. The concepts of cyberspace, cyber security, and cybercrime are defined. A statistical analysis of the number of offenses was carried out and the dynamics of crimes committed in the field of using computers and computer networks for the period from 2013 to 2022 were investigated. Information on the main sectors of hacker attacks was provided and a list of the most common methods of cyber attacks was determined. The article defines the subjects and objects of information protection of the state policy and the list of principles that should guide the information protection system, describes the stages of formation of the information security mechanism and the necessary types of support (financial, informational, legal, personnel). The specified stages include the assessment of cyber security, the establishment of requirements for technologies, the implementation of measures to ensure information security and the monitoring system for cyber security. A list of components of the information security mechanism is proposed, including: 1) provision of the information protection system at all stages of implementation of state policy; 2) information hygiene; 3) introduction of sanctions; 5) development of a cyber threat assessment system; 6) ensuring cyber security of the unified information system of the Ministry of Internal Affairs of Ukraine; 7) development of a monitoring system. Methods of solving information security problems (organizational, legal, psychological, technical, technological) are defined. It was established that the specified met-

hods should correspond to the proposed stages of formation and implementation of the mechanism, which include: 1) assessment of cyber security and cyber protection; 2) assessment of potential cyber threats for future periods; 3) establishing requirements for information and computer technologies; 4) implementation of information security measures; 5) implementation of the system of information security measures of implementation entities; 6) implementation of information support of the information and communication system; 7) implementation of a permanent monitoring system for cyber security.

Discussion. The determining factor in ensuring the information security of the state is the implementation of the state policy of preventing and countering economic crime in the system of guaranteeing the economic security of the state with the help of new and effective mechanisms.

Conclusion. We believe that the mechanism for ensuring information security of the processes of implementation of the researched policy should be based on a systemic approach in the classical understanding of the content of the system as the influence of the subject on the object. Accordingly, the subjects of the state policy information protection system are: the Ministry of Digital Transformation of Ukraine; Ministry of Internal Affairs; The Ministry of Defense of Ukraine and the General Staff of the Armed Forces of Ukraine; Security Service of Ukraine; Cyber police; State Service for Special Communications and Information Protection of Ukraine. In turn, the object of ensuring information protection of state policy is: information leakage, cybercrime and information security of participants in the implementation of state policy and law enforcement processes.

The actual process of forming a system of information protection of the state policy of ensuring and combating economic crime should consist of the following successive stages: 1) assessment of cyber security and cyber protection; 2) assessment of potential cyber threats for future periods; 3) establishing requirements for information and computer technologies; 4) implementation of information security measures; 5) implementation of the system of information security measures of implementation entities; 6) implementation of information support of the information and communication system; 7) implementation of a permanent monitoring system for cyber security. Implementation of the specified stages requires the following types of support: financial, informational, legal, personnel.

Keywords: state policy; economic crime; information security.