Механізм забезпечення кібербезпеки правоохоронної системи

The mechanism for ensuring cyber security of the law enforcement system

Димитрій Грицишен [A]

***Corresponding author**: к. екон. н., доктор наук з державного управління, професор, проректор з науково-педагогічної роботи та інноваційного розвитку, e-mail: grytsyshen-do@ztu.edu.ua, ORCID: 0000-0001-5484-6421

Костянтин Малишев [A]

доктор наук з державного управління, доцент кафедри права та правоохоронної діяльності, e-mail: kppd_mkv@ztu.edu.ua, ORCID: 0009-0002-7984-411X

Валерій Нонік [A]

доктор наук з державного управління, доцент, завідувач кафедри теорії та історії держави і права, e-mail: vr_nvv@ztu.edu.ua, ORCID: 0000-0002-5252-3570

Валерій Молотай [A]

кандидат психологічних наук, доцент кафедри права та правоохоронної діяльності, e-mail: kppd_mva@ztu.edu.ua, ORCID: 0009-0008-0817-1097

Dimitriy Grycyshen [A]

***Corresponding author**: Dr of Economics, Dr of Public Administration, Professor, Vice-Rector for Scientific and Pedagogical Work and Innovative Development, e-mail: grytsyshen-do@ztu.edu.ua, ORCID: 0000-0001-5484-6421

Kostyantyn Malyshev [A]

Dr of Science in Public Administration, Associate Professor of the Department of Law and Law Enforcement, e-mail: kppd_mkv@ztu.edu.ua, ORCID: 0009-0002-7984-411X

Valery Nonik [A]

Dr of Science in Public Administration, Associate Professor, Head of the Department of Theory and History of the State and Law, e-mail: vr_nvv@ztu.edu.ua, ORCID: 0000-0002-5252-3570

Valery Molotai [A]

Candidate of Psychological Sciences, Associate Professor of the Department of Law and Law Enforcement, e-mail: kppd_mva @ztu.edu.ua, ORCID: 0009-0008-0817-1097

[A] Державний університет "Житомирська політехніка", м. Житомир, Україна

[A] Zhytomyr Polytechnic State University, Zhytomyr, Ukraine

Received: August 15, 2023 | Revised: August 28, 2023 | Accepted: August 31, 2023

DOI: 10.33445/sds.2023.13.4.3

Мета роботи: аналіз стану кіберзлочинів та хакерських атак в Україні та світі в цілому; дослідження механізмів державної політики щодо забезпечення кібербезпеки правоохоронної системи в Україні та країн Європи на основі нормативно-правових документів для розробки та вдосконалення комплексного механізму забезпечення кібербезпеки правоохоронної системи України.

Метод дослідження: аналіз, синтез, метод порівняння.

Результати дослідження: розроблено комплексний механізм забезпечення кібербезпеки правоохоронної системи.

Теоретична цінність дослідження: визначення основних діючих механізмів державної політики щодо забезпечення кібербезпеки в Україні та країн Європи, вибірка статистичних даних щодо стану кіберзлочинів в Україні та хакерських атак у світі за останні роки задля порівняння та оцінки їх стану.

Тип статті: аналітичний, теоретично-методичний, описовий.

Purpose: is analysis of the state of cybercrime and hacker attacks in Ukraine and the world as a whole; study of state policy mechanisms for ensuring cyber security of the law enforcement system in Ukraine and European countries on the basis of legal documents for the development and improvement of a comprehensive mechanism for ensuring cyber security of the law enforcement system of Ukraine.

Method: analysis method and synthesis, method of comparison.

Findings: a comprehensive mechanism for ensuring the cyber security of the law enforcement system was developed.

Theoretical implications: identification of the main active mechanisms of state policy to ensure cyber security in Ukraine and European countries, a selection of statistical data on the state of cybercrimes in Ukraine and hacker attacks in the world in recent years for comparison and assessment of their state.

Paper type: analytical, theoretical-methodical, descriptive.

Ключові слова: кіберзлочини, кібербезпека, державна політика, правоохоронні органи.

Key words: cybercrimes, cyber security, state policy, law enforcement agencies.

1. Вступ

Сучасне суспільство характеризується як інформаційне. А це означає, що жодна сфера суспільного розвитку не може не проявляти або існувати поза межами кіберпростору. "Глобальна інформатизація активно впливає на функціонування держав світової спільноти, інформаційні технології застосовуються в процесі вирішення завдань забезпечення національної, військової, економічної безпеки. Водночас одним з фундаментальних наслідків глобальної інформатизації державних та приватних структур стало виникнення принципово

нового середовища протиборства конкурентних держав – кіберпростору. Використання Інтернету та інформаційних технологій не тільки відкриває перед людством безмежні можливості, а й створює нові серйозні загрози. Все більше інформації переміщується в онлайн і за останніми підрахунками у світі вже понад 20 млрд пристроїв підключених до інтернету, що у кілька разів більше, ніж населення Землі. Також на серверах збирається мільярди гігабайт різної інформації. Світ стає відкритим, та таке стрімке зростання потребує формування "правил гри"" [1].

Дані питання не можуть оминути і правоохоронну систему, застосування інноваційних інформаційних технологій дозволяє прискорити та удосконалити процеси реалізації правоохоронної функції, а з іншого боку піддає правоохоронну систему в цілому та її окремі складові кіберзагрозам. Кібербезпека в державній політиці в сфері трансформації правоохоронної системи проявляється з двох позицій: по-перше, правоохоронна система має забезпечити реалізацію заходів із запобігання та протидії кіберзагрозам та кіберзлочинам, що визначені нами в контексті створення відповідної інституції – правоохоронного органу; по-друге, правоохоронна система може стати об'єктом кіберзагроз. Друга позиція актуалізує дослідження щодо розробки механізмів державної політики забезпечення кібербезпеки правоохоронної системи.

2. Теоретичні основи дослідження

Проблематика питань кібербезпеки в цілому та кібербезпенки правоохоронної системи досліджувалися в працях [2]-[4]. Зазначенні вчені розглядали різні аспекти прояву кібербезпеки в правоохоронній діяльності, проте, на сьогодні невирішеними залишилися питання механізмів державної політики щодо забезпечення кібербезпеки правоохоронної системи.

3. Постановка проблеми

"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"" [5].

4. Результати

"XXI століття знаменується активним формуванням шостого технологічного укладу (біо-, нано, інфо-, когнотехнологій, їх конвергенцією) та ризиками, з якими стикається цивілізація внаслідок упровадження новітніх технологій, зокрема їх використання у кіберпросторі. Питома вага кіберзагроз у спектрі загроз національній безпеці країн зростає, і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу на функціонування структур управління як національних, так і транснаціональних формує абсолютно нову безпекову ситуацію з викликами нового технологічного рівня. Між світовими центрами сили

відбувається поділ сфер впливу у кіберпросторі, посилюється їх прагнення за рахунок такого поділу забезпечити реалізацію власних геополітичних інтересів. Кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій, тому спроможність держави захищати національні інтереси в ньому розглядається як важлива складова кібербезпеки. Набирає сили тенденція зі створення нового роду військ – кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, спрямованих на знищення обчислювальних мереж та інформаційних систем збройних сил противника, а також виведення з ладу критично важливих об'єктів противника шляхом руйнування інформаційних систем, які управляють такими об'єктами" [6].

"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 столітті 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" [7].

Кіберзагрози для держави в цілому та провоохоронної 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. "Хакерські атаки протягом 2020 року коштували світовій економіці понад трильйон доларів або 820 мільярдів євро. Про це свідчать оприлюднені у понеділок, 7 грудня, дані американської компанії McAfee, яка спеціалізується на комп'ютерній безпеці, та Центру стратегічних і міжнародних досліджень (CSIS). Завданий цього року хакерами збиток є на 50 відсотків вищим, ніж був ще два роки тому, у 2018 році, встановили дослідники. Таким чином збитки, завдані хакерами у 2020 році, становлять понад один відсоток світового ВВП, інформує агенція AFP" [8].

"Кіберзлочинність у всьому світі щороку завдає збитків на десятки мільярдів доларів США як державам, так і приватним компаніям. Чого лиш варта атака вірусу Petya, який призвів до зупинення багатьох державних інституцій світу та бізнесу, зокрема й в Україні" [9].

Статичні данні щодо кіберзлочинів в Україні свідчать про особливу їх загрозу (табл. 1) для національної безпеки та правоохоронної системи.

Таблиця 1 – Кіберзлочини у 2020 р. за даними Національної поліції

ВИКРИТО КІБЕРЗЛОЧИНІВ [10]			
Платіжні системи	**Кіберезпека**	**Протиправний контент**	**Електронна комерція**
1641	1494	332	744
ПРОТИДІЯ [5]			
Звернень через зворотній зв'язок	**Заблоковані шахрайські інтернет-посилання**	**Заблоковані банківські рахунки шахраїв**	
41568	28559	8798	
ЗБИТКИ ВІД КІБЕЗЛОЧИНІВ [10]			
Завдано	**Відшкодовано**	**%**	
28 млн. грн	17 млн. грн	60	

Дана статистика в цілому показує стан у 2020 році, проте зазначені цифри зросли у порівнянні з попередніми роками, при цьому значно кібзерзлочини активізувалися в 2021 р. Важливе значення в забезпечення кібезбезнеки системи державного управління та правоохоронної системи зокрема, покладається на запобігання та протидію хакерським атакам, що значно активізувалися в довоєнний та воєнний періоди:

- довоєнний період: "За останні місяці Україна не вперше зазнає кібератак: найбільша з них до 15 лютого була зафіксована ще 14–15 січня. В "Українському кіберальянсі" заявляють, що зловмисникам вдалося не лише зламати сайти міністерств та застосунок "Дія", а й викрасти персональні дані мільйонів людей із бази МВС країни. Однак в СБУ повідомили, що витоку даних внаслідок кібернападу не відбулося. Втім, деякі електронні сервіси, наприклад, сервіс перевірки полісу страхування цивільної відповідальності автовласників, не працювали після цієї атаки ще кілька тижнів" [11];

- воєнний період: "За місяць війни вже сталося майже втричі більше хакерських атак різного виду, ніж за аналогічний період минулого року. Найпопулярнішими видами атак залишаються фішингові розсилання, розповсюдження шкідливого програмного забезпечення, DDoS-атаки" [12]. "Загалом за місяць війни вже сталося майже втричі більше хакерських атак різного виду, ніж за аналогічний період минулого року: 198 проти 76. Проте більшість із них – безуспішні та майже не впливають на роботу критичної інформаційної інфраструктури" [13].

Проблема щодо кібератак характерна і для інших країн світу, що представлено в табл. 2 та табл. 3.

Таблиця 2 – Хакерські атаки в світі (07.2020 р. – 06.2021 р.)

КРАЇНИ, ПРОТИ ЯКИХ БУЛИ СПРЯМОВАНІ ХАКЕРСЬКІ АТАКИ				
США	Україна	Великобританія	Бельгія	Німеччина
46%	19%	9%	3%	3%
Ізраїль	Молдова	Португалія	Саудівська Аравія	Інші
2%	2%	1%	1%	11%
ХАКЕРСЬКІ АТАКИ У СВІТІ ЗА КРАЇНАМИ ПОХОДЖЕННЯ				
РФ	КНДР	Іран	Китай	
58%	23%	11%	8%	
Південна Корея	В'єтнам	Туреччина		
< 1%	< 1%	< 1%		
СЕКТОРИ, ПРОТИ ЯКИХ БУЛИ СПРЯМОВАНІ ХАКЕРСЬКІ АТАКИ У СВІТІ				
Держуправління	Неурядові організації та аналітичні центри	Освіта		
48%	31%	3%		
Міжнародні міжурядові організації	IT	Медіа		
3%	2%	1%		
Охорона здоров'я	Енергетика	Інші		
1%	1%	10%		
СПОЖИВЧІ ТА КОРПОРАТИВНІ ЦІЛІ ХАКЕРСЬКИХ АТАК				
Копоративні	Споживчі			
79%	21%			

Джерело: сформовано на основі [14].

Хакерські атаки в світі у період 07.2020 р по 06.2021 р. найбільше здійснювалися проти таких країн, як США (46%), Україна (19%), Великобританія (9%), Бельгія (3%), Німеччина (3%), Молдова (2%), Португалія (1%), Саудівська Аравія (1%) та інших (10%). Так, більша частина хакерських атак (79%) була спрямована на корпоративні цілі. Головними секторами, проти яких були спрямовані хакерські атаки стали: держуправління, неурядові організації та аналітичні центри, освіта, міжнародні міжурядові організації, IT, медія, охорона здоров'я, енергетика та інші. Протягом досліджуваного періоду, найбільшу кількість хакерських атак

було зафіксовано з території РФ (58%). Друге місце у цьому рейтингу посідає КНДР (23%). Наступна країна за місцем походження хакерських атак є Іран (11%). Незначний відрив від Ірану має Китай, з території якого було здійснено 8% хакерських атак. Також, атаки були зафіксовані з території Південної Кореї, В'єтнама, Туреччини та інших країн.

Таблиця 3 – Найбільш активні хакерські групи (07.2020 р. – 06.2021 р.)

Об'єкти хакерських атак	**Група та країна знаходження**							
	РФ	КНДР	Іран	КНДР	Китай	Китай	Іран	Не визначенні
	Nobelium	Nhallium	Phosphorus	Cetrium	Zirconium	Nickel	Curium	
Держуправління	+				+	+	+	
Дипломатія	+	+	+	+	+	+		
Оборона	+			+			+	
Ядерна політика			+					
Неурядові організації	+							
IT	+						+	
Телекомунікації	+							
Аналітичні центри	+	+		+				
Наука		+	+	+				
Журналістика			+					
Економіка					+			
Аерокосмічна галузь				+				
Активність групи	59%	16%	9%	5%	3%	2%	2%	4%

Джерело: сформовано на основі [14]

Найбільш активною хакерською групою можна назвати російське угрупування Nobelium, активність якого сягає 59%. Дане угрупування здійснювало хакерські атаки на сектори держуправління, дипломатії, оборони, неурядових організацій, IT, телекомунікацій та аналітичні центри. Друге місце за активністю посідає угрупування Thallium, яке здійснює свою діяльність з території КНДР. Від діяльності зазначеного угрупування найбільше постраждали сектори дипломатії, науки та аналітичних центрів. Загалом, активність групи сягає 16%. Варто зазначити, що на території КНДР також діє група Cetrium, яка здійснювала атаки на об'єкти аналітичних центрів, дипломатії, оборони, науки, аерокосмічної галузі. Загалом, активність даного угрупування сягає 5%.

Також активне хакерське угрупування Phosphorus, яке здійснює напади на сектори дипломатії, ядерної політики, науки та журналістики. Дана група базується на території Ірану, та же само як і угрупування Curium. Curium здійснює хакерські атаки на об'єкти держуправління, оборони та IT.

Zirconium та Nickel є китайськими угрупуваннями, активність яких сягає 3% і 2% відповідно. Об'єктами їх атак стали сектори держуправління та оборони. Групою Zirconium були здійснені атаки на сектори економіки. Варто зазначити, що понад 4% активності хакерських угрупувань досі не визначені кому належать.

Міжнародним документом відповідно до якого формується державна політика щодо забезпечення кібербезпенки в Україні є Конвенція про кіберзлочинність, яка була ратифікована у 2005 р. ЇЇ структура передбачає наступні види кіберзлочинів (табл. 4).

Дана концепція є основою міжнародного співробітництва між країнами та формування національного законодавства щодо забезпечення кібербезпеки держави та запобігання і протидії кіберзлочинам. Правоохоронну систему в контексті зазначеного можна розглядати в двох аспектах: по-перше, як інструмент запобігання та протидії кіберзлочинам; по-друге, як об'єкт проти яких кіберзагроз.

Таблиця 4 – Структура Конвенції про кіберзлочинність

Розділ	Підрозділ	Статті
Використання термінів	комп'ютерна система, комп'ютерні дані, постачальник послуг, дані про рух інформації	
Заходи, які мають здійснюватися на національному рівні	**МАТЕРІАЛЬНЕ КРИМІНАЛЬНЕ ПРАВО**	
	Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем	Незаконний доступ
		Нелегальне перехоплення
		Втручання у дані
		Втручання в систему
		Зловживання пристроями
	Правопорушення, по-в'язані з комп'ютерами	Підробка, пов'язана з комп'ютерами
		Шахрайство, пов'язане з комп'ютерами
	Правопорушення, пов'язані зі змістом	Правопорушення, пов'язані з дитячою порнографією
	Правопорушення, пов'я-зані з порушенням авто-рських та суміжних прав	Правопорушення, пов'язані з порушенням авторських та суміжних прав
	Додаткова відповідальність і санкції	Спроба і допомога або співучасть
		Корпоративна відповідальність
		Санкції і заходи
	ПРОЦЕДУРНЕ ПРАВО	
	Загальні положення	Сфера процедурних положень
		Умови і запобіжні заходи
	Загальні вимоги	Термінове збереження комп'ютерних даних, які зберігаються
		Термінове збереження і часткове розкриття даних про рух інформації
	Порядок представлення	Порядок представлення
		Обшук і арешт комп'ютерних даних, які зберігаються
	Збирання комп'ютерних даних у реальному масштабі часу	Збирання даних про рух інформації у реальному масштабі часу
		Перехоплення даних змісту інформації
	ЮРИСДИКЦІЯ	
	Юрисдикція	Юрисдикція
Міжнародне співробітництво	**ЗАГАЛЬНІ ПРИНЦИПИ**	
	Загальні принципи міжнародного співробітництва	Загальні принципи міжнародного співробітництва
	Принципи екстрадиції	Екстрадиція
	Загальні принципи взаємної допомоги	Загальні принципи взаємної допомоги
		Добровільно надана інформація
	Процедури, пов'язані із запитами про взаємну допомогу у разі відсутності відповідних міжнародних угод	Процедури, пов'язані із запитами про взаємну допомогу у разі відсутності відповідних міжнародних угод
		Конфіденційність і обмеження у використанні
	КОНКРЕТНІ ПРИНЦИПИ	
	Взаємна допомога щодо тимчасових заходів	Термінове збереження комп'ютерних даних, які зберігаються
		Термінове розкриття збережених даних про рух інформації

Розділ	Підрозділ	Статті
	Взаємна допомога щодо повноважень на розслідування	Взаємна допомога щодо доступу до комп'ютерних даних, які зберігаються
		Транскордонний доступ до комп'ютерних даних, які зберігаються, за згодою або у випадку, коли вони є публічно доступними
		Взаємна допомога у збиранні даних про рух інформації у реальному масштабі часу
		Взаємна допомога у перехопленні даних змісту інформації
	Цілодобова мережа	Цілодобова мережа
Прикінцеві положення	**Прикінцеві положення**	Підписання та набуття чинності
		Приєднання до Конвенції
		Територіальне застосування
		Цілі Конвенції
		Заяви
		Клаузула щодо федеральних держав
		Застереження
		Статус та відкликання застережень
		Зміни
		Вирішення спорів
		Консультації Сторін
		Денонсація
		Повідомлення

Джерело: сформовано автором на основі [15]

Об'єкт даного дослідження передбачає вивчення другої позиції, що визначає необхідність формування механізму державної політики забезпечення кібербезпеки правоохоронної системи. У зв'язку із тим, що Концепція передбачає поділ кібезлочинів на види ("1) Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем. Цей вид охоплює незаконний доступ, нелегальне перехоплення, втручання в дані, втручання у систему, зловживання пристроями; 2) Правопорушення, пов'язані з комп'ютерами. До цього виду належить підробка, пов'язана з комп'ютерами, і шахрайство, пов'язане з комп'ютерами; 3) Правопорушення, пов'язані зі змістом. Це – правопорушення, пов'язані з дитячою порнографією; 4) Правопорушення, пов'язані з порушенням авторських і суміжних прав. Цей вид охоплює правопорушення, пов'язані з порушенням авторських і суміжних прав" [6]), вважаємо положеннями, яким має відповідати механізм забезпечення кібербезпеки правоохоронної системи є позиції 1 та 2.

Відповідно до зазначеної Концепції формується національна система правового забезпечення кібербезпеки держави. Вперше питання правового регулювання кібербепеки в світі було піднято в США. "Найпершим в історії законодавчим актом, котрий регулював забезпечення кібербезпеки у кіберпросторі, був "The Computer Fraud and Abuse Act" (Закон про боротьбу з комп'ютерними шахрайством та комп'ютерними зловживанням), прийнятий в 1986 році у Сполучених Штатах Америки. Даний акт, по суті, визнавав проблему можливості вчинення неправомірних дій у інформаційній сфері, що дало поштовх до розвитку інституту кібербезпеки. Закон закріпив відповідальність за несанкціоноване втручання у роботу комп'ютерних систем чи викрадення інформації з них. Крім цього, актом передбачено санкції до осіб, які вчиняють дії подібного характеру" [16]. "Однією з перших держав, що сприйняла кібербезпеку як питання державного рівня, була США, де 2003 року було опубліковано Національну стратегію безпеки в кіберпросторі. У наступні роки в Європі поширювались плани

заходів та стратегії, покликані розв'язати подібну задачу. Через велику кібератаку 2007 року Естонія стала однією з перших державчленів Євросоюзу, яка опублікувала 2008 року національну стратегію кібербезпеки, у якій особливу увагу зосереджено на безпеці ІКТ" [17].

"Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України" [18].

Правове забезпечення реалізації механізму кібербезпеки правоохоронної системи, складається із наступних нормативно-правових актів:

Кримінальний кодекс України [19] передбачає наступні статті щодо запобігання і протидії кібрезлочинам та забезпечення кібербезпеки:

361 – несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

361-1 – створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут;

361-2 – 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;

362 – несанкціоновані дії з інформацією, яка оброблюється 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;

363 – 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 оброблюється;

363-1 – перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

Законом України "Про основні засади забезпечення кібербезпеки України". Структура даного закону передбачає наступні складові правого регулювання: правові основи забезпечення кібербезпеки, визначення об'єктів кібебезпеки та кіберзахисту, специфіка діяльності суб'єктів забезпечення кібербезпеки, принципи забезпечення кібербезпеки, визначення напрями формування національної системи кібербезпеки, напрями взаємодії державних суб'єктів забезпечення кібербезпеки із приватними структурами, міжнародними організаціями та іншими країнам, фінансове забезпечення заходів кібербезпеки та контроль моніторинг за їх реалізацією. Даним законом визначено, що "Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури" [19]. Відповідно формуванні механізму державної політики забезпечення кібербезпеки правоохоронної системи є потреба в забезпеченні його відповідності даному Закону. Крім того, в даному дослідженні будемо керувати термінами, що визначенні в законі, зокрема: "кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне

виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі; кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту; кіберзагроза – 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; кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем" [19].

Державна політика в сфері забезпечення кібербезпеки держави має враховувати, що правоохоронна система є як інструментом запобігання кіберзагрозам так і є об'єктом кіберзлочинів. Відповідно є необхідність забезпечення кібербезпеки як усіх правоохоронної системи, так і окремих правоохоронних органів чи операцій. Забезпечення кібербезпеки правоохоронної системи має відбуватися в контексті реалізації державної інформаційної політики та політики забезпечення інформаційної безпеки, що в цілому складає систему кібероборони.

Важливе значення щодо забезпечення кібербезпеки в країнах Європи приділяється власне принципам на яких має базуватися механізм забезпечення кібербехпеки держави в цілому та правоохоронної системи зокрема (табл. 5).

Таблиця 5 – Принципи забезпечення кібербезпеки в нормативних документах країн Європи

Нормативний акт	Принципи
Німеччина	
Стратегія кібербезпеки Німеччини (Cyber Security Strategy for Germany) [20]	узгодження набору інструментів для реагування на кібератаки;
	регулярна оцінка ситуації, ризиків та прийняття відповідних засобів захисту;
	регулярні тренування персоналу та тестування обладнання;
	зміцнення IT-безпеки в сфері держуправління
Естонія	
Стратегія кібербезпеки Естонії (Cyber Security Strategy) [21]	кібербезпека є невід'ємною частиною національної безпеки, підтримує функціонування держави і суспільства, конкурентоспроможність економіки та інновацій, забезпечується на основі принципу пропорційності, беручи до уваги існуючі та потенційні ризики і ресурси;
	гарантується дотриманням основних прав і свобод, а також захисту особистої інформації та особистості;
	починається з індивідуальної відповідальності за безпечне використання засобів ІКТ;
	підтримується інтенсивністю і конкурентоспроможністю досліджень і розвитку на міжнародному рівні;

Нормативний акт	Принципи
	забезпечується на узгодженій основі в рамках співпраці між державним, приватним та третім сектором, беручи до уваги взаємозв'язок і взаємозалежність існуючої інфраструктури і сервісів в кіберпросторі;
	забезпечується за допомогою міжнародного співробітництва з союзниками і партнерами
Польща	
Стратегія кібербезпеки Польщі (Cyberspace Protection Policy of the Republic of Poland) [22]	законодавчих заходів
	процедурних і організаційних заходів (система менеджменту)
	виховання, навчання та підвищення обізнаності в галузі безпеки
	технічних дій (збільшення кількості команд для реагування на інциденти безпеки у державних установах, тестування рівня безпеки, розвиток системи попередження, запобігання інцидентам і прийняття профілактичних рішень)
Чорногорія	
Стратегія кібербезпеки Чорногорії (Strategy on Cyber Security of Montenegro to 2017) [23]	визначення інституційної та організаційної структури в сфері кібербезпеки в державі
	захист критичних інформаційних структур,
	зміцнення потенціалу державних правоохоронних органів,
	реагування на інциденти,
	посилення ролі Міністерства оборони та військових Чорногорії в кіберпросторі,
	державно-приватне партнерство,
	підвищення обізнаності громадськості та захисту користувачів
Австрія	
Стратегія кібербезпеки Австрії (Austrian Cyber Security Strategy) [24]	дотримання закону,
	самоврегулювання,
	пропорційність,
	ієрархічність,
	конфіденційність,
	цілісність,
	автентичність,
	доступність,
	приватність
	захист даних
Угорщина	
Стратегія кібербезпеки Угорщини (National Cyber Security Strategy of Hungary) [25]	співпраця на різних рівнях
	підвищення рівня обізнаності та освіченості громадян в сфері кібербезпеки
	захист дітей у кіберпросторі
	розвиток нормативно-правової та технічної бази
	мотивація комерційного сектору

Складовими механізму державної політики забезпечення кібербезпеки правоохоронної системи є наступні (табл.6):

- вихідні положення механізму забезпечення кібербезпеки: об'єкти та суб'єкти кібербезпеки, принципи забезпечення кібербезпеки правоохоронної системи; завдання механізму;

- порядок забезпечення кібербезпеки правоохоронної системи України: нормативне організаційне, фінансове, матеріально-технічне забезпечення; заходи із забезпечення кібербезпеки правоохоронної системи; система обміну інформацією між правоохоронними

органами, суб'єктами державного управління, органами місцевого самоврядування, міжнародними поліцейськими організаціями, правоохоронними органами зарубіжних країн;

- порядок забезпечення кібербезпеки правоохоронного органу: нормативне організаційне, фінансове, матеріально-технічне забезпечення; заходи із забезпечення кібербезпеки правоохоронної системи; система обміну інформацією між співробітниками правоохоронного органу;

- порядок оцінки кіберзагроз та рівня кібербезпеки, моніторинг та контроль за реалізацією заходів забезпечення кібербезпеки правоохоронної системи.

Таблиця 6 – Механізм забезпечення кібербезпеки правоохоронної системи

<table>
<tr><td colspan="5">1. ВИХІДНІ ПОЛОЖЕННЯ МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПРАВООХОРОННОЇ СИСТЕМИ</td></tr>
<tr><td colspan="5">Об'єкти механізму забезпечення кібербезпеки правоохоронної системи</td></tr>
<tr><td colspan="2">Об'єкти кібербезпеки</td><td colspan="3">Об'єкти кіберзахисту</td></tr>
<tr><td>Діяльність правоохоронних органів</td><td>Діяльність суб'єктів формування державної політики</td><td>Комунікаційні системи правоохоронної системи</td><td colspan="2">Відомчі комунікаційні системи правоохоронної системи</td></tr>
<tr><td>Публічні, приватні та суспільні інтереси</td><td>Конституційні права і свободи людини і громадянина</td><td>Комунікаційні системи правоохоронного органу</td><td colspan="2">Комунікаційні системи міжнародних правоохоронних органів</td></tr>
<tr><td>Професійна діяльність правоохоронців</td><td>Інтереси членів сімей правоохоронців</td><td colspan="3">Об'єкти критичної інформаційної інфраструктури правоохоронної системи та / або правоохоронного органу</td></tr>
<tr><td>Об'єкти інфраструктури правоохоронної системи</td><td>Особисті дані правоохоронців та громадян</td><td colspan="3">Комунікаційні системи розвідувальної діяльності правоохоронних органів</td></tr>
<tr><td colspan="5">Суб'єкти забезпечення кібербезпеки правоохоронної системи</td></tr>
<tr><td colspan="2">Суб'єкти забезпечення кібербезпеки держави</td><td colspan="3">Суб'єкти забезпечення кібербезпеки правоохоронної системи</td></tr>
<tr><td colspan="2">Міністерство цифрової трансформації України</td><td>Міністерство внутрішніх справ України</td><td>Відділи інформаційних мереж правоохоронних органів</td><td>Відділи моніторингу за контролю за заходами протидії кіберзагрозам</td></tr>
<tr><td colspan="2">Кіберполіція</td><td>Служба безпеки України</td><td></td><td rowspan="2"></td></tr>
<tr><td colspan="2">Держслужба спеціального зв'язку та захисту інформації України</td><td>Міністерство оборони України та Генеральний штаб ЗСУ</td><td>Служби внутрішньої безпеки</td></tr>
<tr><td colspan="5">Принципи механізму забезпечення кібербезпеки</td></tr>
<tr><td>Законність</td><td>Ієрархічність</td><td>Конфіденційність</td><td colspan="2">Доступність</td></tr>
<tr><td>Приватність</td><td>Захист даний</td><td>Комплексність</td><td colspan="2">Систематичність</td></tr>
<tr><td>Незалежність</td><td>Керованість</td><td>Комунікативність</td><td colspan="2">Мінливість</td></tr>
<tr><td>Динамічності</td><td>Професійності</td><td></td><td colspan="2"></td></tr>
<tr><td colspan="5">Завдання механізму забезпечення кібербезпеки правоохоронної системи</td></tr>
<tr><td colspan="2">1. Протидія кіберзагрозам правоохоронній системі</td><td colspan="2">2. Забезпечення обмеженого доступу до даних правоохоронних органів</td><td>3. Забезпечення безпеки даних про оперативно-розшукові заходи</td></tr>
<tr><td colspan="2">4. Забезпечення безпеки даних про слідчі дії</td><td colspan="2">5. Забезпечення безпеки особистих даних свідків, підозрюваних, звинувачених</td><td>6. Забезпечення безпеки особистих даних співробітників правоохоронних органів</td></tr>
<tr><td colspan="2">7. Формування системи моніторингу та реагування на кіберзагрози</td><td colspan="2">8. Формування забезпечення реалізації механізму</td><td>9. Здійснення оцінки ефективності заходів забезпечення кібербезпеки</td></tr>
<tr><td colspan="5">2. ПОРЯДОК ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПРАВООХОРОННОЇ СИСТЕМИ УКРАЇНИ</td></tr>
<tr><td colspan="2">1. Оцінка кібербезпеки, кіберзахисту правоохоронної системи в цілому</td><td colspan="2">2. Оцінка потенційних кіберзагроз на майбутні періоди</td><td>3. Формування Стратегії забезпечення кібербезпеки правоохоронної системи</td></tr>
</table>

Суб'єкти реалізації процесу		
Можливі варіанти: А. Спільна діяльність державних суб'єктів, що забезпечують кібербезпеку; Б. Залучення приватних сектору В. Партнерство державних та приватних структур Г. Залучення міжнародних інституцій	***Можливі варіанти:*** А. Спільна діяльність державних суб'єктів, що забезпечують кібербезпеку; Б. Залучення приватних сектору В. Партнерство державних та приватних структур Г. Залучення міжнародних інституцій	1) Суб'єкти, що реалізують політику в сфері правоохоронної діяльності; 2) Суб'єкти, що реалізують державну політику в сфері кібербезпеки; 3) Суб'єкти, що реалізують державну політику в сфері національної безпеки; 4) Правоохоронні органи
Забезпечення реалізації процесу		
- фінансування Державним бюджетом; - фінансування за рахунок міжнародної допомоги; - спільне фінансування із залучення приватних ресурсів	- фінансування Державним бюджетом; - фінансування за рахунок міжнародної допомоги; - спільне фінансування із залучення приватних ресурсів	- фінансування Державним бюджетом; - фінансування за рахунок міжнародної допомоги; - спільне фінансування із залучення приватних ресурсів
Результативний документ		
Звіт про оцінку кібербезпеки та кіберзахисту правоохоронної системи, що включає аналіз критичних точок, визначає шляхи здійснення хакерських атак, точки безконтрольного доступу, аналіз та оцінку харакенрських атак за останні 5-ть років, характеристика програмного забезпечення, що було придбано за період	Звіт про оцінку кіберзагроз, що містить результати тестування інформаційної системи правоохоронної діяльності, аналіз розвитку кіберпростору та кіберзлочинності в Україні та Світі, оцінку хакерських атак в Україні та Світі, діяльність хакерських груп, та оцінку інших загроз Національній безпеці	Стратегія забезпечення кібербезпеки правоохоронної системи, що має відображати: результати оцінку кібербезпеки, кіберзахисту правоохоронної системи; оцінку потенційних кіберзагроз; сукупність заходів щодо протидії кібезагрозам; удосконалення інфраструктури забезпечення кіберзахисту; суб'єктів реалізації; джерела та напрями забезпечення реалізації Стратегії
4. Впровадження заходів забезпечення кіберзахисту	**5. Впровадження системи постійного моніто-рингу за кібербезпекою**	**6. Контроль за реалізацією Стратегії та оцінка ефективності заходів**
Суб'єкти реалізації процесу		
1) Міністерство цифрової трансформації; 2) Відділи інформаційних мереж правоохоронних органів; 3) Відділи моніторингу за контролю за заходами протидії кіберзагрозам; 4) Кіберполіція; 5) Держслужба спеціального зв'язку та захисту інформації України; 6) Служби внутрішньої безпеки	1) Створити Державне підприємство, основним видом діяльності якого буде моніторинг кіберпростору, у підпорядкуванні Міністерству цифрової трансформації 2) Служби внутрішньої безпеки 3) Кіберполіція 4) Керівники правоохоронних органів та їх заступники; 5) Кабінет Міністрів України	1) Офіс Президента України; 2) Кабінет Міністрів України; 3) Міністерство внутрішніх справ; 4) Міністерство цифрової трансформації; 5) Керівники правоохоронних органів та їх заступники; 6) Міжнародні інституції, що фінансуватимуть реалізацію стратегії; 7) Приватні інституції на правах аутсорсингу
Забезпечення реалізації процесу		
- фінансування Державним бюджетом; - фінансування за рахунок міжнародної допомоги; - спільне фінансування із залучення приватних ресурсів	- фінансування Державним бюджетом; - фінансування за рахунок міжнародної допомоги	- фінансування Державним бюджетом
Результативний документ		
Звіт про реалізацію заходів забезпечення кібербезпеки, який надається суб'єктам реалізації державної політики в сферах правоохоронної системи, кібербезпеки національної безпеки. Звіт має містити інформацію про	Пояснювальні записки щодо: - кібератак на правоохоронну систему; - заходи щодо протидії кібератакам; - виявленні критичні точки та можливий витік інформації;	Звіт про заходи з реалізації стратегії, який містить інформацію про: заходи, що були реалізовані; відхилення та пояснення їх причин; ресурсне забезпечення та відхилення із причинами; коригування Стратегічних заходів

виконанні заходи, відхилення від запланованих з поясненням причин, витраченні ресурси	- наслідки витоку інформації для публічних, суспільних та приватних інтересів; - виявленні відхилень в реалізації стратегії	на наступні періоди; встановлення відповідальних осіб
3. ПОРЯДОК ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПРАВООХОРОННОГО ОРГАНУ		
1. Оцінка кібербезпеки та кіберзахисту правоохоронного органу	**2. Оцінка потенційних кіберзагроз на майбутні періоди**	**3. Формування нормативів забезпечення кібербезпеки**
Завдання: - аналіз критичних точок; - визначення шляхів здійснення хакерських атак; - ідентифікація найбільш вразливих місць; - аналіз та оцінка хакерських атак минулих періодів	*Завдання:* - тестування інформаційної системи; - аналіз розвитку кіберпростору та кіберзлочинності в Україні та Світі; - оцінка хакерських атак в Україні та Світі; - діяльність хакерських груп, та оцінку інших загроз Національній безпеці	*Завдання:* - розробка та впровадження Положення про кібербезпеку та кіберзахист правоохоронного органу; - впровадження Протоколу протидії хакерським атакам; - розробка та впровадження Положення про оцінку наслідків хакерським атакам
4. Організація системи кіберзахисту правоохоронного органу	**5. Організація безпеки особистих даних**	**6. Організація кібербпеки та кіберзахисту робочого місця**
Завдання: - оновлення матеріальної бази; - встановленні відповідальних осіб за забезпечення кіберзахисту; - організація постійного моніторингу за кіберзагрозами;	*Завдання:* - забезпечення безпеки особистих даних співробітників; - забезпечення безпеки особистих даних свідків; - забезпечення безпеки особистих даних підозрюваних	*Завдання:* - організація періодичного моніторингу за кіберзагрозами на робочому місці; - визначення порядку дій співробітника за умови хакерської атаки
6. Організація кібеззахисту процесів правоохоронної діяльності	**7. Організація системи спеціального зв'язку на випадок несанкціонованого проникнення в інформаційну систему**	**8. Впровадження протоколу знищення даних на випадок фізичного проникнення**
Завдання: - організація захисту каналів зв'язку між співробітниками під час оперативно-розшукової діяльності; - організація захисту каналів зв'язку під час розвідувальної діяльності	*Завдання:* - налагодження системи спеціального зв'язку між співробітниками; - налагодження системи спеціального зв'язку системи управління	*Завдання:* - порядок знищення матеріальних носіїв інформації

5. Висновки

Таким чином, на основі вивчення наукової літератури, аналізу вітчизняного та міжнародного законодавства в сфері забезпечення кібербезпеки, ідентифікації принципів впровадження стратегій забезпечення кібезрбепеки країн ЄС. Нами розроблений комплексний механізм забезпечення кібербезпеки правоохоронної системи. Особливістю даного механізму є те, що він враховує особливості як особливості кібербезпеки правоохоронної системи загалом так і правоохоронного органу зокрема. Щодо вихідних положень було обґрунтовано необхідність виділяти: об'єкти кібербезпеки (діяльність правоохоронних органів; діяльність суб'єктів формування державної політики; публічні, приватні та суспільні інтереси; конституційні права і свободи людини і громадянина; професійна діяльність правоохоронців; інтереси членів сімей правоохоронців; об'єкти інфраструктури правоохоронної системи; особисті дані правоохоронців та громадян) та об'єкти кіберзахисту (комунікаційні системи правоохоронної системи; відомчі комунікаційні системи правоохоронної системи; комунікаційні системи правоохоронного органу; комунікаційні системи міжнародних правоохоронних органів; об'єкти критичної інформаційної інфраструктури правоохоронної системи та / або

правоохоронного органу; комунікаційні системи розвідувальної діяльності правоохоронних органів). Суб'єктами забезпечення кібербезпеки правоохоронної системи запропоновано визначати: суб'єктів забезпечення кібербезпеки держави (Міністерство цифрової трансформації України; Міністерство внутрішніх справ України; Кіберполіція; Служба безпеки України; Держслужба спеціального зв'язку та захисту інформації України; Міністерство оборони України та Генеральний штаб ЗСУ) та суб'єктів забезпечення кібербезпеки правоохоронної системи (Відділи інформаційних мереж правоохоронних органів; Відділи моніторингу за контролю за заходами протидії кіберзагрозам; Служби внутрішньої безпеки). Принципами механізму забезпечення кібербезпеки правоохоронної системи є: законність, ієрархічність, конфіденційність, доступність, приватність, захист даний, комплексність, систематичність, незалежність, керованість, комунікативність, мінливість, динамічності, професійності. Обґрунтовано склад завдань механізму: протидія кіберзагрозам правоохоронній системі; забезпечення обмеженого доступу до даних правоохоронних органів; забезпечення безпеки даних про оперативно-розшукові заходи; забезпечення безпеки даних про слідчі дії; забезпечення безпеки особистих даних свідків, підозрюваних, звинувачених; забезпечення безпеки особистих даних співробітників правоохоронних органів; формування системи моніторингу та реагування на кіберзагрози; формування забезпечення реалізації механізму; здійснення оцінки ефективності заходів забезпечення кібербезпеки.

Запропонований порядок забезпечення кібербезпеки правоохоронної системи України включає наступні завдання: 1) Оцінка кібербезпеки, кіберзахисту правоохоронної системи в цілому; 2) Оцінка потенційних кіберзагроз на майбутні періоди; 3) Формування Стратегії забезпечення кібербзепеки правоохоронної системи; 4) Впровадження заходів забезпечення кіберзахисту; 5) Впровадження системи постійного моніторингу за кібербезпекою; 3) Контроль за реалізацією Стратегії та оцінка ефективності заходів. За кожним напрямом визначено суб'єктів, напрями забезпечення та результативний документ.

Порядок забезпечення кібербезпеки правоохоронного органу має наступні складові:

1) Оцінка кібербезпеки та кіберзахисту правоохоронного органу;
2) Оцінка потенційних кіберзагроз на майбутні періоди;
3) Формування нормативів забезпечення кібербезпеки;
4) Організація системи кіберзахисту правоохоронного органу;
5) Організація безпеки особистих даних;
6) Організація кібербезпеки та кіберзахисту робочого місця;
7) Організація кіберзахисту процесів правоохоронної діяльності;
8) Організація системи спеціального зв'язку на випадок несанкціонованого проникнення в інформаційну систему;
9). Впровадження протоколу знищення даних на випадок фізичного проникнення.

6. Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

7. Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Сліпченко Т. Кібербезпека як складова системи захисту національної безпеки: європейський досвід.

References

1. Slipchenko, T. (2020). Kiberbezpeka yak skladova systemy zakhystu natsionalnoi bezpeky: yevropeiskyi dosvid. Aktualni problemy

Актуальні проблеми правознавства. 2020. №1(21), С.128-0133 URL: http://dspace.wunu.edu.ua/bitstream/316497/38497/1/%D0%A1%D0%BB%D1%96%D0%BF%D1%87%D0%B5%D0%BD%D0%BA%D0%BE.pdf

2. Гусєва, В. О. Теоретичні основи методики розслідування злочинів проти авторитету органів державної влади у сфері правоохоронної діяльності: дис.... д-ра юрид. наук: 12.00. 09. МВС України, Харк. нац. ун-т внутр. справ. Харків (2021).
3. Білас А. І. Правоохоронна діяльність країн ЄС: порівняльно-правове дослідження: автореф. дис. … канд. юрид. наук: 12.00.01. Львів, 2016. 24 с.
4. Кучук А. М. Теоретико-правові засади правоохоронної діяльності в Україні: автореф. дис. ... канд. юрид. наук (12.00.01). Київ, 2007. 22 с.
5. Лісовська Ю. П. Кібербезпека: ризики та заходи: навч. посібник. К.: Видавничий дім «Кондор», 2019. 272 с.
6. Стратегія кібербезпеки України (2021 – 2025 роки).Рада національної безпеки і оборони. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf
7. Капля А. В. Кібербезпека як важливий аспект сьогодення. Конференції Державного університету «Житомирська політехніка». URL: https://conf.ztu.edu.ua/wp-content/uploads/2021/01/29-2.pdf
8. Сидоржевський М. Кіберзлочини у 2020 році завдали збитків на трильйон доларів. Медіакомпанія DW. URL: https://www.dw.com/uk/kiberzlochyny-u-2020-rotsi-zavdaly-svitu-zbytkiv-na-trylion-dolariv-doslidzhennia/a-55857766
9. Вадовський В. Кіберзлочинність в Україні: найпоширеніші злочини та як громадянам подбати про власну інформаційну безпеку. Equity.2021 URL: https://equity.law/press-center/publications/1169.html

pravoznavstva [Cyber security as a component of the national security protection system: European experience. Actual problems of jurisprudence], (Vyp. 1 (21)), 128–133. Available from : http://dspace.wunu.edu.ua/bitstream/316497/38497/1/%D0%A1%D0%BB%D1%96%D0%BF%D1%87%D0%B5%D0%BD%D0%BA%D0%BE.pdf

2. Husieva, V. O. Teoretychni osnovy metodyky rozsliduvannia zlochyniv proty avtorytetu orhaniv derzhavnoi vlady u sferi pravookhoronnoi diialnosti [Theoretical foundations of the methodology of investigating crimes against the authority of state authorities in the field of law enforcement]: dys.... d-ra yuryd. nauk: 12.00. 09. MVS Ukrainy, Khark. nats. un-t vnutr. sprav. Kharkiv (2021).
3. Bilas A. I (2016). Pravookhoronna diialnist krain YeS: porivnialno-pravove doslidzhennia [Law enforcement activities of the EU countries: a comparative legal study]: avtoref. dys....kand. yuryd. nauk: 12.00.01. Lviv, 2016. 24 s.
4. Kuchuk A. M. (2007). Teoretyko-pravovi zasady pravookhoronnoi diialnosti v Ukraini [Theoretical and legal foundations of law enforcement activities in Ukraine]: avtoref. dys. ... kand. yuryd. nauk (12.00.01). Kyiv, 22 s.
5. Lisovska Yu. P. Cyber security: risks and measures: training. manual. Kyiv: Kondor Publishing House, 2019. 272 p.
6. Pro Stratehiiu kiberbezpeky Ukrainy, Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy (2021) (Ukraina). Available from : https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf
7. Kaplia, A. V. (2021, 29 sichnia). Kiberbezpeka yak vazhlyvyi aspekt sohodennia. Konferentsii Derzhavnoho universytetu «Zhytomyrska politekhnika». Available from : https://conf.ztu.edu.ua/wp-content/uploads/2021/01/29-2.pdf
8. Cydorzhevs'kyj M. (2020). Kiberzlochyny u 2020 rotsi zavdaly zbytkiv na tryl'jon dolariv. Media company DW. Available from : https://www.dw.com/uk/kiberzlochyny-u-2020-rotsi-zavdaly-svitu-zbytkiv-na-trylion-dolariv-doslidzhennia/a-55857766 [in Ukrainian].
9. Vadovs'kyj V. (2021). Kiberzlochynnist' v Ukraini: najposhyrenishi zlochyny ta iak

10. Звіт Голови Національної поліції України про результати роботи відомства у 2019 році. Національна поліція України. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2019/zvit-npu-2019.pdf
11. Крутов М. Пустощі чи прелюдія до війни? Хакерські атаки на Україну. Радіо Свобода. URL: https://www.radiosvoboda.org/a/khakerski-ataky-na-ukrayinu/31709601.html
12. Дума В., Цимбалюк В. Правозастосування та форми його здійснення. Правова інформатика. 2006. № 3(11). С. 61-64.
13. Кількість хакерських атак за місяць війни зросла утричі, але більшість з них неуспішні, – Держспецзв'язку. Еспресо. URL: https://espreso.tv/kilkist-khakerskikh-atak-za-misyats-viyni-zrosla-utrichi-ale-bilshist-z-nikh-neuspishni-derzhspetszvyazku
14. Країни-жертви та країни-агресори у хакерських війнах. Слово і діло. Аналітичний портал. URL: https://www.slovoidilo.ua/2021/10/22/infografika/svit/krayiny-zhertvy-ta-krayiny-ahresory-xakerskyx-vijnax
15. Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575/conv#o39
16. Бухарєв В. В. Адміністративно-правові засади забезпечення кібербезпеки України: дисертація на здобуття наукового ступеня кандидата юридичних наук. Суми. 2018. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/70638/1/diss_Bukhariev.pdf
17. Шахова О., Лозова І., Гнатюк С. Рекомендації щодо розробки стратегії забезпечення кібербезпеки України. Захист інформації. 18/1, 2016, URL: https://dspace.nau.edu.ua/bitstream/NAU/36065/1/10113-26205-1-SM.pdf
18. Про основні засади забезпечення кібербезпеки України: Закон України. URL: hromadianam podbaty pro vlasnu informatsijnu bezpeku. Equity. Available from : https://equity.law/press-center/publications/1169.html
10. Zvit Holovy Natsional'noi politsii Ukrainy pro rezul'taty roboty vidomstva u 2019 rotsi. Natsional'na politsiia Ukrainy. Available from :https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2019/zvit-npu-2019.pdf
11. Krutov M.(2022). Pustoschi chy preliudiia do vijny? Khakers'ki ataky na Ukrainu Radio Svoboda. Available from : https://www.radiosvoboda.org/a/khakerski-ataky-na-ukrayinu/31709601.html
12. Duma V., Tsymbaliuk V.(2006). Pravozastosuvannia ta formy joho zdijsnennia Pravova informatyka. 3(11),61-64.
13. Kil'kist' khakers'kykh atak za misiats' vijny zrosla utrychi, ale bil'shist' z nykh neuspishni, – Derzhspetszv'iazku. Espreso. Available from : https://espreso.tv/kilkist-khakerskikh-atak-za-misyats-viyni-zrosla-utrichi-ale-bilshist-z-nikh-neuspishni-derzhspetszvyazku
14. Krainy-zhertvy ta krainy-ahresory u khakerskykh viinakh. (b. d.). Slovo i Dilo. Available from : https://www.slovoidilo.ua/2021/10/22/infografika/svit/krayiny-zhertvy-ta-krayiny-ahresory-xakerskyx-vijnax
15. Konventsiia pro kiberzlochynnist. (b. d.). Ofitsiinyi vebportal parlamentu Ukrainy. Available from : https://zakon.rada.gov.ua/laws/show/994_575/conv#o39
16. Bukhariev, V. V. (2018). Administratyvno-pravovi zasady zabezpechennia kiberbezpeky Ukrainy [Master's thesis, Sumskyi derzhavnyi universytet]. eSSUIR – Electronic Sumy State University Institutional Repository. Available from : http://essuir.sumdu.edu.ua/handle/123456789/69047
17. Shakhoval, O. A., Lozova, I. L., & Hnatiuk, S. O. (2016). Recommendations for cybersecurity strategy of Ukraine development. *Ukrainian Information Security Research Journal*, 18(1). https://doi.org/10.18372/2410-7840.18.10113
18. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy, Zakon Ukrainy № 2163-VIII (2022) (Ukraina). Available from :

https://zakon.rada.gov.ua/laws/show/2163-19/conv#n94
19. Кримінальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
20. Cyber Security Strategy for Germany. Federal Ministry of the Interior. Berlin, 2011. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile
21. Cyber Security Strategy of Estonia. Ministry of Economic Affairs and Communication. 2014. URL: https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf
22. Cyberspace Protection Policy of the Republic of Poland. Ministry of Administration and Digitisation, Internal Security Agency. Warsaw, 2013. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-securitystrategies-ncsss/copy_of_PO_NCSS.pdf
23. Strategy on Cyber Security of Montenegro to 2017. Podgorica, 2013. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-securitystrategies-ncsss/CyberSecurityStrategyforMontenegro.pdf
24. Austrian Cyber Security Strategy. Vienna, 2013. URL: https://www.bka.gv.at/DocView.axd?CobId=50999
25. National Cyber Security Strategy of Hungary. Prime Minister's Office. Budapest, 2013. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-securitystrategies-ncsss/HU_NCSS.pdf

https://zakon.rada.gov.ua/laws/show/2163-19#Text
19. Kryminalnyi kodeks Ukrainy, Kodeks Ukrainy № 2341-III (2023) (Ukraina). Available from : https://zakon.rada.gov.ua/laws/show/2341-14#Text
20. Cyber Security Strategy for Germany. Federal Ministry of the Interior. (2011), Berlin. Available from : https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile
21. Cyber Security Strategy of Estonia. Ministry of Economic Affairs and Communication.(2014). Available from : https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf
22. Cyberspace Protection Policy of the Republic of Poland. (2013). Ministry of Administration and Digitisation, Internal Security Agency. Warsaw. Available from : https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-securitystrategies-ncsss/copy_of_PO_NCSS.pdf
23. Strategy on Cyber Security of Montenegro to 2017. (2013) Podgorica. Available from : https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-securitystrategies-ncsss/CyberSecurityStrategyforMontenegro.pdf
24. Austrian Cyber Security Strategy. (2013). Vienna Available from : https://www.bka.gv.at/DocView.axd?CobId=50999
25. National Cyber Security Strategy of Hungary.(2013) Prime Minister's Office. Budapest. Available from : https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-securitystrategies-ncsss/HU_NCSS.pdf