УДК 342. 52 **DOI:** https://doi.org/10.32631/v.2021.4.12

Станіслав Геннадійович Петров,
доктор юридичних наук,
Науково-дослідний центр
Інституту спеціального зв'язку та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»;
https://orcid.org/0000-0001-7786-4657,
e-mail: kibpetrov@gmail.com

РОЗБУДОВА НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ ЯК НЕОБХІДНИЙ ЕЛЕМЕНТ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

У статті досліджено сучасні проблеми розбудови національної системи кібербезпеки України. У зв'язку з появою нових викликів та загроз у кіберпросторі виникає необхідність пошуку нових методів і способів протидії кіберзлочинності та кібертероризму. Обґрунтовано необхідність в умовах зростання кількості й складності кіберзлочинів посилення міжнародної співпраці та вдосконалення чинного законодавства.

Ключові слова: кібербезпека, кіберзагрози, кіберстійкість, об'єкти критичної інфраструктури, міжнародне співробітництво.

Оглядова стаття

Постановка проблеми

В Україні активно формується інформаційне суспільство в інтересах громадян і бізнесу з метою інтеграції до європейської інформаційної спільноти. Активно вдосконалюється нормативно-правова база у сфері інформаційних технологій, а з 1 грудня 2021 р. у Верховній Раді України навіть створено міжфракційне депутатське об'єднання «Цифрова країна», метою якого є активне просування сучасних цифрових технологій. Це дасть змогу прискорити імплементацію сучасного законодавства ЄС у сфері цифровізації, а також сприятиме розвитку економіки та подоланню корупції.

Водночас розвитку інформаційного суспільства загрожує збільшення кількості кіберзагроз та їх інтенсивність. У новій Стратегії кібербезпеки України прогнозується зростання інтенсивності міждержавного протиборства й розвідувально-підривної діяльності у кіберпросторі, розширюється коло держав, які намагаються сформувати власну кіберрозвідку, оволодіти сучасними технологіями

розвідувально-підривної діяльності у кіберпросторі, посилюють державний контроль за національними сегментами мережі Інтернет[1].

Зазначені тенденції вимагають якнайшвидшого прийняття адекватних заходів протидії вчиненню актів кібертероризму, боротьби з кіберзлочинністю, поширенню дезінформації шляхом посилення спроможностей суб'єктів забезпечення кібербезпеки, досягнення необхідного рівня кіберстійкості, особливо на об'єктах критичної інфраструктури, поглиблення міжнародного співробітництва у сфері кібербезпеки та кібероборони.

Стан дослідження проблеми

Питанням посилення кібербезпеки останніми роками присвятили свої праці науковці з різних галузей науки і техніки. Слід відзначити таких дослідників, як П. Д. Біленчук [1], В. Л. Бурячок [2], М. В. Гуцалюк [3], О. В. Корнейко [4], А. І. Марущак [5], Н. А. Ткачук [6] та інші.

Водночас сучасний розвиток технологій, зростання кількості нових кіберзагроз, складність кібератак потребують нових підходів до підвищення ефективності кіберзахисту інформаційних ресурсів і протидії кіберзлочинності.

Мета і завдання дослідження

Метою статті є розкриття особливостей розбудови національної системи кібербезпеки України у контексті розвитку інформаційного суспільства. Задля досягнення мети поставлено такі *завдання*: обґрунтувати необхідність посилення спроможності й ефективної взаємодії основних суб'єктів системи кібербезпеки України для захисту суверенітету та розвитку інформаційного суспільства в нашій державі на основі аналізу вітчизняного та міжнародного законодавства, а також навести приклади правозастосування в цій сфері.

Наукова новизна дослідження

У дослідженні зроблено спробу проаналізувати сучасний стан протидії кіберзагрозам і надати пропозиції щодо вдосконалення законодавства у сфері кібербезпеки та кіберзахисту.

Виклад основного матеріалу

Через переведення багатьох працівників на віддалений режим роботи кількість кіберінцидентів у розвинутих країнах значно зросла після поширення вірусу COVID-19. Серед кіберзагроз особливо небезпечними залишаються кібератаки на основі вірусів-вимагачів (ransomware).

[1] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021 // Президент України : офіц. сайт. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 15.12.2021).

За повідомленням агентства Рейтерс, у Сан-Франциско у липні 2021 р. відбулася атака на компанію «Kaseya» – розробника програмного забезпечення для віддаленого управління комп'ютерних мереж. Після поновлення програми «Kaseya» VSA, яке було направлене замовникам та містило вірус-вимагач, було паралізовано роботу близько 1500 організацій. На адресу «Kaseya» був направлений лист від зловмисників із вимогою виплати 70 млн доларів США. На думку експертів з кібербезпеки, це стало для кіберзлочинців початком інтенсивного пошуку подібних вразливостей в інших організаціях[1].

Унаслідок іншої кібератаки на електроенергетичну компанію штату Колорадо «Delta-Montrose Electric Association (DMEA)» було знищено всі дані із системи розрахунків зі споживачами за останні 25 років. Через кібератаку компанії довелося відключити 90 % своїх внутрішніх комп'ютерних систем[2].

Подібні атаки здійснювалися на об'єкти критичної інфраструктури України, зокрема у грудні 2015 р. були здійснені кібератаки на енергетичні компанії України. Найбільше постраждали споживачі «Прикарпаттяобленерго» (було вимкнено близько 30 підстанцій, близько 230 тис. мешканців залишались без світла протягом однієї-шести годин)[3].

Також особливе занепокоєння викликають кібератаки на виборчий процес у різних країнах світу. Під час президентських виборів 2014 р. в Україні російські хакери на 20 годин вивели з ладу інформаційну систему ЦВК України «Вибори». Вони намагалися скомпрометувати результати виборів у пропагандистських цілях, вивівши лідера партії «Правий сектор» Дмитра Яроша на перше місце[4].

У квітні 2016 р. було виявлено несанкціоноване втручання в інформаційну виборчу систему США. У результаті проведеного розслідування було встановлено, що кібератаки здійснювали два угрупування російських хакерів – «Cozy Bear» (CozyDuke або APT29) та

[1] Kaseya ransomware attack sets off race to hack service providers–researchers // REUTERS : сайт. 03.08.2021. URL: https://www.reuters.com/technology/kaseya-ransomware-attack-sets-off-race-hack-service-providers-researchers-2021-08-03/ (дата звернення: 15.12.2021).

[2] Utility biz Delta-Montrose Electric Association loses billing capability and two decades of records after cyber attack // The Register : сайт. 03.12.2021. URL: https://www.theregister.com/2021/12/03/dmea_colorado_cyber_attack_billing_systems/ (дата звернення: 15.12.2021).

[3] Після кібератаки на «Прикарпаттяобленерго» в США переглянуть захист енергомереж // DW : сайт. 07.01.2016. URL: https://www.dw.com/uk/a-18964517 (дата звернення: 15.12.2021).

[4] Кібератаки Російської Федерації. Хронологія // Міністерство оборони України : офіц. сайт. 07.05.2018. URL: https://www.mil.gov.ua/ukbs/kiberataki-rosijskoi-federaczii-hronologiya.html (дата звернення: 15.12.2021).

«Fancy Bear» (Sofacy Group або APT28). Група «Cozy Bear» отримала несанкціонований доступ до інформаційної системи ще влітку 2015 р., а «Fancy Bear» – у квітні 2016 р.[1] Як свідчать матеріали розслідувань, за подібними кібератаками стоять не просто злочинні угруповання, а добре організовані професійні хакери, діяльність яких підтримується державними структурами РФ.

Нещодавно фахівці СБУ із кібербезпеки ідентифікували хакерів російського угрупування «Armageddon/Gamaredon», які під керівництвом 18-го Центру ФСБ РФ (Москва) здійснили з 2014 р. понад 5000 атак проти України. За даними спецслужби, зловмисниками виявились офіцери ФСБ у тимчасово окупованому Криму, а також зрадники, які перейшли на півострові на бік ворога. Їх встановили поіменно, перехопили телефонні розмови, а також отримали докази щодо їхньої причетності до кібератак. Основними їхніми цілями були: контроль над об'єктами критичної інфраструктури (електростанції, системи тепло- та водопостачання); викрадення та збирання розвідданих, включно із секретною інформацією (сектор безпеки та оборони, держустанови); проведення акцій інформаційно-психологічного впливу / пропаганди; блокування інформаційних систем[2].

Зазначені приклади змушують шукати нові методи протидії діяльності організованих злочинних кіберугруповань та кібертерористів, а особливо підрозділів спецслужб іноземних держав, передусім РФ, які інтенсивно нарощують кіберзброю та можуть здійснювати деструктивний вплив на безпековий сектор нашої держави й об'єкти критичної інфраструктури.

Як відомо, основними суб'єктами національної системи кібербезпеки відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які відповідно до законів виконують в установленому порядку основні завдання щодо запобігання, виявлення, припинення правопорушень у кіберпросторі, захисту прав і свобод

[1] Кібератака на Національний комітет Демократичної партії США // Вікіпедія : віл. енцикл. URL: https://uk.wikipedia.org/wiki/Кібератака_на_Національний_комітет_Демократичної_партії_США (дата звернення: 15.12.2021).

[2] Армагеддон скасовується. Кіберспеціалісти СБУ розкрили хакерів ФСБ РФ – ті атакували із Криму // ЛІГА.НОВИНИ : сайт. 04.11.2021. URL: https://news.liga.net/ua/politics/news/armageddon-otmenyaetsya-kiberspetsy-sbu-raskryli-hakerov-fsb-takje-iz-predateley-v-krymu (дата звернення: 15.12.2021).

людини та громадянина, інтересів суспільства і держави, здійснюють заходи з підготовки держави до відбиття воєнної агресії в кіберпросторі (кібероборони) [3]. Водночас у зв'язку з поширенням ландшафту загроз і мілітаризації кіберпростору національна система кібербезпеки потребує певного реформування для більш ефективної діяльності відповідно до визначених напрямів.

Відповідно до Указу Президента України «Про рішення Ради національної безпеки і оборони України від 22 жовтня 2021 року "Про Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України"», зокрема, передбачається до 2025 р.:

– розширення функціональних можливостей Національної телекомунікаційної мережі, що дасть можливість забезпечити інтеграцію наявних систем спеціального зв'язку та уніфікацію захищених електронних комунікацій різних державних органів у загальному безпековому контурі з використанням сучасних цифрових технологій;

– розширення напрямів співробітництва з Організацією Північноатлантичного договору з метою набуття повноправного членства України в НАТО та забезпечення виконання національних зобов'язань щодо акредитації з питань безпеки національних комунікаційно-інформаційних систем, у яких обробляється інформація НАТО, з обмеженим доступом;

– розгортання системи кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури;

– захист національних інтересів у сфері безпеки та оборони, зниження ймовірності негативного впливу зовнішніх і внутрішніх чинників на телекомунікаційну складову системи управління державою, забезпечення кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури, зменшення втрат особового складу, озброєння та військової техніки тощо[1].

Указом Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави"» від 26 серпня 2021 р. № 446/2021 розпочато створення кібервійськ в Україні. Після проведення розрахунків щодо матеріально-технічного та кадрового забезпечення відповідних структур передбачено розробити та внести на розгляд Верховної Ради України законопроєкт щодо створення та

[1] Про рішення Ради національної безпеки і оборони України від 22 жовтня 2021 року «Про Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України» : Указ Президента України від 22.10.2021 № 544/2021 // Президент України : офіц. сайт. URL: https://www.president.gov.ua/documents/5442021-40437 (дата звернення: 15.12.2021).

функціонування у системі Міністерства оборони України кібервійськ[1].

У зв'язку із цим вбачається необхідним на законодавчому рівні чітко передбачити заходи кібероборони держави в мирний час та функції військових кіберпідрозділів під час ведення бойових дій, а також можливість превентивних кібератак і процедури приведення військ кібероборони до активних бойових дій. При цьому важливим залишається питання громадського контролю щодо діяльності кібервійськ, а також мобілізація наявних сил і засобів територіальних громад, у тому числі приватного сектора (провайдерів) для виконання завдань кібервійськ в особливий період. Безумовно, необхідною складовою кібероборони держави повинна бути взаємодія нових підрозділів з аналогічними службами країн НАТО.

У Проекті Закону про внесення змін до Закону України «Про Службу безпеки України» щодо удосконалення організаційно-правових засад діяльності Служби безпеки України визначено завдання щодо забезпечення державної безпеки у кіберпросторі, зокрема шляхом:

– протидії спеціальним інформаційним операціям і впливам спеціальних служб іноземних держав, організацій, груп та осіб;

– попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі;

– здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством;

– протидії кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України;

– розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога стосовно захисту якої встановлена законом, критичної інформаційної інфраструктури та її окремих об'єктів;

– здійснення тестування готовності захисту об'єктів критичної інформаційної інфраструктури до можливих кібератак та кіберінцидентів;

– забезпечення реагування на комп'ютерні інциденти у сфері державної безпеки тощо[2].

---

[1] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави» : Указ Президента України від 26.08.2021 № 446/2021 // Президент України : офіц. сайт. URL: https://www.president.gov.ua/documents/4462021-40009 (дата звернення: 15.12.2021).

[2] Проект Закону про внесення змін до Закону України «Про Службу безпеки України» щодо удосконалення організаційно-правових засад діяльності

Провідна роль у вивченні розвідувально-підривної діяльності спецслужб іноземних держав відводиться розвідувальним і контррозвідувальним органам України. Зазначені органи отримують інформацію про кіберрозвідки іноземних держав та інші джерела загроз національній безпеці у кіберпросторі (кібертероризм, кіберзлочинність тощо). Адже кібератаки, вмотивовані державою-агресором та спрямовані на викрадення інформації з обмеженим доступом, знищення або блокування доступу до них з метою отримання політичних, економічних, військових переваг у зовнішньополітичних стосунках, можуть бути вкрай небезпечними і загрожувати національній безпеці України.

При цьому підрозділи Служби зовнішньої розвідки (далі – СЗР) України можуть отримати дані про підготовку до злочинних посягань на кібербезпеку інформаційних ресурсів та їх інфраструктуру. Особливу увагу в діяльності СЗР України слід приділити питанням кібербезпеки закордонних дипломатичних установ України, адже вони постійно піддаються кібератакам із боку країни-агресора.

Слід зазначити, що ключову роль у виявленні та розслідуванні кіберзлочинів відіграє Національна поліція України, до складу якої входить департамент кіберполіції – міжрегіональний територіальний орган, який організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність і спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних інтернет-мереж і систем.

Діяльність Департаменту кіберполіції з 2015 р. постійно вдосконалюється, що позначається на ефективності його роботи. Нещодавно його працівниками спільно з Головним слідчим управлінням Національної поліції, представниками Офісу Генерального прокурора із залученням колег з Європолу, Євроюсту, правоохоронцями Республіки Франції, США, Нідерландів та Норвегії було викрито транснаціональне злочинне угруповання, яке завдало збитків іноземним компаніям на суму в 120 мільйонів доларів. Використовуючи програмне забезпечення типу ransomware, фігуранти здійснили атаки на понад 50 компаній у країнах Європи та Америки. За відновлення доступу до закриптованих даних вимагали викуп у криптовалюті. Фігуранти отримували контроль над комп'ютерними системами компаній,

Служби безпеки України : від 26.10.2020 № 3196-д / ініціатори О. М. Завітневич, М. В. Безугла, Ю. М. Мисягін та ін. // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70243 (дата звернення: 15.12.2021)

використовуючи їхні вразливості. Відкрито кримінальне провадження за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку), ч. 4 ст. 189 (Вимагання), ст. 209 (Легалізація (відмивання) майна, одержаного злочинним шляхом) Кримінального кодексу України[1].

Однією з проблем під час розслідування кіберзлочинів є те, що про проведену кібератаку власник інформаційної системи може не здогадуватися протягом значного часу. Комп'ютерні дані можуть бути змінені моментально (наприклад, для корегування повідомлень на вебсайті), знищені через декілька місяців (наприклад, під час певної політичної події) або взагалі не змінюватися, а лише передаватися певними каналами для викрадення інформації. Тобто з початку кібератаки для правоохоронців залишається невідомою мета кіберзлочинців. Тому не завжди визначеною є підслідність кіберінцидентів, особливо на об'єктах критичної інфраструктури.

Ухвалений Закон України «Про критичну інфраструктуру» передбачає створення уповноваженого органу у сфері захисту критичної інфраструктури, який буде здійснювати функціональне управління національною системою захисту критичної інфраструктури та забезпечуватиме координацію діяльності міністерств та операторів критичної інфраструктури з питань забезпечення стійкості та захисту таких об'єктів. Одним із першочергових завдань новоствореного державного органу повинно стати формування Реєстру об'єктів критичної інформаційної інфраструктури розслідування кіберзлочинів.

Також необхідно зазначити, що для ефективної протидії та нейтралізації кібератак необхідною умовою є своєчасна взаємодія та координація всіх суб'єктів забезпечення кібербезпеки, що може попередити настання аналогічних кіберінцидентів у різних інформаційних системах. Важливу роль у цьому процесі повинен відігравати Національний координаційний центр кібербезпеки при РНБО України.

Також особливо важливим питанням у сфері забезпечення кібербезпеки є налагодження ефективного міжнародного співробітництва. Одним з основних міжнародних документів, який використовується у кримінальних провадженнях, пов'язаних із кіберзлочинністю, є Конвенція про кіберзлочинність, підписана 20 років тому в Будапешті[2]. На сьогодні міжнародну угоду підписали 78 країн, співпраця є з більш ніж 150 країнами світу.

[1] Там само.

[2] Конвенція про кіберзлочинність : від 23.11.2001 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 15.12.2021).

У зазначеному документі, який був ратифікований Україною у вересні 2006 р., передбачено, що кожна Сторона призначає орган для здійснення контактів цілодобово впродовж тижня з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів в електронній формі, що стосуються кримінального правопорушення. Така допомога включає в себе сприяння або, якщо це дозволяється її внутрішньодержавним законодавством і практикою, пряме:

a) надання технічних порад;

b) збереження даних;

c) збирання доказів, надання юридичної інформації і встановлення місцезнаходження підозрюваних[1].

Відповідний контактний пункт 24/7 створено на базі Департаменту кіберполіції Національної поліції України.

Водночас отримання електронних доказів часто потребує більш швидкого реагування задля їх збереження та отримання. Тому Комітет Ради Європи з Конвенції про кіберзлочинність 12 квітня 2021 р. опублікував проєкт Другого додаткового протоколу до Конвенції про кіберзлочинність щодо посилення співпраці та розкриття електронних доказів, яким, зокрема, передбачається: пряма співпраця з постачальниками послуг (ст. 6) і суб'єктами, що надають доменне ім'я реєстраційні послуги (ст. 7), для розкриття інформації для ідентифікації підозрюваних; прискорені форми співпраці між Сторонами для розкриття інформації про абонентів та дані про рух (ст. 8); пришвидшена співпраця та розкриття інформації в надзвичайних ситуаціях (статті 9 та 10); додаткові інструменти взаємодопомоги (статті 11 та 12); захист даних та інші гарантії верховенства права (статті 13 та 14). Обговорення вказаних новацій та пропозиції своїх варіантів цього міжнародного нормативного акта повинні стати важливим етапом усіх зацікавлених суб'єктів протидії кіберзлочинності [7].

Крім держав – підписантів Конвенції про кіберзлочинність, необхідно поглиблювати співробітництво з такими міжнародними організаціями, як Європол, на базі якого створено Європейський центр із кіберзлочинності, та Інтерпол, який має значний досвід в організації спільних слідчих груп для проведення розслідувань в інтернет-просторі.

Також у зв'язку з інтеграцією України в європейську спільноту необхідна подальша співпраця з Агентством ЄС з кібербезпеки (ENISA), у тому числі з імплементації Директиви Європейського Парламенту і

[1] Там само.

Ради Європи 2016/1148 про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу, нова редакція якої була оприлюднена 16 грудня 2020 р. (revised NIS Directive or «NIS 2»)[1].

Висновки

Сьогодні Україна знаходиться в активній фазі реформування національної системи кібербезпеки та кіберзахисту. Зокрема, ухвалено низку нормативно-правових актів у зазначеній галузі, серед яких Стратегія кібербезпеки України на 2021–2025 роки, посилюються спроможності суб'єктів забезпечення кібербезпеки.

У зв'язку з посиленням кіберзагроз та новітніх викликів необхідним є чітке виконання запланованих Стратегією заходів та участь у процесі захисту кіберпростору усіх учасників інформаційного суспільства, адже відповідно до ст. 17 Конституції України захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу.

На законодавчому рівні доцільно передбачити заходи кібероборони держави в мирний час та функції військових кіберпідрозділів під час ведення бойових дій, а також можливість превентивних кібератак і процедури приведення військ кібероборони до активних бойових дій. З іншого боку, доцільно передбачити гарантії громадського контролю щодо діяльності кібервійськ.

Перспективами подальших наукових пошуків визначаємо питання закріплення в законодавстві та науковій практиці поняття «кіберправо».

Список бібліографічних посилань: 1. Біленчук П. Д., Обіход Т. В. Кібербезпека і засоби запобігання та протидії кіберзлочинності й кібертероризму. *Часопис Київського університету права.* 2018. № 3. С. 235–239. **2.** Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник. Київ, 2015. 288 с. **3.** Науково-практичний коментар Закону України «Про основні засади забезпечення кібербезпеки України». Станом на 1 січня 2019 року / за ред. М. В. Гребенюка. Київ, 2019. 220 с. **4.** Корнейко О. В., Хахановський В. Г. Основи забезпечення кібербезпеки, захисту інформації та протидії кіберзлочинності : метод. рек. Київ, 2019. 100 с. **5.** Марущак А. І., Петров С. Г. Сучасний стан розвитку національної системи кібербезпеки (на прикладі СБ України та

[1] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of Cybersecurity across the Union, repealing Directive (EU) 2016/1148 // European Union : сайт. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_14337_2021_INIT&from=EN (дата звернення: 15.12.2021).

Держспецз'вязку України). *Інформація і право.* 2020. № 2 (33). С. 77–84. **6.** Ткачук Н. А. Стан та проблемні питання реалізації Стратегії кібербезпеки України. *Інформація і право.* 2019. № 1 (28). С. 129–134. **7.** Гуцалюк М. В. Напрями посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю. *Інформація і право.* 2021. № 4 (39). С. 141–147. DOI: https://doi.org/10.37750/2616-6798.2021.4(39).248840.

Надійшла до редколегії 17.12.2021

Petrov S. H. Development of the national cybersecurity system of Ukraine as a necessary element of information society development

The article examines modern development problems of the national cybersecurity system of Ukraine. With the emergence of new challenges and threats in cyberspace, there is a need to find new methods and ways to combat cybercrime and cyberterrorism. The current state of the fight against cybercrime in Ukraine and the prospects for capacity building and reform of the main subjects in cybersecurity in Ukraine are outlined.

In the course of the research general philosophical, comparative and phenomenological methods were used. The aim of the article is to reveal the peculiarities of building the national cybersecurity system of Ukraine in the context of information society development. Among cyber threats, special attention is paid to cyberattacks based on ransomware viruses.

The need to implement the provisions of the Convention on Cybercrime, in particular in the context of the draft Second Additional Protocol to the Convention on Cybercrime to strengthen cooperation and disclosure of electronic evidence, in particular on direct cooperation with service providers (Article 6) and domain names registration services (Article 7), for the disclosure of information for the identification of suspects, accelerated forms of cooperation between the Parties for the disclosure of subscriber information and traffic data (Article 8), acceleration of cooperation and disclosure of information in emergencies (Articles 9 and 10). Attention is drawn to the unconditional fulfillment of the tasks of the new Cyber Security Strategy of Ukraine, especially those related to cyber protection of critical infrastructure. It is noted that at the legislative level it is advisable to provide for cyber defense measures in peacetime and the functions of military cyber units during hostilities, as well as the possibility of preventive cyberattacks and procedures for bringing cyber defense troops to active hostilities.

The necessity of strengthening international cooperation and improving the current legislation in the conditions of growing number and complexity of cybercrimes is substantiated.

Key words: cybersecurity, cyber threats, cyber resilience, critical infrastructure, international cooperation.