Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2024. № 5.

DOI: http://doi.org/10.32702/2307-2156.2024.5.3
УДК 351.865:004.946.5.056(477)

О. Я. Лазор,
д. держ. упр., професор,
професор кафедри публічного управління та адміністрування, Вінницький державний педагогічний університет імені Михайла Коцюбинського
ORCID ID: https://orcid.org/0000-0002-5989-8527
І. Г. Юник,
к. ю. н., доцент, доцент кафедри публічного управління та адміністрування, Вінницький державний педагогічний університет імені Михайла Коцюбинського
ORCID ID: https://orcid.org/0000-0002-0985-1800
А. М. Чемерпільська,
магістр публічного управління та адміністрування Вінницького державного педагогічного університету імені Михайла Коцюбинського

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ: ФОРМУВАННЯ ТА РОЗВИТОК

O. Lazor,
Doctor of Sciences in Public Administration, Professor,
Professor of the Department of Public Management and Administration, Vinnytsia Mykhailo Kotsiubynsky State Pedagogical University
I. Yunyk,
PhD in Law, Associate Professor of the Department of Public Management and Administration, Vinnytsia Mykhailo Kotsiubynsky State Pedagogical University
A. Chemerpilska,
Master's student of Public Management and Administration, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University

ORGANIZATIONAL AND LEGAL BASIS FOR ENSURING CYBER SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE FACILITIES IN UKRAINE: THEIR FORMATION AND DEVELOPMENT

У статті проаналізовано чинне законодавство України у сфері кібербезпеки об'єктів критичної інформаційної інфраструктури. Досліджено процес становлення Національної системи кібербезпеки та її структурних підрозділів, їх завдання та частково діяльність. Проведений аналіз становлення інституційної системи вказує на чималу кількість суб'єктів протидії загрозам у сфері кібербезпеки, що є частиною національної системи кібербезпеки. Такий підхід не сприяє ефективному функціонуванню цієї системи, можливості чіткого визначення суб'єктності реалізації тих чи інших заходів, критеріїв їх виконання, рівня відповідальності суб'єкта тощо.

Пропонується об'єкти критичної інфраструктури визначати як «стратегічні, небезпечні або життєзабезпечувальні об'єкти незалежно від форми власності». Необхідно зазначити про відсутність розробленої методики оцінки стану об'єкту критичної інфраструктури, чітких критеріїв розмежування категорій критичності об'єктів критичної інформаційної інфраструктури.

Затверджена «Стратегія національної безпеки України» (2020 р.) дає реальну оцінку викликам і загрозам безпеці, розставляє пріоритети політики у цій сфері, основні засади якої: стримування, стійкість та взаємодія. Означені засади закладають модель, за якою має розвиватися весь сектор безпеки та оборони держави. Посилення спроможностей національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі – є одним із пріоритетних напрямків дій держави.

Важливість кіберпростору підтверджується створенням спеціальних структур у складі збройних сил країн світу. Незважаючи на усвідомлення ролі та важливості кібербезпекової складової в системі забезпечення національної безпеки держави де-юре, де-факто – очевидна відсутність належної координації діяльності відповідних відомств та узгодженості дій з функціонування як окремих елементів системи кібербезпеки, так і загалом її як системи з боку Національного координаційного центру кібербезпеки як загальнонаціональної координаційної структури.

The current legislation of Ukraine in the field of cybersecurity of critical information infrastructure facilities is analyzed.

The process of formation of the National Cyber Security System and its structural divisions, their tasks and partly their activities have been studied. The

analysis of the formation of the institutional system indicates a large number of subjects countering threats in the field of cybersecurity that are part of the National Cybersecurity System. This approach does not contribute to the effective functioning of this system, the possibility of clearly determining the subjectivity of the implementation of certain measures, the criteria for their implementation, the level of responsibility of the subject, etc.

It is proposed to define critical infrastructure facilities as "strategic, dangerous or life-supporting facilities, regardless of the form of ownership." It is necessary to note the lack of a developed methodology for assessing the condition of a critical infrastructure object, clear criteria for delimiting the categories of criticality of critical information infrastructure objects.

The approved "National Security Strategy of Ukraine" (2020) gives a realistic assessment of security challenges and threats, sets policy priorities in this area, the main principles of which are deterrence, sustainability and interaction. These principles lay down the model according to which the entire security and defense sector of the state should develop. Strengthening the capabilities of the national cybersecurity system to effectively counter cyber threats in the modern security environment is one of the priority areas of government action identified in the Strategy.

The importance of cyberspace is confirmed by the creation of special structures within the armed forces of the world. Despite the awareness of the role and importance of cybersecurity in the system of ensuring the national security of the state is de jure, de facto an obvious lack of proper coordination of the activities of the relevant departments and coordination of actions on the functioning of both individual elements of the cybersecurity system and as a system as a whole on the part of the National Coordination cybersecurity center as a national coordination structure.

Ключові слова: *об'єкти критичної інфраструктури, інформаційна інфраструктура, оцінка ризиків, система кібербезпеки, система кіберзахисту, національна безпека.*

Keywords: *critical infrastructure facilities, information infrastructure, risk assessment, cybersecurity system, cyber defense system, national security.*

Постановка проблеми. Сучасні виклики та загрози, пов'язані з розбудовою інформаційного суспільства, розвитком інформаційно-

комунікативних технологій та й загалом глобальної мережі Інтернет – зумовлюють необхідність підвищення рівня інформаційної та кібернетичної безпеки об'єктів критичної інфраструктури (далі – ОКІ), протидії кіберзлочинності та кібератакам, формування ефективного захисту в означеній сфері. Як і більшість країн світу, Україна, намагається здійснювати впевнені кроки на всіх рівнях кібербезпеки ОКІ, які задля ефективного функціонування системи кібербезпеки необхідно вдосконалювати постійно.

Щодалі частіше дискутуються питання взаємодії влади та бізнесу стосовно формування та дієвості національної системи кібербезпеки як однієї з основних складових цифровізації суспільства та держави, економіки та бізнесу. Адже кіберврразливість ОКІ може бути подолана лише за умови ефективної взаємодії та партнерства всіх учасників кіберпростору.

Метою публікації є дослідження трансформації організаційно-правових засад кібербезпеки ОКІ України та напрямів їх удосконалення.

Аналіз останніх досліджень. Проблематика кібербезпеки дедалі частіше стає предметом досліджень як вітчизняних, так і зарубіжних науковців за різними напрямками, що зумовлено викликами часу. Чимало наукових публікацій приділено питанням: кібербезпеки та формуванню теоретико-методологічних засад, побудові моделей захисту (О. Баранов, В. Бурячок, С. Василенко, О. Виговська, В. Гирда, С. Гнатюк, В. Горбулін, В. Дереко, І. Діордіца, О. Додонов, Д. Дубов, Ю. Кожедуб, О. Корченко, Є. Котух, Д. Ланде, А. Максимець та ін.); правового регулювання кібербезпеки в Україні (В. Бухарєв, І. Доронін, І. Забара, М. Ільницький, Н. Коваленко та ін.); створення національної системи публічного управління в означеній сфері, зокрема питанням функціонування системи захисту та її механізмів (Р. Бердибаєв, С. Гнатюк, В. Гурковський, Є. Живило, В. Жигаревич, І. Жиляєв, В. Загорняк, В. Зайцев, О. Зозуля, І. Козубцов, Л. Козубцова, Д. Мельник, А. Семенченко, В. Сидоренко, Т. Смирнова, Т. Станіславський, Ю. Хлапонінб, О. Черноног, Р. Штунда та ін.); міжнародної співпраці та вивченню зарубіжного досвіду (В. Акульшина, К. Бонарєва, Д. Василенко, М. Гребенюк, Л. Дешко, В. Дитюк,

С. Єсімов, Б. Леонов, В. Маслак та ін.); пошуку шляхів вирішення проблем, інновацій і сучасних підходів з метою забезпечення кібербезпеки ОКІ (О. Богданов, З. Бржевська, В. Козачак, Я. Машталяр) та ін.

За умов наростаючої агресії Росії та підтримки її союзників, процеси вдосконалення чинного законодавства та підвищення ефективності функціонування інституційної системи кібербезпеки об'єктів критичної інформаційної інфраструктури (далі – ОКІІ) України стають дедалі актуальнішими, що спонукає до проведення наукових досліджень і пошуків.

Виклад основного матеріалу. Кібербезпека кожної держави забезпечується шляхом формування виваженої державної політики відповідно до прийнятих нормативно-правових актів та їх втілення ефективною системою інституційного забезпечення. Упродовж останніх років законодавці прийняли низку законодавчих актів, які визначили організаційно-правову основу кібербезпеки. У зв'язку зі збройним вторгненням росії на територію України, ці процеси активізувались щодо ОКІ.

За твердженням науковців, необхідність контролю та подальшого врегулювання відповідних взаємовідносин обумовлювалась невідкладністю створення надійної системи кібернетичної безпеки ОКІІ, відсутність якої потенційно може призвести до втрати політичної незалежності будь-якої держави світу. Важливим практичним кроком у формуванні національної інституційної системи було створення у 2007 р. Центру реагування на комп'ютерні інциденти (Computer Emergency Response Team of Ukraine, CERT-UA), що ввійшов до складу Держспецзв'язку України. Ця структура виконує роль технічного координатора органів публічної влади, військових формувань, підприємств, установ і організацій незалежно від форми власності з питань запобігання, виявлення, усунення наслідків кіберінцидентів.

На виконання ст. 35 Конвенції Ради Європи про кіберзлочинність [19] у червні 2009 р. при Службі безпеки України (далі – СБУ) на базі спеціального підрозділу для боротьби з кіберзагрозами розпочав своє функціонування Національний контактний пункт формату 24/7 із реагування та обміну

терміновою інформацією про вчинені кіберзлочини.

У липні 2010 р. у структурі МВС України на базі Департаменту боротьби зі злочинами, пов’язаними з торгівлею людьми, створено новий структурний підрозділ – Департамент боротьби з кіберзлочинністю та торгівлею людьми. Указом Президента України «Про виклики та загрози національній безпеці України у 2011 році» (2010 р.) ухвалено рішення про початок створення Єдиної загальнодержавної системи протидії кіберзлочинності.

Безпека держави напряму залежить від захищеності її інформаційного та кіберпростору. Відтак, на виконання Указу Президента України (2012 р.) [12] у структурі СБУ створено Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки (далі – ДКІБ СБУ), який відповідає за стан державної безпеки в кібернетичній та інформаційній сферах, координує та контролює діяльність регіональних органів і підрозділів Центрального Управління СБУ. У межах своєї компетенції вносить Президенту України пропозиції про видання актів, обов'язкових для виконання органами державного управління, підприємствами, установами, організаціями і громадянами. Сферу діяльності ДКІБ СБУ визначають закони «Про Службу безпеки України» [20], «Про контррозвідувальну діяльність» [14], «Про основні засади забезпечення кібербезпеки» [18] та ін. Кіберфахівці спецслужби у 2021 р. встановили хакерів всесвітньо відомого угрупування «ARMAGEDON», яке здійснило понад 5 тис. кібератак на державні органи та ОКІ України [22].

Сьогодні СБУ [6] реалізує весь комплекс заходів щодо захисту ОКІ, що є однією з важливих компонент безпекової політики держави. В умовах війни СБУ максимальну увагу надає контррозвідувальному захисту об’єктів енергетики, транспортного комплексу та інших стратегічно важливих галузей з метою запобігання спробам агентурного проникнення ворога на такі об’єкти та його намірам вчиняти диверсії. Значний масив роботи СБУ пов’язаний із блокуванням активів прокремлівських компаній та осіб, причетних до підтримки війни в Україні, протиправного вивезення українського зерна тощо. СБУ накладено арешт на 11 морських суден, які росія використовувала для незаконного

вивезення зерна. За результатами 2022 р. кіберфахівці СБУ:

– нейтралізували понад 4 500 кібератак і критичних кіберінцидентів;

– блокували 45 ботоферм потужністю понад 2 млн. рейкових акаунтів;

– блокували майже 500 антиукраїнських Youtube-каналів з аудиторією більше, ніж 15 млн. підписників;

– викрили понад 1 200 інтернет-агітаторів, які поширювали російські фейки та наративи;

– повідомили майже 600 підозр [22, с. 41].

Активність російських кібератак упродовж 2020-2022 рр. зросла в 5,6 разів (рис.1). Побудова прогностичних моделей, відображених за допомогою теоретичних ліній регресії різних функціональних форм, зокрема поліноміальної (R^2=1) та лінійної (R^2=0,8679), вказують на посилення цієї негативної тенденції у найближчій перспективі.

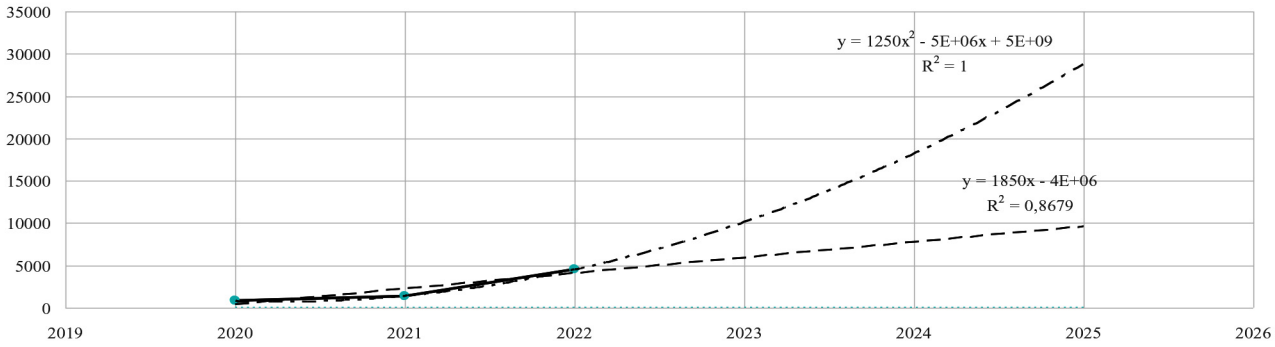

Рис. 1. Прогностичні моделі зростання активності російських кібератак

Джерело: побудовано на основі статистичних даних [22, с. 42]

Запровадження СБУ платформи MISP-UA ще до початку активної фази воєнних дій сприяє ефективнішому запобіганню кібератакам і кіберінцидентам на ОКІ, державних інформресурсах. Також кіберфахівці забезпечили під'єднання критично важливих об'єктів до єдиної системи управління інформаційною безпекою (SIEM, Security Information and Event Management), яка моніторить події в режимі реального часу, що уможливлює постійний аналіз

стану інформаційної безпеки.

На виконання постанови Кабінету Міністрів України [21], а також відповідно до наказів МВС від 15.10.2015 р. № 1250 та № 1251 [5], з метою проведення якісного відбору висококваліфікованих фахівців у підрозділи кіберполіції 15.10.2015 р., Міністр внутрішніх справ України оголосив про початок реформування підрозділів боротьби з кіберзлочинністю МВС у кіберполіцію Національної поліції та добір кандидатів на заміщення вакантних посад у кіберполіції.

Згідно із Положенням про Департамент кіберполіції (далі – ДКП) Національної поліції України, затвердженого наказом Національної поліції від 10.11.2015 р. № 85 [5], створено міжрегіональний територіальний орган, який є юридичною особою публічного права. До його складу входять структурні підрозділи, які діють за міжрегіональним принципом та безпосередньо підпорядковані начальникові Департаменту. З метою забезпечення міжнародної діяльності кіберполіції у штатній структурі ДКП створено сектор Національного контактного пункту з реагування на кіберзлочини. ДКП відповідно до законодавства України забезпечує реалізацію державної політики у галузі протидії кіберзлочинності, здійснює інформаційно-аналітичне забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, що належать до його компетенції [17]. ДКП бере участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку [13]. Цей суб’єкт публічного права сприяє в порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції України в попередженні, виявленні та припиненні кримінальних правопорушень.

За результатами роботи за 2023 р. ДКП [4] виявлено понад 3 600 кіберзлочинів; оголошено підозру понад 1 700 особам за вчинення понад 3 700 злочинів, що на 59 % перевищує аналогічний показник 2022 року.

У 2017 р. Верховна Рада України прийняла Закон України «Про основні засади забезпечення кібербезпеки України» [18], норми якого визначають організаційно-правові основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Відповідно до положень п. 19 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» (2017 р.) [18] визначено, що ОКІІ є його комунікаційна або технологічна система, кібератака на яку безпосередньо вплине на його стале функціонування. Нормами ст. 6 визначено ОКІ – підприємства, установи, організації незалежно від форми власності, які:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, ІКТ, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров’я;

3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;

4) є підприємствами, що мають стратегічне значення для економіки і безпеки держави;

5) є об’єктами потенційно небезпечних технологій і виробництв.

Вважаємо, що дефініція ОКІ, наведена у ст. 1 цього закону, є громіздкою та розмитою. Пропонуємо формулювати ОКІ як «стратегічні, небезпечні або життєзабезпечувальні об’єкти незалежно від форми власності», оскільки ознака виокремлення їх важливості, приналежності до такої категорії чи переліку об’єктів не залежить від того чи цей об’єкт працює, чи виведений з ладу, чи

здійснює негативний вплив на середовище, чи людей.

Нормами ст. 4 цього закону [18] означено об'єкти кібербезпеки та кіберзахисту, до списку яких належать ОКІ, а саме: системи управління, канали зв'язку, системи навігації, розвідки банківські та фінансові системи, різні реєстри та інші елементи інформаційного середовища різних сфер: економіки, транспорту, енергетики, охорони здоров'я, інших сфер, що забезпечують безпеку та оборону держави.

Забезпечення кібербезпеки в Україні ґрунтується на принципах, визначених у ст. 7 закону [18] та Стратегії кібербезпеки України (2021 р.) [23], що розуміються як закономірності, відносини, взаємозв'язки, керівні засади, на яких ґрунтуються його організація та здійснення та які можуть бути сформульовані в певні правила.

У ст. 5 вище згадуваного закону [18] визначено суб'єкти забезпечення кібербезпеки: Президент України, Рада національної безпеки і оборони України, Національний координаційний центр кібербезпеки, Кабінет Міністрів України, а також напрями координації зусиль між ними та сфери контролю. Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони (далі – РНБО) України. Національний координаційний центр кібербезпеки [9], як робочий орган РНБО України, здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на ОКІ (крім ОКІ у банківській системі України). Необхідно зауважити, що Кабінет Міністрів

України затверджує:

– порядок формування переліку ОКІІ;

– їх перелік та порядок їх внесення до державного реєстру ОКІІ;

– порядок формування та забезпечення функціонування державного реєстру ОКІІ.

Повноваження щодо формування та забезпечення функціонування реєстру ОКІ у банківській системі покладаються на Національний банк України.

Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, відповідно до п. 4 ст. 5 закону [18] є:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

5) Збройні Сили України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

7) підприємства, установи та організації, віднесені до ОКІ;

8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

У межах своєї компетенції суб'єкти забезпечення кібербезпеки здійснюють низку заходів, передбачених положеннями п. 5 ст. 5 закону [18].

Важливим етапом у процесі становлення організаційного забезпечення у цій сфері є формування національної системи кібербезпеки в Україні, елементи та структура якої визначена нормами ст. 8 вище згадуваного закону [18]. Зокрема зазначається, що національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних політичних, науково-технічних,

інформаційних, освітніх, організаційно-правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту ОКІІ. Визначено, що основними суб'єктами національної системи кібербезпеки є Держспецзв'язку України, Національна поліція України, СБУ, Міністерство оборони України та Генеральний штаб ЗСУ, розвідувальні органи, Національний банк України, які відповідно до Конституції і законів України виконують в установленому порядку основні завдання, визначені ч. 2 ст.8 [18]:

Аналізуючи викладене вище, зауважимо, що такий підхід стосовно визначення різних суб'єктів у ст.ст. 5 і 8 [18] вносить певне різночитання та тлумачення, оскільки суб'єкти, вказані у ст. 5, не входять до Національної системи кібербезпеки, вказаної у ст. 8, що є некоректним, оскільки кожна система складається з керівної та керованої підсистем, структурні елементи яких розподіляються і взаємодіють за певними ієрархічними рівнями адміністративно-територіального устрою держави, наданими повноваженнями.

Разом з цим у п. 3 ст. 8 означеного закону наведено перелік різнопланових заходів (25 пунктів), спрямованих на забезпечення функціонування національної системи кібербезпеки, але без зазначення конкретного суб'єкта їх реалізації. Такий підхід не дає можливості чітко визначити суб'єктність реалізації тих чи інших заходів, критерії їх виконання, рівень відповідальності того чи іншого суб'єкта тощо, що вказує загалом на уявність виконання означених заходів. Не дивлячись на те, що Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, зокрема через відповідні: міністерства внутрішніх справ, цифрової трансформації, оборони, що входять у національну систему кібербезпеки, є заходи, що стосуються ЦОВВ, які до такої системи не належать. Зокрема п. 14: «підготовки фахівців освітньо-кваліфікаційних рівнів бакалавра і магістра за державним замовленням в обсязі, необхідному для задоволення потреб державного сектору економіки, а також за небюджетні кошти, у тому числі для підвищення кваліфікації та проведення

обов’язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки ОКІ, з урахуванням міжнародних стандартів». Те саме стосується і виконання п. 1 та п. 2 вказаних заходів, зокрема щодо вироблення й оперативної адаптації державної політики, створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у цій сфері, що напряму торкається сфери компетенцій та функцій Верховної Ради України, яка серед суб’єктів Національної системи кібербезпеки не вказана також.

Водночас, такі структури як СБУ відповідно до Закону України (1992 р.) [20], норми якого визначають її статус як державного органу спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку України, підпорядковується тільки Президентові України (ст. 1).

Нормами ст. 9 Закону [18] передбачено урядову команду реагування на комп’ютерні надзвичайні події України CERT-UA, забезпечення функціонування якої здійснює Держспецзв'язку України у межах штатної чисельності та виділених обсягів фінансування [8]. Завданнями CERT-UA є: накопичення та проведення аналізу даних про кіберінциденти, ведення їх державного реєстру; надання власникам об’єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об’єктів; організація та проведення практичних семінарів з питань кіберзахисту для суб’єктів національної системи кібербезпеки та власників об’єктів кіберзахисту та ін.

Власник та/або керівник ОКІ, відповідно до п. 8 Загальних вимог до кіберзахисту ОКІ [2], організовує невідкладне інформування урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA (у разі наявності – галузевої команди реагування на комп’ютерні надзвичайні події), а також функціонального підрозділу контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління СБУ (Ситуаційний центр забезпечення кібербезпеки СБУ) або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки, які

стосуються його ОКІІ.

В умовах гібридної війни, яку розв'язала росія, ризики для ОКІ суттєво зростають, оскільки від рівня їх захищеності залежить і національна безпека. З огляду на це, фахівці СБУ зосереджені на контррозвідувальному, контртерористичному та протидиверсійному захисті об'єктів енергетики, транспортного комплексу, інших стратегічно важливих галузей, постійно блокуючи: спровоковані агресором нештатні та аварійні ситуації; перебої в роботі об'єктів життєдіяльності; маніпуляції у фінансово-банківському секторі.

Сьогодні Україна активно формує державну систему захисту критичної інфраструктури з урахуванням досвіду країн НАТО та ЄС. У цій галузі серед пріоритетних завдань СБУ: протидія іноземній економічній експансії, недопущення використання фінансових інструментів для створення системних кризових явищ в українській економіці.

Згідно зі ст. 15 аналізованого Закону України «Про основні засади забезпечення кібербезпеки України» [18], передбачено також і форми контролю в означеній сфері дослідження. Контроль за дотриманням законодавства при здійсненні заходів із забезпечення кібербезпеки здійснюється Верховною Радою в порядку, визначеному Конституцією України. Контроль за діяльністю із забезпечення кібербезпеки суб'єктів сектору безпеки і оборони, інших державних органів здійснюється Президентом та урядом у порядку, визначеному Конституцією і законами України. Кабінет Міністрів України не лише реалізує державну політику у сфері кібербезпеки, але й повинен здійснювати контролюючі функції.

Незалежний аудит діяльності основних суб'єктів національної кібербезпеки, визначених ч. 2 ст. 8 закону [18], щодо ефективності системи забезпечення кібербезпеки держави проводиться щороку згідно з міжнародними стандартами аудиту. Звіти про результати проведення такого аудиту за попередній рік подаються Президентові, Верховній Раді та Кабінету Міністрів України у 45-тиденний строк після закінчення календарного року.

Відповідні комітети Верховної Ради України, до предмета відання яких

належать питання національної безпеки і оборони, інформатизації та зв’язку, на своїх засіданнях розглядають звіти основних суб’єктів національної кібербезпеки, визначених ч. 2 ст. 8 цього закону, про результати незалежного аудиту їхньої діяльності щодо ефективності системи забезпечення кібербезпеки держави. Ці суб’єкти щорічно подають звіти про стан виконання ними заходів з питань забезпечення кібербезпеки держави, віднесених до їх компетенції. За результатами аналізу звітів комітет може порушити питання про розгляд цих питань Верховною Радою України.

Ще одна важлива структура, яка функціонує у сфері кібербезпеки – Державний центр кіберзахисту (далі – ДЦКЗ) Держспецзв'язку України – це державна установа, створена для здійснення впровадження організаційно-технічної моделі кіберзахисту як складової національної системи конфіденційного зв’язку України. Відповідно до п. 5 ст. 8 [76] впровадження організаційно-технічної моделі кібербезпеки, як складової національної системи кібербезпеки, здійснюється ДЦКЗ, який забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту ОКІІ, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об’єктів кіберзахисту, системи взаємодії команд реагування на комп’ютерні надзвичайні події, а також у взаємодії з іншими суб’єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань. Забезпечення функціонування ДЦКЗ у межах штатної чисельності та виділених обсягів фінансування здійснює Держспецзв'язку України згідно з законом «Про основні засади забезпечення кібербезпеки України» [18].

Відповідно до п. 5 «Порядку внесення ОКІІ до державного реєстру ОКІІ, його формування та забезпечення функціонування» [10], розпорядником інформаційно-телекомунікаційної системи реєстру та володільцем інформації, що міститься у реєстрі, є Адміністрація Держспецзв’язку, яка:

– вживає заходів до створення та адміністрування реєстру;

– встановлює організаційні та методичні засади функціонування реєстру, а також забезпечує його функціонування;

– встановлює порядок та форми подання відомостей до реєстру, а також визначає порядок доступу до відомостей реєстру;

– на підставі отриманих відомостей забезпечує формування та оновлення відомостей реєстру;

– забезпечує захист відомостей реєстру відповідно до вимог законодавства у сфері захисту інформації та державної таємниці;

– проводить інші заходи щодо забезпечення функціонування реєстру.

Проведений аналіз становлення інституційної системи вказує на чималу кількість суб'єктів протидії у сфері кібербезпеки, частина з яких ввійшла в Національну систему кібербезпеки. Проте фахівці [1, с. 11] стверджують, що важливість кіберпростору підтверджується необхідністю створення у складі збройних сил країн світу спеціальних структур, наприклад:

– об'єднаного Кіберкомандування (U. S. Cyber Command-USCYBERCOM) та спеціалізованого кібернетичного розвідувального центру у США;

– Управління мережних операцій у Німеччині;

– Центрального управління з кібербезпеки, Оперативного центру забезпечення кібербезпеки (CSOC) та Центру державного зв'язку (GCHQ) у Великобританії;

– Центру інформаційних систем Служби безпеки (CISSS) та Національного агентства безпеки інформаційних систем (ANSSI) у Франції;

– спеціалізованого центру захисту національного кіберпростору Tehila в Ізраїлі тощо.

Вказані підрозділи призначено для ведення кіберборотьби – комплексу заходів, спрямованих на здійснення управлінського і/або деструктивного впливу на автоматизовані ІТ-системи протиборчої сторони та захисту від такого впливу власних інформаційно-обчислювальних ресурсів завдяки використанню

спеціально розроблених програмно-апаратних засобів, а також проведенню системи спеціалізованих навчань.

Порядок формування переліку ОКІІ (2020 р.) [11], визначає механізм формування національного та секторальних переліків ОКІІ. У цьому документі доповнено термінологічний апарат у сфері дослідження, зокрема категоріями: безпека ОКІ, власник та/або керівник ОКІ, захист ОКІІ, критична інформаційна інфраструктура та ін.

Відповідно до п. 2 [11] власник та/або керівник ОКІ як оператор основних послуг – державний орган, підприємство, установа, організація будь-якої форми власності, юридична та/або фізична особа, якому/якій на правах власності, оренди або на інших законних підставах належить ОКІ або який/яка відповідає за його поточне функціонування. Цей оператор основних послуг визначає:

– всі об’єкти інформаційної інфраструктури (автоматизовані, інформаційні, телекомунікаційні, інформаційно-телекомунікаційні системи, автоматизовані системи управління технологічними процесами), що експлуатуються на ОКІ;

– які з наведених ОКІ необхідні для забезпечення безперервного та стійкого його функціонування з точки зору надання ним основних послуг та проводить оцінку їх критичності.

Отже, в питаннях безпеки, зокрема і кібербезпеки, вся відповідальність лежить на операторові основних послуг, який для оцінки критичності ОКІІ використовує такі три критерії:

– необхідність об’єкта інформаційної інфраструктури як для стійкого та безперервного його функціонування, так і для надання ним основних послуг;

– кібератака, кіберінцидент, інцидент з інформаційної безпеки на об’єкті інформаційної інфраструктури істотно впливає на безперервність та стійкість надання ОКІ основних послуг;

– у разі порушення безперервності та стійкості надання основних послуг ОКІ відсутній альтернативний об’єкт (спосіб) для їх надання.

Такі структури, що відповідають усім трьом критеріям, визначаються

оператором основних послуг як ОКІІ. Категорія критичності (I-IV) ОКІІ встановлюється за категорією критичності ОКІ.

Уповноважений орган на підставі цієї інформації формує та веде секторальний перелік ОКІІ, а також оновлює його кожні два роки. Відомості про ОКІІ, включені до національного переліку, вносяться до державного реєстру ОКІІ, власник якого зобов'язаний вжити першочергових заходів із захисту такого об'єкта від кібератак. Разом з цим, необхідно зазначити про відсутність чітких критеріїв розмежування категорій критичності (I-IV) ОКІІ. Проблема є також і щодо відповідальності оператора основних послуг, якому належить ОКІ або який відповідає за його поточне функціонування.

У зв'язку із прийняттям Закону України «Про основні засади забезпечення кібербезпеки України» [18], були внесені зміни у низку чинних законів України, що загалом зміцнило загальну законодавчу базу в означеній сфері.

Закон України «Про національну безпеку України» (2018 р.) [16] відповідно до статей 1, 2, 17, 18 і 92 Конституції України визначає основи та принципи національної безпеки і оборони, цілі та основні засади державної політики, дотримання яких гарантуватимуть захист від загроз. Стаття 31 закону [16] присвячена Стратегії кібербезпеки України як документу «довгострокового планування, в якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі», пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики, підвищення ефективності основних суб'єктів забезпечення кібербезпеки, а також потреби бюджетного фінансування.

Загальні вимоги до кіберзахисту ОКІ, затверджені постановою Кабінету Міністрів України (2019 р.) [2], визначають організаційно-методологічні, технічні та технологічні умови їх кіберзахисту, що є обов'язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства належать до ОКІ. Кіберзахист таких об'єктів є складовою робіт зі створення, модернізації й експлуатації ОКІІ.

Президент України підписав указ «Про Стратегію національної безпеки України» (2020 р.) [24] (далі – Стратегія), яка відрізняється від попередніх документів такого роду та є особливою, оскільки відповідно до Закону України «Про національну безпеку України» є основою для розроблення інших документів стратегічного планування, які визначатимуть шляхи та інструменти її реалізації. На її ґрунті створюється нова нормативно-правова база у сфері національної безпеки та оборони, визначається реальний стан і перспективи розвитку складових національної безпеки, формується державна політика.

У п. 4 Стратегії викладено три основні засади державної політики у сфері національної безпеки, на яких вона ґрунтується: стримування, стійкість та взаємодія. Саме ці засади закладали модель, за якою мав би розвиватись увесь сектор безпеки та оборони країни. Посилення спроможностей національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі – є одним із нових пріоритетних напрямків дій держави. Наголошено також, що основним завданням розвитку системи кібербезпеки – є гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації.

Згідно з чинним законодавством та відповідно до укладених міжнародних договорів, Україна здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю. Україна може брати участь у спільних заходах із забезпечення кібербезпеки, зокрема у проведенні спільних навчань суб’єктів сектору безпеки і оборони в рамках заходів колективної оборони з дотриманням вимог законів «Про порядок направлення підрозділів Збройних Сил України до інших держав» та «Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України».

Згодом, шляхом унесення змін до закону [18] у 2021 р., сформовано Національний центр резервування державних інформаційних ресурсів – як організовану сукупність об’єктів, створених з метою забезпечення надійності та

безперебійності роботи державних інформаційних ресурсів, кіберзахисту, зберігання національних електронних інформаційних ресурсів, резервного копіювання інформації та відомостей національних електронних інформаційних ресурсів державних органів, військових формувань, утворених відповідно до законів, підприємств, установ та організацій.

Наприкінці 2021 р. Верховною Радою України прийнято Закон «Про критичну інфраструктуру» [15], у якому визначено організаційно-правові засади створення та функціонування національної системи захисту критичної інфраструктури. Відповідно до ч. 1 ст. 5 метою державної політики у сфері захисту критичної інфраструктури є забезпечення безпеки ОКІ, запобігання проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям. Попри недоліки, закон має чимало переваг, знято певні проблемні питання, актуалізовані у попередніх законодавчих актах.

У ст. 6 закону [15] сформульовано п’ять засадничих принципів державної політики у сфері національної безпеки: єдність методологічних засад; координованість; державно-приватне партнерство; безпека, захист та охорона інформації з обмеженим доступом; міжнародне співробітництво.

Визначено чотири рівні управління національною системою захисту критичної інфраструктури: об’єктовий, місцевий, регіональний / галузевий та загальнодержавний, а також визначено суб’єктів, уповноважених у сфері захисту суб’єктів критичної інфраструктури України. Попри встановлення критеріїв приналежності до ОКІ, визначених відповідно до рівнів управління, зазначимо їх нечіткість, неузгодженість з іншими нормативно-правовими актами. Сформульовано 17 видів життєво важливих функцій та / або послуг, порушення яких призведе до негативних наслідків національної безпеки України. З метою визначення потенційних загроз розробляється паспорт безпеки ОКІ та формується їх реєстр.

Представлена у розділі IV закону [15] національна система захисту ОКІ не позбавлена певних недоліків. Здебільшого вказані назви суб’єктів цієї системи, проте, окремі з них, залучені до цього процесу, визначені за функціями. Так,

наприклад, «секторальні та функціональні органи», «уповноважений орган» у сфері захисту критичної інфраструктури України. Сумнівним, виходячи із концептуальних положень щодо суб'єктів формування та реалізації державної політики [3], надання цим суб'єктам таких повноважень (ч. ч. 2, 3 ст. 13). Натомість, уже у ст. 16 йдеться про «уповноважений орган у сфері захисту критичної інфраструктури України, який забезпечує формування та реалізує державну політику».

Серед 17-ти зазначених у цьому законі суб'єктів національної системи захисту критичної інфраструктури є чимало нових (ЦВК, Національні комісії, Фонд державного майна та ін.), але немає ні Президента, ні Верховної Ради, яка якраз і є головним суб'єктом формування політики у будь якій сфері. До процесу планування заходів щодо забезпечення стійкості та захисту ОКІ долучаються Національна Гвардія України, ДСНС, які попередньо не конкретизувались як елементи цієї системи. Актуалізуються також питання парламентського та громадського контролю, міжнародного співробітництва.

Висновки. Необхідно зазначити, що сьогодні кількість міжнародних документів у сфері кібербезпеки стрімко зростає, що підтверджують статистичні дані сайту документів європейського права EUR-Lex [7] на якому розміщено 3 813 актів станом на квітень 2024 р., зокрема 782 нових за 2023 р. Незважаючи на те, що в Україні впродовж останніх років прийнято низку концептуальних законодавчих та нормативно-правових актів проблема їх реального впровадження, взаємоузгодження, зокрема з міжнародними стандартами, координування дій та взаємодії основних суб'єктів кібербезпеки та кіберзахисту, їх відповідності вимогам надійного та оперативного реагування на комплекс загроз в означеній сфері – залишається актуальною.

Беручи до уваги роль та вагомість кібербезпекової складової в системі забезпечення національної безпеки держави де-юре, де-факто – очевидна недостатня координація діяльності відповідних відомств та узгодженості дій з функціонування як окремих елементів системи кібербезпеки, так і загалом її як системи з боку Національного координаційного центру кібербезпеки, як

загальнонаціональної координаційної структури, уповноваженої узгоджувати й координувати діяльність правоохоронних органів, силових структур і відомств щодо протидії реальним загрозам інформаційного та кіберпростору України, керувати проведенням комплексних навчань із забезпечення кібернетичної безпеки держави.

Література

1. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект. К. : ДУТ, 2015. 288 с.

2. Постанова Кабінету Міністрів України № 518 від 19.06.2019 р. «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text

3. Лазор О. Я., Лазор О. Д. Формування та реалізація державної політики: теоретико-правовий дискурс. *Публічне управління і право: історія, теорія, практика*. 2021. Вип. 1. С. 54-62.

4. Михайлов Д. За 2023 рік кіберполіція виявила понад 3600 кіберзлочинів. URL : https://suspilne.media

5. Офіційний портал Національної поліції України. URL: https://mvs.gov.ua/contacts/national-police-ukraine

6. Офіційний портал Служби безпеки України. URL : https://ssu.gov.ua

7. Офіційний портал EUR-Lex. URL: http://eur-lex.europa.eu

8. Постанова Кабінету Міністрів України № 411 від 03.09.2014 р. «Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України». URL: https://zakon.rada.gov.ua/laws/show/411-2014-п#Text

9. Указ Президента України № 242/2016 від 07.06.2016 р. «Про Національний координаційний центр кібербезпеки». URL : https://zakon.rada.gov.ua/laws/show/242/2016#Text

10. Постанова Кабінету Міністрів України № 943 від 09.10.2020 р. «Деякі питання об'єктів критичної інформаційної інфраструктури»: URL: https://zakon.rada.gov.ua/laws/show/943-2020- п#Text

11. Указ Президента України № 34 від 25.01.2012 р. «Про внесення змін до деяких законів України про структуру і порядок обліку кадрів Служби безпеки України». URL: https://zakon.rada.gov.ua/laws/show/4157-17#Text

12. Постанова Кабінету Міністрів України № 877 від 28.10.2015 р. «Про затвердження Положення про Національну поліцію». URL: https://zakon.rada.gov.ua/laws/show/877-2015- п#Text

13. Закон України № 374-IV від 26.12.2002 р. «Про контррозвідувальну діяльність». URL: https://zakon.rada.gov.ua/laws/show/374-15#Text

14. Закон України № 1882-IX від 16.11.2021 р. «Про критичну інфраструктуру». URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

15. Закон України № 2469-VIII від 21.06.2018 р. «Про національну безпеку України». URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

16. Закон України № 580-VIII від 02.07.2015 р. «Про національну поліцію». URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

17. Закон України № 2163-VIII від 05.10.2017 р. «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

18. Закон України № 2824-IV від 07.09.2005 р. «Про ратифікацію Конвенції про кіберзлочинність» URL: https://zakon.rada.gov.ua/laws/show/2824-15

19. Закон України № 2229-XII від 25.03.1992 р. «Про Службу безпеки України» URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text

20. Постанова Кабінету Міністрів України № 830 від 13.10.2015 р. «Про утворення територіального органу Національної поліції» URL: https://zakon.rada.gov.ua/laws/show/830-2015-п#Text

21. Щорічний звіт СБУ «2022 рік: захист держави в умовах війни». URL: https://ssu.gov.ua/uploads/documents/2023/04/24/ssu-report-2022-web.pdf

22. Указ Президента України № 447/2021 від 26.08.2021 р. «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»». URL:

https://zakon.rada.gov.ua/laws/show/447/2021#Text

23. Указ Президента України № 392/2020 від 14.09.2020 р. «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»» URL: https://www.president.gov.ua/documents/3922020-35037

References

1. Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O. and Toliupa, S. V. (2015), *Informatsijna ta kiberbezpeka: sotsiotekhnichnyj aspekt* [Information and cyber security: socio-technical aspect], DUT, Kyiv, Ukraine.

2. Cabinet of Ministers of Ukraine (2019), Resolution "On Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects", available at: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text (Accessed 28 March 2024).

3. Lazor, O. Ya. and Lazor, O. D. (2021), "Formation and implementation of state policy: theoretical and legal discourse", *Publichne upravlinnia i pravo: istoriia, teoriia, praktyka,* vol. 1, pp. 54–62.

4. The official site of "Social news" (2023), "In 2023, the cyber police detected more than 3,600 cybercrimes", available at: https://suspilne.media (Accessed 20 April 2024).

5. The official site of National Police of Ukraine (2024), available at: https://mvs.gov.ua/contacts/national-police-ukraine (Accessed 25 March 2024).

6. The official site of Security Services of Ukraine (2024), available at: https://ssu.gov.ua (Accessed 18 April 2024).

7. The official site of EUR-Lex (2024), available at: http://eur-lex.europa.eu (Accessed 22 April 2024).

8. Cabinet of Ministers of Ukraine (2014), Resolution "On approval of the Regulation on the Administration of the State Service of Special Communication and Information Protection of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/411-2014-п#Text (Accessed 23 April 2024).

9. President of Ukraine (2016), Decree "About the National Coordination Center

of Cyber Security", available at: https://zakon.rada.gov.ua/laws/show/242/2016#Text (Accessed 29 March 2024).

10. Cabinet of Ministers of Ukraine (2020), Resolution "Some issues of objects of critical information infrastructure", available at: https://zakon.rada.gov.ua/laws/show/943-2020-p#Text (Accessed 12 April 2024).

11. President of Ukraine (2012), Decree "On Amendments to Some Laws of Ukraine on the Structure and Procedure of Personnel Accounting of the Security Service of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/4157-17#Text (Accessed 28 March 2024).

12. Cabinet of Ministers of Ukraine (2015), Resolution "On approval of the Regulation on the National Police", available at: https://zakon.rada.gov.ua/laws/show/877-2015-p#Text (Accessed 28 March 2024).

13. The Verkhovna Rada of Ukraine (2020), The Law of Ukraine "About counter-intelligence activities", available at: https://zakon.rada.gov.ua/laws/show/374-15#Text

14. The Verkhovna Rada of Ukraine (2021), The Law of Ukraine "On Critical Infrastructure", available at: https://zakon.rada.gov.ua/laws/show/1882-20 (Accessed 21 March 2024).

15. The Verkhovna Rada of Ukraine (2018), The Law of Ukraine "On the national security of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/2469-19#Text (Accessed 28 March 2024).

16. The Verkhovna Rada of Ukraine (2015), The Law of Ukraine "About the national police", available at: https://zakon.rada.gov.ua/laws/show/580-19#Text (Accessed 28 March 2024).

17. The Verkhovna Rada of Ukraine (2017), The Law of Ukraine "On the main principles of ensuring cyber security of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text (Accessed 28 March 2024).

18. The Verkhovna Rada of Ukraine (2021), The Law of Ukraine "On the ratification of the Convention on Cybercrime", available at: https://zakon.rada.gov.ua/laws/show/2824-15 (Accessed 21 March 2024).

19. The Verkhovna Rada of Ukraine (1992), The Law of Ukraine "About the

Security Service of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/2229-12#Text (Accessed 24 April 2024).

20. Cabinet of Ministers of Ukraine (2015), Resolution "On the formation of a territorial body of the National Police", available at: https://zakon.rada.gov.ua/laws/show/830-2015-п#Text (Accessed 24 April 2024).

21. The official site of of Security Services of Ukraine (2023), "Annual report of the Security Service of Ukraine "Year 2022: Defense of the State in Conditions of War"", available at: https://ssu.gov.ua/uploads/documents/2023/04/24/ssu-report-2022-web.pdf (Accessed 21 April 2024).

22. President of Ukraine (2021), Decree "On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "About cyber security strategy of Ukraine"", available at: https://zakon.rada.gov.ua/laws/show/447/2021#Text (Accessed 22 April 2024).

23. President of Ukraine (2020), Decree "On the decision of the National Security and Defense Council of Ukraine dated September 14, 2020 "About cyber security strategy of Ukraine"", available at: https://zakon.rada.gov.ua/laws/show/447/2021#Text (Accessed 20 April 2024).

Стаття надійшла до редакції 28.04.2024 р.