УДК 343
DOI https://doi.org/10.32689/2523-4625-2024-4(76)-10

Юлія ЛЕПЕХ
кандидат юридичних наук, доцент кафедри права, ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», y0979793133@gmail.com
ORCID: 0000-0003-4530-4924

ДІЯЛЬНІСТЬ ОРГАНІВ КІБЕРБЕЗПЕКИ В УКРАЇНІ ЯК НАПРЯМ ЗАПОБІГАННЯ ТА ПРОТИДІЇ НАСИЛЬСТВА В ДЕРЖАВІ

Подано законодавче визначення кібербезпеки в Україні та статистичні дані щодо цього питання. Зазначено про низьку кількість наукових праць із даного питання. Визначено основні причини кіберзлочинності. Подано причини прогалин у нормативно-правовому регулюванні питання забезпечення кібербезпеки в Україні. Виокремлено психологічні, соціальні та економічні аспекти вищевказаного. Зазначено, що кібербезпека є терміном ширшим за своїм значенням, ніж кіберзахист. Подано систему суб'єктів кібербезпеки в Україні. Визначено рівні суб'єктів забезпечення кібербезпеки в Україні. Подано перелік спеціальних суб'єктів у сфері забезпечення кібербезпеки в Україні. Визначено структурні елементи механізму протидії та запобігання кіберзлочинності. Зазначено про низьку кількість наукових праць та досліджень у сфері реалізації механізму забезпечення кібербезпеки в Україні. Зроблено висновок щодо міжнародного досвіду запобігання та протидії насильства у сфері кіберзлочинності. Зроблено висновок про те, що відсутність належного механізму протидії та запобігання кібербезпеки в Україні призводить до виникнення, поширення психологічного, економічного, сексуального, фізичного насильства, що є загрозою функціонування правової Української держави та розвитку громадянського суспільства. Подано пропозицію щодо отримання працівниками кібербезпеки вищої освіти у спеціальних навчальних закладах, та при необхідності проходити спеціальні курси. Звернено увагу на те, що освітній напрям підготовки працівників кібербезпеки, зважаючи на темпи зростання кіберзлочинності в Україні, в умовах сьогодення повинен здійснюватися з урахуванням матеріальних потреб суспільства та можливостей їхніх громадян.Запропоновано зазначити те, що належний економічний соціальний розвиток держав та суспільства сприяє відсутністю високих показників вчинення кіберзлочинів.

Ключові слова: *кібербезпека, насильство, причини, напрями запобігання, напрями протидії, кіберзлочини.*

Yulia Lepekh. ACTIVITIES OF CYBER SECURITY BODIES IN UKRAINE AS A DIRECTION OF PREVENTING AND COMBATING VIOLENCE IN THE STATE

The legislative definition of cyber security in Ukraine and statistical data on this issue are presented. It is noted that there is a low number of scientific works on this issue. The main causes of cybercrime are identified. The reasons for the gaps in the normative and legal regulation of the issue of ensuring cyber security in Ukraine are presented. The psychological, social and economic aspects of the above are highlighted. It is noted that cyber security is a broader term than cyber defense. The system of cyber security entities in Ukraine is presented. The levels of cyber security enforcement entities in Ukraine have been determined. A list of special entities in the field of cyber security in Ukraine is provided. The structural elements of the mechanism of combating and preventing cybercrime are defined. The low number of scientific works and studies in the field of implementation of the cyber security mechanism in Ukraine was noted. A conclusion was made regarding the international experience of preventing and countering violence in the field of cybercrime. It was concluded that the lack of a proper mechanism for countering and preventing cyber security in Ukraine leads to the emergence and spread of psychological, economic, sexual, and physical violence, which is a threat to the functioning of the legal Ukrainian state and the development of civil society. A proposal has been submitted for cyber security workers to receive higher education in special educational institutions and, if necessary, take special courses. Attention was drawn to the fact that the educational direction of training cyber security workers, taking into account the rate of growth of cybercrime in Ukraine, in today's conditions should be carried out taking into account the material needs of society and the capabilities of their citizens. It is proposed to note that proper economic and social development of states and society contributes to the absence of high rates of cybercrime.

Key words: *cyber security, violence, causes, directions of prevention, directions of countermeasures, cyber crimes.*

Зважаючи на інтенсивний розвиток віртуального середовища в Україні та поширення використання інтернет-мережі, можемо констатувати необхідність нормативно-правового регулювання та практичного застосування системи кібербезпеки як в Україні, так і за її межами.

Зазначимо, що тлумачення кібербезпеки є різних видів: офіційне та неофіційне. Офіційне роз'яснення вищевказаного правового терміну подається в Законі України «Про основні засади забезпечення кібербезпеки України». Неофіційне тлумачення здійснюється в наукових публікаціях та інтернет-

мережах. Згідно із Законом України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року визначено, що: «Кібербезпека – це комплекс процесів, практичних порад і технологічних рішень, які допомагають захищати важливі системи й мережу від кібератак» [1].

У законодавстві визначено, що: «Оскільки об'єм даних збільшується й усе більше користувачів працюють і спілкуються звідусіль, кіберзлочинці розробляють складні методи, щоб отримувати доступ до ресурсів, викрадати дані, саботувати роботу компаній або вимагати гроші. Щороку кількість атак збільшується, а зловмисники розробляють нові методи для уникнення виявлення. Ефективна програма з кібербезпеки включає фахівців, процеси й технологічні рішення, які разом зменшують ризик перерв у роботі компаній, фінансових втрат і підриву репутації внаслідок атак» [2].

Науковці зазначають, що джерела загрози кіберзлочинності нерівномірно розподілені по всьому світу. Так, найпершою в рейтингу кіберзлочинності стала Росія (58,39 бала), за нею з великим відривом ідуть Україна (36,44 бала), Китай (27,86 бала), США (25,01 бала), Нігерія (21,28 бала) та Румунія (14,83 бала). Велика Британія посідає восьме місце у списку (9,01 бала) [2]. Результати роботи кіберполіції за 2023 рік: виявлено понад 3600 кіберзлочинів. За оперативного супроводу кіберполіції оголошено підозру понад 1700 особам за вчинення понад 3700 злочинів, що на 59% перевищує аналогічний показник у 2022 році. Направлено до суду матеріали щодо 42 організованих злочинних груп, у тому числі 7 злочинних організацій, що на 83% перевищує аналогічний показник у 2022 році [2].

За минулий рік також проведено 18 міжнародних спецоперацій спільно з правоохоронцями з Грузії, Швейцарії, Чехії, Ізраїлю, Норвегії, Нідерландів, Франції, Німеччини та США [2].

За оперативного супроводу кіберполіції направлено до суду обвинувальні акти щодо вчинення понад 4000 злочинів [2]. Відшкодовано майже 144 млн грн збитків (з урахуванням арештованого та вилученого майна) [2]. Заблоковано майже 13 тис. ворожих вебресурсів [2]. Необхідно зазначити, що у правовій науковій спільності не має достатньої кількості, а можна стверджувати про низьку кількість авторефератів на здобуття наукового ступеня кандидата юридичних наук, а тим більше відсутні наукові праці докторів юридичних наук у сфері кібервідносин [3, 4].

Останнє пов'язано із відсутністю фахівців у сфері права інтелектуальної власності, що пояснюється тим, що навчальні посібники з даної навчальної дисципліни є складними для розуміння та сприйняття студентами і викладачами у тому числі [5].

Зважаючи на вищевказані статистичні показники, вважаємо, що кількість виявлених злочинів та порушень є досить незначною, що свідчить про неналежну організацію трудової діяльності суб'єктів протидії та запобігання кіберзлочинності.

Необхідно зазначити, що у вищевказаному нормативно-правовому акті вказано, що даний закон не поширюється на: «1) відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах; 2) діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення; 3) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів; 4) комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем)» [6].

Проте вже у п. 2 статті 4 Закону України «Про основні засади забезпечення кібербезпеки України» визначено, що об'єктами кіберзахисту є: 1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; 2) об'єкти критичної інформаційної інфраструктури; 3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу. Отже, зазначаємо, що ч. 1 п. 1 статті 2 Закону України «Про основні засади забезпечення кібербезпеки України» суперечить п. 1 ч. 2 ст. 4 Закону України «Про основні засади забезпечення кібербезпеки України». Оскільки комунікаційні системи є

і об'єктами кіберзахисту в Україні, і змістом відносин, на які поширюється дія вищевказаного правового акту.

Основними причинами кіберзлочинності є:

1) низький духовний, фізичний та освітній розвиток особи-кіберзлочинця;

2) низька ефективність діяльності компетентних державних органів;

3) відсутність у Кодексі України про адміністративні правопорушення та Кримінальному кодексі України ОКРЕМОЇ ГЛАВИ, яка повинна передбачати кримінальні та адміністративні правопорушення у різних сферах використання віртуальної інформації.

Основними причинами останнього є:

1) психологічні аспекти:

а) воєнний стан в Україні;

б) відсутність освітніх та соціальних навичок;

2) соціальні аспекти, які пов'язані із новітніми технологіями та створенням інтернет-джерел;

3) економічні аспекти, які пов'язані із тимчасовою фінансовою нестабільністю.

Звертаємо увагу на те, що система кібербезпеки та кіберзахисту в Україні складається з: 1) об'єкту (ст. 4); 2) суб'єкту (ст. 5); 3) змісту.

Кібербезпека є терміном ширшим за своїм значенням, ніж кіберзахист, оскільки кіберзахист здійснюється вже при порушенні норм кібербезпеки, а саме під час вчинення адміністративних та кримінальних правопорушень.

Систему суб'єктів забезпечення кібербезпеки в Україні складається з таких рівнів: 1) національний; 2) міністерський; 3) місцевий; 4) спеціалізований.

Перший рівень суб'єктів здійснення кібербезпеки передбачає діяльність, яка здійснюється Національним координаційним центром кібербезпеки, який є робочим органом Ради національної безпеки і оборони України.

Другий рівень суб'єктів здійснення кібербезпеки в Україні передбачає діяльність міністерств та інших центральних органів виконавчої влади.

Третій місцевий рівень суб'єктивного складу відносин у сфері кібербезпеки охоплює діяльність місцевих державних адміністрацій та органів місцевого самоврядування.

Спеціальними органами забезпечення кібербезпеки є: «правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України, інші військові формування, утворені відповідно до закону; Національний банк України; підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; 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» [6].

Окремо необхідно зазначити, що у ч. 2 ст. 8 основного нормативно-правового акту, який регулює відносини захисту прав осіб у кіберпросторі, є перелік суб'єктів національної системи кібербезпеки, а саме:

1) Державна служба спеціального зв'язку та захисту інформації;

2) Національна поліція України;

3) Служба безпеки України;

4) Міністерство оборони України;

5) Генеральний штаб Збройних Сил України;

6) розвідувальні органи;

7) Національний банк України [6].

Окремо наголошуємо про те, що законодавством України визначено суб'єктів забезпечення кібербезпеки та суб'єктів національної системи кіберзахисту, що відрізняється один від одного.

До останніх відносимо виключно органи, які забезпечують захист порушених прав. До першої групи суб'єктів належать органи, які беруть участь у створенні системи кібербезпеки: а це і виконавчі органи влади, і правоохоронні суб'єкти.

Таким чином, можна зробити висновок про те, що основними суб'єктами, які здійснюють захист прав осіб у кібер-відносинах є правоохоронні органи України.

Окремо пропонуємо зазначити про необхідність чіткого визначення у законодавстві України фізичних та юридичних осіб усіх форм власності (приватної у тому числі), які беруть участь у забезпеченні механізму захисту прав осіб у кіберпросторі.

Наприклад, важливою складовою частиною механізму забезпечення та захисту прав осіб у віртуальному середовищі є діяльність таких приватних організацій, як «Київстар», «Приватбанк» та ін., діяльність служб безпек яких повинні відповідати нормам чинного законодавства України!

Належне фінансове забезпечення суб'єктів механізму правових відносин у сфері захисту прав осіб від будь-якого виду насильства у кіберпросторі є одним із напрямів розвитку правової держави та належного функціонування громадянського суспільства.

Результатом правотворчості у відносинах, що є предметом нашого дослідження у

даному підрозділі, є Стратегія кібербезпеки в Україні, яка передбачає виконання таких нормативно-правових актів:

1) Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом: постанова Кабінету Міністрів України від 11 листопада 2020 року № 1176 [7];

2) Про затвердження плану заходів на 2023–2024 роки з реалізації Стратегії кібербезпеки України [8];

3) Індикатори виконання Стратегії кібербезпеки України [9].

Механізм правових відносин у сфері захисту прав осіб від будь-якого виду насильства у кіберпросторі передбачає наявність таких структурних елементів: 1) суб'єкт; 2) об'єкт; 3) засоби; 4) способи; 5) етапи створення та реалізації політики кібербезпеки; 6) відповідальність.

Напрями створення належного механізму забезпечення та захисту прав осіб у кібепросторі:

1) перевірка належності до громадянства України претендентів на посаду;

2) перевірка знань (у тому числі рівень володіння українською мовою) та освіти працівників, які претендують на посаду;

3) оцінка духовного та фізичного розвитку претендентів на посаду.

Механізм протидії та запобігання кіберзлочинності в Україні включає такі структурні елементи: 1) освітня перевірка; 2) державний контроль та нагляд; 3) належна адміністративна та кримінальна відповідальність винних у порушенні законодавства осіб.

Окремо пропонуємо зазначити, що працівники системи забезпечення та захисту прав осіб у кіберпросторі повинні мати: 1) вищу юридичну освіту; 2) спеціальні знання у ІТ-сфері; 3) спеціальні знання у сфері відносин, які є предметом їх діяльності (банківська справа, відносини зв'язку, освіта та ін.).

Проте, зазначаємо, що вищевказане є необхідністю на нетривалий термін, а саме – перші 5 років після прийняття змін до чинного законодавства щодо вищевказаних освітніх вимог. У подальшому, пропонуємо, для претендентів на вищевказані посади отримувати вищу юридичну освіту, освітній ступінь бакалавра в ІТ-сфері та в інших необхідних напрямах (психології, педагогіки, економіки).

Зазначимо, що у структурі Міністерства внутрішніх справ відсутній Департамент кібербезпеки в Україні, що є порушенням загальних принципів права, діяльності правової держави та громадянського сусупільства [10].

Вважаємо, що відділи у державних структурних підрозділах повинні мати назву «Відділи запобігання та протидії кібезлочинності» [11].

Необхідно також додатково зазначити, що в офіційних інтернет-джерелах відсутні статистичні показники та річний звіт щодо діяльності органів кібербезпеки кожної області.

Насамкінець, пропонуємо подати загально правову характеристику кримінально-правової відповідальності у сфері кібервідносин.

Отже, у Кримінальному кодексі України є окремий розділ «Кримінальна відповідальність за кіберзлочини», що включає такі статті:

1) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (стаття 361 Кримінального кодексу України);

2) створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (стаття 361-1 Кримінального кодексу України);

3) 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 (стаття 361-2 Кримінального кодексу України);

4) 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 (стаття 362 Кримінального кодексу України);

5) 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 (стаття 363 Кримінального кодексу України);

6) перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (стаття 363-1 Кримінального кодексу України) [12].

Окремо, необхідно зазначити, що у Кодексі України про адміністративні правопорушення

відсутні адміністративні правопорушення у сфері використання та застосування комунікаційних та технологічних систем.

Кримінальна відповідальність за кіберзлочини карається: 1) штрафом, обмеженням волі, позбавленням волі з позбавленням права обіймати певні посади чи займатися певною діяльністю.

Зважаючи на все вищевказане, пропонуємо також доповнити у правові норми Кримінального кодексу України про те, що у випадку настання летальних наслідків від кіберзлочинів, необхідно міру кримінальної відповідальності збільшити, що є компетентністю представників наукової спільноти у сфері кримінального права.

Пропонуємо також визначати кримінальну відповідальність за кіберзлочини у залежності від майнового стану порушника та його близьких родичів. А це означає, що, якщо особа вчиняє порушення у віртуальному середовищі, то штраф можна визначати у залежності від кількості набутого нерухомого та рухомого майна батьків та інших близьких родичів.

Також зазначимо, що зважаючи на економічну ситуацію в Україні у воєнний період необхідністю є штрафувати злочинців, а вже у випадку повторних кримінальних порушень позбавляти волі чи обмежувати її.

Зазначимо, що під час пошуку правових джерел нормативно-правового регулювання кібербезпеки, у віртуальному середовищі відсутній доступ до наукових статей спеціалістів у даній сфері.

Вважаємо, що основними причинами останнього є:

1) відсутність бажання авторів статей реалізувати політику протидії та запобігання кібербезпеки в Україні та за її межами;

2) значна кількість порушень авторських прав або інших прав у сфері інтелектуальної власності, що призводить до плагіату – незаконного використання авторської інформації;

3) необхідність пошуку інформації у бібліотеках, де повинні знаходитися офіційні джерела публікації наукових статей з різних галузей права.

Щодо останнього, то пропонуємо зазначити, що в останні роки рівень відвідування бібліотек та медіатек малолітніми та неповнолітніми дітьми та їхніх батьків є низьким, що призводить до збільшення часу використання дітьми віртуальних засобів спілкування.

Вважаємо, що вищевказане є однією із передумов виникнення кібер-правопорушень та кіберзлочинів.

Отже, для запобігання та протидії кіберзлочинності необхідним є:

1) підвищення, а в деяких випадках, започаткування духовного розвитку особистості;

2) виховання у сімейному та родинному середовищі дисциплінованості дітей щодо часу використання комп'ютерних технологій, що, на нашу думку, має включати двогодинний ліміт інтернет-ресурсу. У цьому випадку необхідністю є залучення батьків до виховного процесу, що також передбачає вивчення правил поведінки у віртуальному середовищі та виховання самодисципліни;

3) зарахування до освітніх програм спеціальних предметів щодо протидії та запобігання злочинності у віртуальному середовищі;

4) підготовка бакалаврів щодо даної спеціальності;

5) внесення змін до Кодексу про адміністративні правопорушення та Кримінального кодексу України щодо визначення відповідних видів юридичної відповідальності;

6) належна законна система державного нагляду та контролю у вищевказаній сфері.

Здобуття вищої освіти у сфері кібербезпеки є необхідним етапом належного функціонування та реалізації механізму протидії та запобігання насильства в Україні.

Необхідно звернути увагу на те, що освітній напрям підготовки працівників кібербезпеки, зважаючи на темпи зростання кіберзлочинності в Україні, в умовах сьогодення повинен здійснюватися з урахуванням матеріальних потреб суспільства та можливостей їхніх громадян.

А це означає, що у перші 7 років працівниками кібербезпеки можуть бути повнолітні громадяни України, які мають здібності в ІТ-сфері, в тому числі володіють іноземною мовою, пройшли відповідні курси та навчання, здали екзамен без будь-яких корупційних проявів, та мають нормальні показники роботи у кінцевому результаті.

У подальшому, пропонуємо все таки працівникам кібербезпеки отримувати вищу освіту у спеціальних навчальних закладах, та при необхідності проходити спеціальні курси. Але зазначаємо, що виключним у цьому питанні є кримінальне правопорушення «Одержання хабаря» та «Давання хабаря», що є змістом статті 369 Кримінального кодексу України «Пропозиція, обіцянка або надання неправомірної вигоди службовій особі».

Зважаючи на все вищевказане, можемо зробити висновок про те, що відсутність належного механізму протидії та запобігання

кібербезпеки в Україні призводить до виникнення, поширення психологічного, економічного, сексуального, фізичного насильства, що є загрозою функціонування правової Української держави та розвитку громадянського суспільства.

Щодо міжнародного досвіду запобігання та протидії насильства у сфері кіберзлочинності, то пропонуємо зазначити те, що належний економічний соціальний розвиток держав та суспільства сприяє відсутністю високих показників вчинення кіберзлочинів.

Література:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 24.09.2024).
2. В Україні торік виявили 3600 кіберзлочинців URL: https://www.ukrinform.ua/rubric-world/3820636-u-peterburzi-zaavili-pro-vibuhi-ta-potuznu-pozezu.html
3. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ : автореф. дис. … канд. юрид. наук: 12.00.08. Харків, 2016. 14 с. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/8da73c50-5c7d-4ae4-85b4-30fa7107489f/content
4. Буяджи С. А. Правове регулювання боротьби із кіберзлочинністю: теоретико-правовий аспект: автореф. дис. ... канд. юрид. наук: 12.00.01. Теорія та історія держави і права; історія політичних і правових учень. Івано-Франківськ, 2018. URL: https://library.megu.edu.ua:9443/jspui/handle/123456789/1525
5. Джунь В. В. Право інтелектуальної власності: навч. посіб. для студ. вищ. навч. закл. К.: ДП «Видавничий дім «Персонал», 2017. 432 с.
6. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 24.09.2024).
7. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом: постанова Кабінету Міністрів України від 11 листопада 2020 року № 1176 URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text (дата звернення 27.09.2024)
8. Про затвердження плану заходів на 2023–2024 роки з реалізації Стратегії кібербезпеки України URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planu-zakhodiv-na-20232024-roky-z-realizatsii-stratehii-kiberbezpeky-ukrainy-i191223-116 3 (дата звернення 27.09.2024).
9. Індикатори виконання Стратегії кібербезпеки України URL: https://cip.gov.ua/ua/news/strategiya-kiberbezpeki-ukrayini (дата звернення 28.09.2024).
10. До загальної структури Міністерства внутрішніх справ України входять URL: https://mvs.gov.ua/ministry/struktura Структура Національної поліції. URL: https://www.npu.gov.ua/pro-policiyu/struktura-nacionalnoyi-policiyi
11. Кримінальний кодекс України від 5 квітня 2001 року. Відомості Верховної Ради України. 2001. № 25-26. ст. 131.