УДК 342.7:[34:004](477)

https://doi.org/10.52058/2786-5274-2023-13(27)-317-328

Повалена Мар'яна Василівна кандидат юридичних наук, доцент кафедри адміністративного та інформаційного права, Інститут права, психології та інноваційної освіти, Національний університет «Львівська політехніка», доцент кафедри теорії права, конституційного та приватного права, Інститут з підготовки фахівців для підрозділів Національної поліції, Львівський державний університет внутрішніх справ, м. Львів, https://orcid.org/0000-0001-5638-200X

КІБЕРПОЛІЦІЯ ТА ВИКЛИКИ ДОТРИМАННЯ ПРАВ ЛЮДИНИ: БАЛАНС МІЖ БЕЗПЕКОЮ ТА СВОБОДОЮ В МЕРЕЖІ ІНТЕРНЕТ

Анотація. В статті описано діяльність кіберполіції у сфері прав людини. Кіберризики та кіберзагрози дедалі збільшуються, запобігання та протидія яким вимагає якнайшвидшого втручання та обізнаності всіх зацікавлених сторін щодо пов'язаних з ними чинників ризику. Індивідуальні свободи та права нерозривно поєднані з особистою, соціальною та національною безпекою. Тому є нагальна потреба віднайти баланс між безпекою та свободою в мережі Інтернет.

Метою цієї статті є вивчення особливих функцій кіберполіції, які забезпечують баланс між безпекою та свободою з дотриманням прав людини. Департамент кіберполіції Національної поліції України — це внутрішній підрозділ Національної поліції України, який займається боротьбою зі злочинністю в цифровому просторі та входить до складу Національної кримінальної поліції, що відповідає за реалізацію державної політики у сфері протидії кіберзлочинності. Департамент кіберполіції є порівняно новим підрозділом, який аналізує та застосовує у своїй роботі зарубіжний досвід. У статті обґрунтовано значення Департаменту кіберполіції Національної поліції України, як міжрегіональної інституції, яка виконує завдання Національної поліції України у боротьбі з кіберзлочинністю, надаючи інформацію та консультації органам державної влади. Визнано, що наразі є нагальна потреба у правовому регулюванні мережі Інтернет для забезпечення балансу між безпекою та свободою учасників. Кіберполіція є тимчасовим органом Національної податкової служби України та покликана сприяти реалізації державної політики у сфері протидії кіберзлочинності. Кіберзлочинність має вирішальне значення для ланцюга незаконних, а подекуди й злочинних інформаційних операцій. На співробітників кіберполіції покладено завдання створювати джерела для фішингу, виявляти кібершахрайство та інші

правопорушення, атакувати кіберзлочинців через соціальні мережі, додатки для обміну повідомленнями та Telegram-канали, а також запобігати передачі порнографічних матеріалів. Як наслідок, цей правоохоронний орган працює над протидією використанню великих даних для злочинів, що порушують безпеку персональних даних і приватної інформації.

Ключові слова: департамент, кіберполіція, Національна поліція України, діяльність, безпека.

Povalena Mariana Vasylivna PhD in Law, Assistant professor of the Department of administrative and informational law of Educational and Scientific Institute of Jurisprudence, Psychology and Innovative Education Lviv Polytechnic National University, Assistant professor of the Department of Theory of Law, Constitutional and Private Law, Institute for the Training of Specialists for Units of the National Police, Lviv State University of Internal Affairs, Lviv, https://orcid.org/0000-0001-5638-200X

CYBER POLICING AND HUMAN RIGHTS CHALLENGES: BALANCING SECURITY AND FREEDOM ON THE INTERNET

Abstract. The article describes the activities of the cyberpolice in the field of human rights. Cyber risks and cyber threats are increasing, preventing, and combating which requires early intervention and awareness of all stakeholders of the risk factors involved**.** Individual freedoms and rights are inextricably linked to personal, social and national security. Therefore, there is a pressing need to strike a balance between security and freedom on the Internet.

The purpose of this article is to study the special functions of cyberpolice that ensure a balance between security and freedom in compliance with human rights**.** The Cyberpolice Department of the National Police of Ukraine is an internal unit of the National Police of Ukraine that deals with combating crime in the digital space and is part of the National Criminal Police, which is responsible for implementing the state policy in the field of combating cybercrime. The Cyber Police Department is a relatively new unit which analyses and applies foreign experience in its work. **In the article was grounded the value of the Cyber Police Department of the National Police of Ukraine as an interregional institution, fulfilling the tasks of the National Police of Ukraine in combating cybercrime by providing information and advice to public authorities.** It is recognised that there is an urgent need for legal regulation of the Internet to ensure a balance between security and the freedoms of participants. The Cyberpolice is a temporary body of the National Tax Service of Ukraine and is designed to facilitate the implementation of the state policy in the field of combating cybercrime. Cybercrime is crucial for the chain of illegal and sometimes criminal information operations. Cyberpolice officers are tasked with identifying sources of phishing, detecting cyber fraud and other

offences, attacking cybercriminals through social media, messaging apps and Telegram channels, and preventing the transmission of pornographic material. As a result, this law enforcement agency is working to counteract the use of data for crimes that violate the security of personal data and private information.

Keywords: department, cyber police, National Police of Ukraine, activity, security.

Постановка проблеми. З розвитком технологій, інформаційного суспільства та поступовою трансформацією суспільства в бік цифровізації, активне застосування цифрових технологій у всіх сферах життя, поставило питання про необхідність і достатність прав і свобод людини, розрізняючи концепцію цифрової людини. Сьогодні мережа Інтернет є прямим інструментом реалізації прав і свобод людини та платформою для участі громадян у демократичних процесах, а отже, потребує захисту та реалізації прав людини. Нажаль, нинішній рівень захисту є доволі низьким і вимагає вдосконалення задля покращення практики дотримання прав людини. Сучасна реальність є такою, що кіберзагрози швидко прогресують, а кіберзлочинність стає дедалі складнішою, організованішою та транснаціональнішою. Це відбувається тому, що мережа Інтернет, цифрові послуги та інформаційно-комунікаційні технології (ІКТ) стали невід'ємною частиною глобальної економіки — від електронного документообігу, онлайн-покупок та онлайн-банкінгу до систем мережі Інтернет речей та інтелектуальних систем управління підприємством. Оскільки бізнес і підприємництво стають все більш залежними від використання ІКТ, кіберризики та кіберзагрози зростають, а це вимагає завчасних дій для їхнього запобігання або усунення, а також підвищення інформованості про чинники ризику для всіх зацікавлених сторін. Індивідуальні права і свободи невіддільні від безпеки індивідів, суспільств і держав. Тому виникає нагальна потреба в досягненні балансу між безпекою та свободою в мережі Інтернет

Аналіз останніх досліджень і публікацій. Аналізуючи джерела з теми статті, можна дійти висновку, що тема діяльності кіберполіції викликає значний інтерес у вітчизняних науковців, наприклад, цю тему досліджували В. Береза [1], Г. Шевчук [15] та інші.

Важливою для цього дослідження є стаття Ю. Хоббі, в якій охарактеризовано права людини на кібербезпеку, як одного з інформаційних прав людини [14].

Змістовні характеристики та аналіз ролі та місця Департаменту кіберполіції Національної поліції України у системі суб'єктів забезпечення кібербезпеки держави висвітлила в своєму дослідженні Т. Білоброва [16].

Доречно зазначити, що праця Т. Ткач [13] дає додатковий матеріал щодо організації кіберполіції в Україні.

Проте треба враховувати, що проблема дослідження потребує проведення поглибленого аналізу. Тому аналіз нормативно–правової бази

українського законодавства доповнює теоретичну основу даного наукового дослідження.

Мета статті — дослідження особливостей дотримання прав людини кіберполіцією, забезпечення балансу між безпекою та свободою в мережі Інтернет.

Виклад основного матеріалу. Сьогодні людство живе в інформаційному суспільстві. Інформаційні технології та глобальні комп'ютерні мережі стали невід'ємною частиною всіх видів людської діяльності та дають змогу людям легше отримувати доступ до інформації, спілкуватися з іншими людьми та проводити дозвілля. Однак інформаційні технології та мережа Інтернет мають як безсумнівні переваги, так і недоліки. Зловживання інформаційними технологіями є причиною існування інтернет-поліції.

В сучасних умовах інформаційна безпека — це не лише гарантування безпеки інформації, що зберігається або зберігалася на електронних носіях, серверах і персональних пристроях. Це також раціональна інформаційна політика на рівні держави та компаній, яка не обмежує законні права людини та громадянина на доступ до інформації і в такий спосіб регулює інформаційні відносини.

Отже, концепція інформаційної безпеки сприяє, з одного боку, забезпеченню надання якісної інформації та вільного доступу громадян до різних джерел інформації, а з іншого — захисту інтересів суспільства і держави, зміцненню здоров'я населення, захисту від несприятливого інформаційного впливу, забезпеченню одержання громадянами повної та якісної інформації. Це також передбачає регулювання щодо унеможливлення поширення інформації.

Сьогодні роль соціальних мереж в Інтернеті значно зросла. Люди створюють і надсилають текстові, фото- та відео повідомлення в мережі Інтернет, спілкуються з друзями, вітають із днем народження, знайомляться з новими людьми, просять про допомогу тощо. Соціальні інформаційні системи стали частиною повсякденного життя. Тому цей соціальний розвиток не може бути проігнорований поліцією, яка зобов'язана стежити за дотриманням громадянами правопорядку в інтернеті.

Інтернет-поліція — це збірний термін для позначення поліції, державних органів, міністерств і кіберполіцій, що відповідають за контроль мережі Інтернет у всьому світі. Основні завдання інтернет-поліції в кожній державі різні, але вони стосуються боротьби з кіберзлочинністю, контролю громадської думки в мережі Інтернет, цензури і пропаганди, тобто численних заходів, яких вживають держави для контролю за використанням мережі Інтернет.

Як зауважує Г. Шевчук, запобігання кіберзлочинності зараз має бути комплексним, спрямованим на мінімізацію ризиків кіберзагроз та збільшення засобів і методів захисту у віртуальному просторі [15].

Українські поліцейські структури прагнуть йти в ногу з цими змінами. В Україні досить ефективно працює кіберполіція, з якою громадяни активно співпрацюють і на яку покладаються в різних питаннях, зокрема й у сфері кібербезпеки. Водночас поліцейські через доступ до соціальних мереж мають можливість отримувати доступ до необхідної інформації.

Люди сприймають технології, як необхідність використання їх, як в робочому процесі так і в особистих комунікаціях. Такий підхід дає поліцейським високий ступінь свободи, допомагаючи їм контролювати тих, хто використовує соціальні мережі в злочинних цілях, і запобігати потенційним загрозам та їхнім джерелам.

Поліцейські реагують на різні соціальні мережі та обирають модульний підхід. Це дає їм змогу реагувати на зміни, наприклад, на мережу, яка не є популярною сьогодні, але буде дуже популярною з-поміж населення завтра.

Комплексний моніторинг мережі Інтернет є складним процесом. Це пов'язано не лише з тим, що мережа Інтернет не має кордонів, а й з тим, що закони, які регулюють її використання, а також методи фільтрації та блокування контенту є специфічними для кожної країни. Тому інформація, яка порушує закони певної країни і блокується національними ресурсами, може бути розміщена на веб серверах в інших країнах. Крім того, мережа Інтернет наразі не перебуває під загальним контролем, а розподілений між багатьма комерційними організаціями.

Постановою КМУ № 831 [12] створено Департамент кіберполіції як міжрегіональний орган Національної поліції («кіберполіція»). Саме ця організація реалізує державну політику у сфері протидії кіберзлочинності та є провідним органом кіберзахисту в Україні. Департамент кіберполіції Національної поліції України — міжрегіональний орган Національної поліції України, що входить до складу кримінальної поліції Національної поліції, який відповідно до законодавства України забезпечує реалізацію державної політики у сфері протидії кіберзлочинності, організовує та проводить оперативно-розшукову діяльність відповідно до законодавства.

Департамент кіберполіції Національної поліції України, який є новоствореною організацією, також зосереджує увагу на аналізі та застосуванні іноземного досвіду у своїй діяльності.

Як міжрегіональний орган Національної поліції України, Департамент кіберполіції Національної поліції України забезпечує реалізацію державної політики у сфері протидії кіберзлочинності відповідно до законодавства України та здійснює інформаційно-аналітичне забезпечення керівництва Національної поліції України та органів державної влади про стан справ з питань, віднесених до його компетенції. Одним із завдань Департаменту є своєчасний розгляд звернень і запитів громадян, підприємств, установ та організацій з питань, що належать до компетенції кіберполіції, а також контроль за дотриманням порядку їх прийняття, реєстрації, обліку та розгляду.

Кіберполіція також має проводити інформаційно-роз'яснювальну роботу серед населення щодо використання нових технологій у повсякденному житті та дотримання законодавства України у сфері захисту від кіберзагроз та протидії їм, але незрозуміло, як саме це має відбуватися.

В цьому контексті роль Національної поліції полягає у захисті прав і свобод людини і громадянина, а також інтересів суспільства і держави від злочинних посягань у кіберпросторі, створюючи в такий спосіб необхідні умови для розбудови безпечного життєвого середовища, що є основою безпеки України. Тобто метою створення кіберполіції є організація ефективних заходів протидії кіберзлочинності та забезпечення дієвого впливу на оперативну обстановку в цій сфері [16].

Інакше кажучи, теоретично можна було б звернутися до цього департаменту для реалізації права на кібербезпеку та захист, але до його функцій не входило б безпосереднє забезпечення кібербезпеки громадян, а лише запобігання, виявлення та припинення злочинів у сфері протидії кіберзлочинності.

Слід зазначити, що на законодавчому рівні немає розмежування між основними та другорядними функціями, є уніфікований перелік функцій, які стосуються різних аспектів діяльності поліції. Однак, з огляду на специфіку завдань, функцій та повноважень кіберполіції у сфері інформаційної безпеки, необхідно зазначити, що кіберполіція є складною системою, яка характеризується самостійним структурним підрозділом поліції, єдністю та цілісністю всіх елементів, особливим порядком призначення та функціонування тощо. Крім того, для забезпечення інформаційної безпеки важливо шукати нові та ефективні форми і методи, які разом з іншими правоохоронними органами допоможуть поліції вирішувати всі завдання із захисту життєво важливих інтересів особи, суспільства і держави. У зв'язку з цим необхідна чітка правова база при встановленні правил, що регулюють діяльність поліцейських організацій у сфері інформаційної безпеки.

Кіберпростір, поряд з іншими фізичними просторами, визнаний одним з театрів воєнних дій. Зростає тенденція до створення кібервійськ, які не лише захищають критично важливу інформаційну інфраструктуру від кібератак, але й проводять превентивні ударні операції в кіберпросторі, наприклад, виводять з ладу та нейтралізують інформаційні системи, які контролюють ключові об'єкти противника.

Насамперед у боротьбі з шахраями необхідно дотримуватися елементарних правил кібергігієни. Водночас важливо пам'ятати, що під час війни навіть перевірені ЗМІ та посадовці можуть припускатися помилок. Прочитавши важливу новину, варто дочекатися її спростування або підтвердження. У випадку з «Діпфейками» [2] ситуацію ускладнюють фейкові відео з публічними особами та прослуховуванням їхніх виступів. Наприклад, Центр інформаційної безпеки повідомив, що в мережі Інтернет може з'явитися

відео виступу президента Володимира Зеленського, який нібито говорить про капітуляцію. Однак це використовується для того, щоб заплутати слухачів і деморалізувати громадян. У цьому випадку спершу варто звернути увагу на такі ознаки: неприродний тон голосу, текстура шкіри, тіні на обличчі, «мерехтіння кадру», кліпання очима тощо. Головне — довіряти лише офіційним ЗМІ.

З-поміж пріоритетних завдань, що постають перед українськими державними інституціями у сфері забезпечення інформаційного та цифрового суверенітету, — автоматичний моніторинг інформаційного простору, запровадження законодавства щодо відповідальності за контент, впровадження законодавчих норм, які регулюватимуть фільтрацію інтернет-контенту, впровадження законодавства щодо суспільно шкідливих ідей та закликів (расизм, ксенофобія, екстремізм), запобігання розповсюдженню сучасних технологій, захист культур та мов в мережі Інтернет.

Одним з головних завдань кіберполіції є збереження балансу між безпекою та свободою в мережі Інтернет (табл. 1).

Таблиця 1

Основні заходи забезпечення балансу між безпекою та свободою в мережі Інтернет

Захист свободи слова	Забезпечити свободу слова і захист прав людини в мережі Інтернет з дотриманням необхідних протоколів безпеки, вживати всіх практичних заходів для запобігання появі цензури в мережі Інтернет.
Безпечне використання мережі Інтернет і протидія кіберзлочинності	Активно долучатися до боротьби з кіберзлочинністю та розвивати співробітництво з урядовими та неурядовими організаціями в цій галузі. Дотримуватися українського законодавства в галузі запобігання розкраданню обладнання та порушення прав третіх осіб.
Захист телекомунікацій та інформаційна безпека	Сприяти вдосконаленню правових механізмів, спрямованих на посилення відповідальності за шкоду, заподіяну інфраструктурі.

Джерело: Складено автором на основі власних спостережень.

З таблиці видно, що кіберполіція вживає всіх можливих заходів для сприяння свободі вираження поглядів і прав людини в мережі Інтернет та запобігання цензурі в мережі Інтернет, забезпечуючи водночас необхідні

умови безпеки. Цензура в мережі Інтернет — це регулювання або призупинення публікації інформації чи доступу до інформації в мережі Інтернет. В цьому сенсі цензуру треба чітко відрізняти від припинення кримінальних або інших антигромадських публікацій, що може бути пов'язано із захистом інформаційного простору і відповідати принципам Європейської конвенції з прав людини, згідно з якими держави можуть фільтрувати інформацію, яка суперечить їхнім законам.

З іншого боку, якщо розглядати цензуру з погляду міжнародного права та міжнародних організацій, то експерти визначають цензуру як негативне явище, що перешкоджає поширенню достовірної інформації та заважає вільнодумству і розвитку суспільства загалом.

Також триває активна робота з протидії кіберзлочинності, розвивається співпраця в цій сфері з державними та недержавними організаціями через забезпечення дотримання законодавства України та положень Конвенції про кіберзлочинність, імплементація Конвенції в національне законодавство, а також захист інтересів через реалізацію інших видів участі в цій сфері. Наша держава ратифікувала Конвенцію Ради Європи про кіберзлочинність [9], Загальну декларацію прав людини [3], Міжнародний пакт про громадянські та політичні права [5], Міжнародний пакт про економічні, соціальні та культурні права [6], Конвенцію проти катувань та інших жорстоких, нелюдських або таких, що принижують гідність, видів поводження і покарання, та інші міжнародні документи з прав людини [4]. Отже, загалом українське законодавство відповідає міжнародним стандартам у цій сфері.

Щодо внутрішнього регулювання, то в Україні це питання забезпечується Законами України «Про національну безпеку України» від 21 червня 2018 року [7] і «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року [8]. 15 березня 2016 року Україна ухвалила Стратегію кібербезпеки [11]. Стратегія кібербезпеки України визначає принципи, на яких має базуватися інформаційне суспільство: повага до верховенства права, прав і свобод людини та громадянина; забезпечення національних інтересів України; відкритість, доступність, стабільність та доступ до інформації, що є основою інформаційного суспільства. Відповідно до законодавства України, кібербезпека — захищеність життєво важливих інтересів людини і громадянина, суспільства і держави під час використання кіберпростору, сталого розвитку інформаційного суспільства та цифрового комунікаційного середовища, реальних і потенційних загроз національній безпеці України в кіберпросторі, — це гарантія їх своєчасного виявлення, запобігання та нейтралізації.

Водночас, триває процес розмежування різноманітних видів безпеки на певних геополітичних рівнях і розуміння ролі кібербезпеки на кожному з них.

Потреба в такому усвідомленні ролі кібербезпеки зумовлена насамперед активізацією діяльності міжнародних терористичних організацій, екстре-

містських організацій та злочинних угруповань, а також поодиноких держав, які здійснюють кібервплив на громадян, суспільства та держави для здійснення власних цілей. Тому питання забезпечення кібербезпеки на міжнародному, регіональному та національному рівнях є одним із найважливіших складників системи національної безпеки будь-якої держави.

Варто зазначити, що значну увагу приділяють аналізу національної стратегічної ситуації щодо кіберзагроз, консолідації та розповсюдженню даних про відповідні інциденти задля ефективнішого реагування, а також підготовці регулярних публічних звітів щодо кіберзагроз не рідше, ніж раз на рік і їхньому вчасному оприлюдненню на відповідних вебсайтах. Безперечно, дієва нормативно-правова база є основою ефективної системи кібербезпеки, а тому особливого значення набуває Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» [10]. Ця стратегія створює можливості для побудови найбільш вільного, безпечного, відкритого та стабільного кіберпростору в інтересах дотримання прав людини. Сьогодні, коли Україна опинилася в умовах воєнного стану, важливо, щоб не лише ІТ-фахівці, а й усі громадяни мали необхідні знання з цифрової грамотності, цифрового етикету та кібергігієни. Коли почалася війна, ІТ-фахівці з усієї України долучилися до кіберполіції та змогли дати відсіч загарбникам. Внаслідок їхніх злагоджених дій головні інформаційні системи окупаційних військ виявилися непридатними для застосування.

Розвиток потенціалу кібербезпеки у сфері безпеки та оборони потребує розроблення та впровадження ефективних інструментів і засобів реагування на агресію в кіберпросторі, що можуть бути використані як інструмент стримування воєнних конфліктів і загроз в інформаційному просторі.

Кіберполіція може сприяти вдосконаленню правових механізмів, спрямованих на посилення відповідальності за шкоду, заподіяну інфраструктурі телекомунікаційних мереж, та забезпечення адекватного реагування відповідних державних органів на випадки викрадення або пошкодження кабелів та обладнання.

Діяльність кіберполіції спрямована на розкриття злочинів, пов’язаних зі створенням фішингових ресурсів, проведенням фішингових атак, інтернет-шахрайства з використанням соціальних мереж, месенджерів і Telegram-каналів, а також на запобігання розповсюдженню порнографічних матеріалів. Відтак, правоохоронне відомство працює над злочинами, що використовують великі дані і загрожують інформаційній безпеці та персональним даним. Зокрема, у воєнний час ним було виявлено безліч злочинців, які ошукували людей під виглядом гуманітарної допомоги, державних виплат і перевезення з поля бою, а також заблоковано безліч ворожих інтернет-ресурсів, що розміщували дезінформацію та російську пропаганду і вводили людей в оману.

Отже, передові державні органи, що захищають кіберпростір в Україні, використовують великі дані та технічні знання для запобігання злочинам проти персональних даних і національної безпеки.

Висновки. Тож можна дійти висновку, що наразі є нагальна потреба в законодавчому регулюванні інтернет-мереж задля дотримання балансу між безпекою та свободою учасників. Кіберполіція є міжрегіональним підрозділом Національної податкової служби України, який забезпечує реалізацію державної політики у сфері протидії кіберзлочинності. Кіберзлочинність є потрібною ланкою в ланцюгу між свободою публічної інформації та незаконними, подекуди злочинними, інформаційними операціями. Кіберполіція вживає всіх можливих заходів для сприяння свободі вираження думок і прав людини в мережі Інтернет, а також для запобігання цензурі в мережі Інтернет, підтримуючи водночас необхідні умови безпеки. Основними заходами забезпечення балансу між безпекою та свободою в мережі Інтернет є безпечне використання його і протидія кіберзлочинності, захист свободи слова, телекомунікацій та інформаційну безпеку.

Діяльність кіберполіції охоплює виявлення таких правопорушень, як кібершахрайство через створення фішингових ресурсів, фішингові атаки, кібершахрайство з використанням соціальних мереж, месенджерів і Telegram-каналів, а також запобігання поширенню порнографічних матеріалів. Отже, цей правоохоронний орган покликаний протидіяти використанню великих даних для вчинення злочинів, що загрожують безпеці персональних даних і приватної інформації.

Питання діяльності кіберполіції в умовах воєнного стану потребує більш детального аналізу в майбутніх дослідженнях.

Література:

1. Береза В. В. Щодо визначення функцій департаменту кіберполіції національної поліції України. Держава та регіони. 2019. Vol. 82, no. 3. P. 30–39. URL: https://doi.org/10.32631/v.2018.3.03 (дата звернення: 17.10.2023)

2. Діпфейк. URL: https://slovotvir.org.ua/words/dipfeik

3. Загальна декларація прав людини: Декларація Орг. Об'єдн. Націй від 10.12.1948 р. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 17.10.2023).

4. Конвенція проти катувань та інших жорстоких, нелюдських або таких, що принижують гідність, видів поводження і покарання : Конвенція Орг. Об'єдн. Націй від 10.12.1984 р. : станом на 13 листоп. 1998 р. URL: https://zakon.rada.gov.ua/laws/show/995_085#Text (дата звернення: 17.10.2023).

5. Міжнародний пакт про громадянські і політичні права : Пакт Орг. Об'єдн. Націй від 16.12.1966 р. : станом на 19 жовт. 1973 р. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (дата звернення: 17.10.2023).

6. Міжнародний пакт про економічні, соціальні і культурні права : Пакт Орг. Об'єдн. Націй від 16.12.1966 р. : станом на 19 жовт. 1973 р. URL: https://zakon.rada.gov.ua/laws/show/995_042#Text (дата звернення: 17.10.2023).

7. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 17.10.2023).

8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 17 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 17.10.2023).

9. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 р. № 2824-IV : станом на 14 жовт. 2010 р. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text (дата звернення: 17.10.2023).

10. Про Стратегію кібербезпеки України : Рішення Ради нац. безпеки і оборони України від 14.05.2021 р. : станом на 28 серп. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/n0055525-21#Text (дата звернення: 17.10.2023).

11. Про Стратегію кібербезпеки України : Рішення Ради нац. безпеки і оборони України від 27.01.2016 р. : станом на 18 берез. 2016 р. URL: https://zakon.rada.gov.ua/laws/show/n0003525-16#Text (дата звернення: 17.10.2023).

12. Про утворення територіального органу Національної поліції: Постанова Кабінету Міністрів України від 13.10.2015 р. №831. URL: https://zakon.rada.gov.ua/laws/show/831-2015-п#Text (дата звернення: 17.10.2023).

13. Ткач Т. В. Юридичні гарантії діяльності департаменту кіберполіції національної поліції україни. Scientific journal of public and private law. 2019. № 6. С. 240–245. URL: https://doi.org/10.32844/2618-1258.2019.6.42 (дата звернення: 17.10.2023).

14. Хоббі Ю. Право людини на кібербезпеку: проблеми визначення та гарантування. Юридичний вісник. 2020. № 2. С. 37–43. URL: https://doi.org/10.32837/yuv.v0i2.1701 (дата звернення: 17.10.2023).

15. Шевчук Г. В. Особливості діяльності департаменту кіберполіції національної поліції україни. Scientific journal of public and private law. 2019. Т. 3, № 1. С. 244–249. URL: https://doi.org/10.32844/2618-1258.2019.3-1.42 (дата звернення: 17.10.2023).

16. Bilobrova T. V. Role and place of the Cyber Police Department of the National Police of Ukraine in the system of subjects for providing cybersecurity of a state. Legal novels. 2020. No. 11. P. 127–132. URL: https://doi.org/10.32847/ln.2020.11.17 (date of access: 17.10.2023).

References:

1. Bereza, V. V.(2019) Shchodo vyznachennia funktsii departamentu kiberpolitsii natsionalnoi politsii Ukrainy.[Regarding the definition of the functions of the Cyber Police Department of the National Police of Ukraine.] Derzhava ta rehiony — State and regions, 82(3). 30–39. [in Ukrainian]

2. Deepfake. URL: https://slovotvir.org.ua/words/dipfeik

3. Zahalna deklaratsiia prav liudyny: Deklaratsiia Orh. Obiedn. Natsii vid 10.12.1948 [Universal Declaration of Human Rights, United Nations Declaration (1948).].zakon.rada.gov.ua Retrieved from zakon.rada.gov.ua/laws/show/995_015#Text [in Ukrainian]

4. Konventsiia proty katuvan ta inshykh zhorstokykh, neliudskykh abo takykh, shcho prynyzhuiut hidnist, vydiv povodzhennia i pokarannia : Konventsiia Orh. Obiedn. Natsii vid 10.12.1984 r. : stanom na 13 lystop. 1998 r.[Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Convention United Nations (1998)] zakon.rada.gov.ua Retrieved from: https://zakon.rada.gov.ua/laws/show/995_085#Text (data zvernennia: 17.10.2023).

5. Mizhnarodnyi pakt pro hromadianski i politychni prava : Pakt Orh. Obiedn. Natsii vid 16.12.1966 r. : stanom na 19 zhovt. 1973 r.[International Covenant on Civil and Political Rights, United Nations Covenant (1973).] zakon.rada.gov.ua Retrieved from: https://zakon.rada.gov.ua/laws/show/995_043#Text [in Ukrainian]

6. Mizhnarodnyi pakt pro ekonomichni, sotsialni i kulturni prava : Pakt Orh. Obiedn. Natsii vid 16.12.1966 r. : stanom na 19 zhovt. 1973 r.[International Covenant on Economic, Social and Cultural Rights, United Nations Covenant (1973).] zakon.rada.gov.ua Retrieved from: https://zakon.rada.gov.ua/laws/show/995_042#Text [in Ukrainian]

7. Pro natsionalnu bezpeku Ukrainy : Zakon Ukrainy vid 21.06.2018 r. № 2469-VIII : stanom na 31 berez. 2023 r.[On National Security of Ukraine, Law of Ukraine No. 2469-VIII (2023) (Ukraine).] zakon.rada.gov.ua Retrieved from: https://zakon.rada.gov.ua/laws/show/2469-19#Text [in Ukrainian]

8. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid 05.10.2017 r. № 2163-VIII : stanom na 17 serp. 2022 r.[On the main principles of ensuring cyber security of Ukraine, Law of Ukraine No. 2163-VIII (2022) (Ukraine).] zakon.rada.gov.ua Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian]

9. Pro ratyfikatsiiu Konventsii pro kiberzlochynnist : Zakon Ukrainy vid 07.09.2005 r. № 2824-IV : stanom na 14 zhovt. 2010 r.[On the ratification of the Cybercrime Convention, Law of Ukraine No. 2824-IV (2010) (Ukraine)] zakon.rada.gov.ua Retrieved from:https://zakon.rada.gov.ua/laws/show/2824-15#Text [in Ukrainian]

10. Pro Stratehiiu kiberbezpeky Ukrainy : Rishennia Rady nats. bezpeky i oborony Ukrainy vid 14.05.2021 r. : stanom na 28 serp. 2021 r.[About the Cybersecurity Strategy of Ukraine, Decision of the National Security and Defense Council of Ukraine (2016)] zakon.rada.gov.ua Retrieved from:https://zakon.rada.gov.ua/laws/show/n0055525-21#Text [in Ukrainian]

11. Pro Stratehiiu kiberbezpeky Ukrainy : Rishennia Rady nats. bezpeky i oborony Ukrainy vid 27.01.2016 r. : stanom na 18 berez. 2016 r.[About the Cybersecurity Strategy of Ukraine, Decision of the National Security and Defense Council of Ukraine (2021)] zakon.rada.gov.ua Retrieved from: https://zakon.rada.gov.ua/laws/show/n0003525-16#Text [in Ukrainian]

12. Pro utvorennia terytorialnoho orhanu Natsionalnoi politsii: Postanova Kabinetu Ministriv Ukrainy vid 13.10.2015 r. №831.[On the establishment of a territorial body of the National Police: Resolution of the Cabinet of Ministers of Ukraine dated 13.10.2015] zakon.rada.gov.ua Retrieved from:https://zakon.rada.gov.ua/laws/show/831-2015-p#Text [in Ukrainian]

13. Tkach, T. V.(2019) Yurydychni harantii diialnosti departamentu kiberpolitsii natsionalnoi politsii ukrainy.[Legal guarantees of the cyber police department of the National Police of Ukraine]. Scientific journal of public and private law. 6. 240–245. [in Ukrainian]

14. Khobbi, Yu.(2020) Pravo liudyny na kiberbezpeku: problemy vyznachennia ta harantuvannia.[The human right to cyber security: problems of definition and guarantee.] Yurydychnyi visnyk — Legal Bulletin, (2), 37–43. [in Ukrainian]

15. Shevchuk, H. V.(2019) Osoblyvosti diialnosti departamentu kiberpolitsii natsionalnoi politsii ukrainy. [Peculiarities of the Cyber Police Department of the National Police of Ukraine].Scientific journal of public and private law, 3(1), 244–249. [in Ukrainian]

16. Bilobrov, T. V. (2020). Role and place of the Cyber Police Department of the National Police of Ukraine in the system of subjects for providing cybersecurity of a state. Legal novels, (11), 127–132. https://doi.org/10.32847/ln.2020.11.17