УДК 341.01
DOI https://doi.org/10.24144/2307-3322.2021.64.71

МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА КІБЕРШАХРАЙСТВУ

Саєнко М.І.,
доцент, кафедри теорії та історії держави і права,
кандидат юридичних наук, доцент
Дніпропетровського державного університету внутрішніх справ
ORCID:https://orcid.org/0000-0003-1768-2143

Савела Є.А.,
слухач магістратури факультету
підготовки фахівців для органів досудового розслідування
Дніпропетровського державного університету внутрішніх справ

Тополянський Ю.Ю.,
слухач магістратури факультету
підготовки фахівців для органів досудового розслідування
Дніпропетровського державного університету внутрішніх справ

Саєнко М.І., Савела Є.А., Тополянський Ю.Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству

У статті розглянуто механізми протидії кіберзлочинності та кібершахрайству боротьби з ними на міжнародному рівні (в системі ООН), проаналізовано міжнародні правові акти, які регулюють процес боротьби з зазначеними явищами. Акцентовано, увагу на масштабній проблемі світового співтовариства щодо кіберзлочинності та кібершахрайтва, чисельність яких щороку зростає. Незважаючи на активне зростання ІТ індустрії та інформаційного простору, бізнес все ще, не до кінця усвідомлює значимість кібербезпеки. Потенційними жертвами злочинних посягань стають як населення, так і державні (недержавні) організації.

Під кібербезпекою розуміється насамперед оперативне реагування на загрози всередині мережі Інтернет. Зазначається, що в більшості випадків об'єктами кібератак стають інтернет речей і промисловий інтернет речей, так як, по-перше, невисока ступінь захисту пристроїв і портів, хмарних додатків, інтерфейсів програмування додатків; по-друге, відсутні стандарти підтримки безпеки.

Вивчено міжнародний досвід протидії таким новим викликам і загрозам, як кіберзлочинність, кібершахрайство, інформаційний тероризм, фішинг, вішинг та смішинг, цілеспрямований фішинг, видавання себе за іншу особу та інші способи кібершахрайства, операції інформаційної боротьби, з якими не здатна впоратися кожна окремо з країн.

Проаналізовано міжнародні правові акти з досліджуваної тематики, такі як: Конвенція «Про кіберзлочинність», Директива про протидію сексуальній експлуатації дітей онлайн і дитячої порнографії, Директива щодо атак проти інформаційних систем, Директива про безпеку мереж та інформаційних систем.

Відзначено важливість інтернаціональних договорів в даній сфері, серед яких Модельний Закон Співдружності Націй про комп'ютерні злочини 2002 р., Модельний Закон країн Карибського Басейну про кіберзлочинність (проект HIPCAR), спільний проект Європейського союзу і Міжнародного Союзу Електрозв'язку для держав Тихоокеанського регіону, проект ООН з розробки законодавства в галузі кіберзлочинності для країн Африки.

Ключові слова: кіберзлочинність, кібершахрайство, комп'ютерні системи, кібератаки, фішинг, вішинг, смішинг, цілеспрямований фішинг, видавання себе за іншу особу, технології, мережа Internet, правові механізми, декларації, правові акти.

Saenko M.I., Savela E.A., Topolyansky Y.Y. International experience against cyber crime and cyber crime

The article considers the concept of cybercrime, mechanisms for combating it at the international level (in the UN system), analyzes international legal acts governing the process of combating cybercrime. It is noted that today a large-scale problem of the world community is cybercrime, the number of which is growing every year. Despite the active growth of the IT industry and information space, businesses are still not fully aware of the importance of cybersecurity. Both the population and state (non-state) organizations become potential victims of criminal encroachments.

Cybersecurity means first and foremost responding quickly to threats within the Internet. It is noted that in most cases, the objects of cyberattacks are the Internet of Things and the industrial Internet of Things, as, first, a low degree of protection of devices and ports, cloud applications, application programming interfaces; second, there are no security standards.

The experience of counteracting such new challenges and threats as cybercrime, information terrorism and extremism, information fight operations, which not every country is able to cope with, is being studied.

International experience in counteracting such new challenges and threats as cybercrime, cyber-fraud, information terrorism, phishing, vishing and smuggling, targeted phishing, impersonating another person and other methods of cyber-fraud, information control operations, which each is unable to deal with .

The importance of international treaties in this area is noted, including the Commonwealth Model Law on Cybercrime of 2002, the Caribbean Model Law on Cybercrime (HIPCAR project), a joint project of the European Union and the International Telecommunication Union for the Pacific and Pacific States. UN project to develop cybercrime legislation for African countries.

Keywords: cybercrime, computer systems, cyber attacks, technologies, Internet, phishing, vishing, mixing, purposeful phishing, impersonating another person, legal mechanisms, declarations, legal acts.

Постановка проблеми. У сучасному глобалізованому світі разом з інноваційними технологіями виникають і нові види злочинів, що, по суті є закономірним явищем. Використання та удосконалення сфери інформаційних технологій спричинило появу кіберзлочинності – характерного наслідку глобалізації інформаційних процесів. Кіберзлочинність стала загрозою не лише для окремих осіб, а й для держав, оскільки передбачає руйнування економічної та інформаційної сфер. Характерні ознаки кіберзлочинності приваблюють людство, що означає, у свою чергу, збільшення кількості осіб, що чинять протиправну діяльність. Більшість методів соціальної інженерії не вимагають особливих технічних знань з боку зловмисників, а отже використовувати ці методи може будь-хто — від дрібних злодіїв до досвідчених кіберзлочинців.

Існує багато методик, які підпадають під загальний термін соціальної інженерії в галузі кібербезпеки. Серед найвідоміших методик — спам та фішинг, вішинг та смішинг, цілеспрямований фішинг, видавання себе за іншу особу та інші способи кібершахрайства, у яких часто використовують один або навіть декілька методів соціальної інженерії. Ні законодавство ні моральні устої людей не можуть випередити розвиток у даній сфері злочинів, ні попередити їх. Вагомим питанням постає проблема механізмів боротьби з кіберзлочинністю як на національному, так і на міжнародному рівнях.

Аналіз останніх досліджень і публікацій свідчить про те, що питання міжнародного досвіду з протидії протиправним посяганням на електронні інформаційні ресурси були предметом досліджень лише частково. Дана тема знаходить своє відображення в засобах масової інформації (далі – ЗМІ), на конференціях, семінарах, круглих столах та окремих публікаціях. Головним документом, що регулює боротьбу і попередження кіберзлочинності, є конвенція «Про кіберзлочинність», ратифікована у 2005 р. державами Ради Європи та іншими державами.

Окремі дослідники обґрунтовують потребу в прийнятті на рівні ООН універсального міжнародно-правового акта, наприклад, Конвенції протидії кіберзлочинності, задля врегулювання міжнародно-правових питань взаємодії державних органів у процесі протидії кіберзагрозам. Інші стверджують, що достатньо дієвими є механізми, передбачені Конвенцією Ради Європи про кіберзлочинність (далі – Конвенція) від 23 листопада 2001 року, яка спрямована на підвищення ефективності кримінальних розслідувань і переслідувань, що стосуються кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними на надання можливості збирання доказів, що стосуються кримінального злочину, в електронній формі [1].

Сучасні аспекти розвитку та становлення інформаційних відносин, питання здійснення протидії кіберзлочинності та кібершахрайтву розглядались провідними вітчизняними науковцями М. О. Будаковим, В. М. Бутузовим, М. М. Галамбою, Р. А. Калюжним, В. В. Коваленко, Я. Ю. Кондратьєвим, Б. А. Кормичем, Ю. Є. Максименко, А. І. Марущаком, Г. В. Новицьким та іноземними фахівцями А. Робертом, К. Осакве, Т. Блентаном, Д. Банісаром та ін. Однак необхідність подальшого наукового пошуку обґрунтовується

наявністю прогалин у національному законодавстві щодо регламентації адміністративно-правової протидії кіберзлочинності та кібершахрайству в Україні. Однак виявлення і припинення протиправних посягань на електронні інформаційні ресурси неможливе без тісної співпраці між правоохоронними органами різних країн. Відповідна взаємодія ґрунтується на двосторонніх та багатосторонніх міжнародних договорах про взаємну правову допомогу, взаємне визнання іноземних судових рішень.

Метою статті є аналіз міжнародного досвіду з протидії кіберзлочинності та кібершахрайству з метою його використання у діяльності правоохоронних органів України.

Одне з найбільш ґрунтовних діянь, зорієнтованих на регулювання цієї проблеми, є ухвалення Рекомендацією Європи 23 листопада 2001 р. Конвенції про кіберзлочинність (ратифікована 1 липня 2004 р.).

Конвенція про кіберзлочинність представляється первинною міжнародною угодою у сфері протидії правопорушенням, вчиненим посередництвом комп'ютера. В рамках одинадцятого і дванадцятого Конгресів організації щодо запобігання злочинності та кримінального правосуддя (UN Congress on Crime Prevention and Criminal Justice) обговорювалися проблемні проблеми інтернаціонального партнерства у війні з кіберзлочинністю. Члени Конгресів обговорювали заходи щодо інтенсифікації інтернаціонального партнерства і поліпшення державного законодавства у галузі боротьби з відмиванням коштів, торгівлі наркотиками, тероризмом та кіберзлочинністю. Тобто, ООН встановила комп'ютерні правопорушення в єдиний цикл з тероризмом, що вказує на спеціальний інтерес до даного питання зі сторони світової спільноти [3, с. 109, 110].

Серед універсальних міжнародно-правових документів, окрім згаданої Конвенції, вирізняємо Довідник ООН із запобігання і контролю злочинності, пов'язаної з комп'ютерами, 1995 рік; Конвенцію ООН проти транснаціональної організованої злочинності, 2000 рік. Одним із перших міжнародних документів у боротьбі з кіберзлочинністю є «Мінімальний список» правопорушень у цій сфері, прийнятий Європейським комітетом з проблем злочинності Ради Європи у 1990 році, який передбачав наступні злочини: комп'ютерне шахрайство, комп'ютерний підлог, пошкодження комп'ютерної інформації чи програм, комп'ютерний саботаж, несанкціонований доступ до комп'ютерних систем, несанкціоноване перехоплення інформації, несанкціоноване копіювання захищених комп'ютерних програм, незаконне виготовлення топографічних копій. Згодом ця класифікація злочинних посягань була скорегована Конвенцією 2001 року. З метою протидії міжнародній кіберзлочинності, а також для координації діяльності правоохоронних органів країн світу такі злочини класифікуються за кодифікатором міжнародної кримінальної поліції Генерального Секретаріату Інтерполу, який з 1991 року інтегровано в автоматизовану систему пошуку, і сьогодні він доступний підрозділам Національних центральних бюро Інтерполу більшості країн світу, зокрема, й НЦБ Інтерполу МВС України.

У Європейському Союзі нормативно-правовими актами, прийнятими для протидії протиправним посяганням на електронні інформаційні ресурси є Директива ЄС щодо протидії кібератакам на інформаційні системи, 2013 рік; Директива Єврокомісії щодо боротьби з шахрайством та іншими фінансовими злочинами в мережі Інтернет, 2017 рік.

У ЄС значна увага приділяється проблематиці раннього виявлення й оперативного реагування на кіберінциденти та кібератаки проти електронних інформаційних ресурсів. Так, Стратегія кібербезпеки Європейського Союзу [4] у поняття «кіберзахист» додає виявлення і блокування кібератак, локалізацію їх наслідків незалежно від походження стосовно цивільних об'єктів усіх форм власності, а також встановлення і розслідування кіберзлочинів.

Європейська агенція мережевої та інформаційної безпеки (European Network and Information Security Agency, ENISA) забезпечує виконання функції виявлення і блокування кібератак, а також локалізації їх наслідків незалежно від походження стосовно цивільних об'єктів усіх форм власності. CERT-EU (Computer Emergency Response Team) – це структура, яка виявляє кібератаки за допомогою спеціалізованої технологічної системи датчиків, встановлених на абонентських лініях доступу до серверів. У разі здійснення кібератаки спрацьовує датчик, про що оперативно сповіщається CERT-EU. Якщо CERT-EU виявляє кібератаки з ознаками злочинних дій, то відповідна інформація передається до Європейського центру з розслідування кіберзлочинів (European Cybercrime Centre, ECC), який, у свою чергу, може поінформувати про них Європейську агенцію оборони (European Defence Agency) для організації кібероперацій або Європейську службу зовнішніх справ (European External Action Service) [4].

Приклади ефективної кооперації, заснованої на правовій співпраці деяких держав, які за допомогою регіональних угод створюють необхідний рівень гармонізації своїх правових норм і правові механізми взаємодії з урахуванням специфіки кіберзлочинів.

Норми матеріального права гармонізовані за допомогою цілого ряду директив, зокрема, Директива про протидію сексуальній експлуатації дітей онлайн і дитячої порнографії (Directive2011 / 93 / EUof the European

Parliament and of the Council of 13 December 2011 on combating sexual abuse and sexual exploitation of children, and child pornography, replacing the Council Framework – Decision 2004/68 / JHA), Директива про безпеку мереж та інформаційних систем (Directive (EU) 2016/1148 of the European Parliament a nd of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union) [5].

Результативний нагляд несприятливих явищ в кібепросторі, зокрема, таких, як протизаконність, закликає до значно більш активного інтернаціонального партнерства, чим наявні заходи по боротьбі з різними іншими формами міжнародної злочинності. Власне, отже, крім гармонізації кримінально-правових норм, необхідна гармонізація процесуальних важелів і формування нових елементів інтернаціонального партнерства. Важливу значимість у війні з кіберзлочинністю представляють інтернаціональні договори в належній сфері, подібні, так само як Конвенція Ради Європи про кіберзлочинність, рішення Ради Європейського Союзу, Модельний Закон Співдружності Націй про комп'ютерні злочини 2002 р., Модельний Закон країн Карибського Басейну про кіберзлочинність (проект HIPCAR), спільний проект Європейського союзу і Міжнародного Союзу Електрозв'язку для держав Тихоокеанського регіону (проект ICB4PAC), проект ООН з розробки законодавства в галузі кіберзлочинності для країн Африки (проект ESCWA) та ін. [6].

Розуміння важливості розробки і прийняття міжнародно-правових актів, спрямованих на боротьбу із комп'ютерними злочинами, було сприйнято низкою міжнародних організацій починаючи з дев'яностих років XX сторіччя. ООН, враховуючи роль і значення інформації, розвиток інформаційно-комунікаційних технологій, створення світових баз даних, глобальних інформаційних мереж і систем та їх захисту, взяла на себе координуючу роль у розробці як концептуальних, так і правових засад регулювання ключових питань, серед яких: боротьба із злочинним використанням інформаційних технологій, положення викладені в Резолюціях ГА ООН 2011-2016 рр. Крім того, Економічна і Соціальна Рада ООН прийняла кілька резолюцій щодо особистих даних особи (Резолюції ЕКОСОР «Міжнародне співробітництво у справі щодо попередження і розслідування шахрайства, злочинного неправомірного використання і фальсифікації особистих даних і пов'язаних з ними злочинів, а також переслідування та покарання за них» № 2004/26 від 21 липня 2004 року, № 2007/20 від 26 липня 2007 року) [7, с. 2].

Резолюцією Генеральної Асамблеї A/RES/58/199 наголошено на потреби охорони інформативних інфраструктур, запропонований цикл компонентів з метою охорони найбільш значних з них, зокрема: присутність мереж з метою негайного відвернення про умови уразливості, небезпеки і конфлікті в кібернетичному сфері; збільшення рівня поінформованості причетних сторін для того, щоб вони повніше усвідомлювали вид і масштаби своїх основних інформативних інфраструктур і ту значимість, яку будь-яка з них повинна виконувати в охороні даних інфраструктур; присутність відповідних речових і процесуальних законів і відомого персоналу з тією метою, щоб країни мали можливість з'ясовувати намагання порушення охорони головних інформативних будівель і залучити до відповідальності причетних осіб; формування та надання функціонування концепцій комунікації і переломні умови та контроль їх функціонування з метою забезпечення їх нормальної діяльності в критичних моментах; спільна робота держав з мішенню спостереження зусиль злому головних інформативних будівель і т.д. [8, с. 5].

Передбачаючи ціль формування слушних умов для прогресу інформаційно-комунікаційних технологій, в рамках програми Нове партнерство на користь розвитку Африки (НЕПАД) ООН співробітничає з Комісією Африканського союзу в розробці конвенції по кібербезпеку в Африці за зразком Конвенції про кіберзлочинність. У всьому світі розбіжності у сфері обхвату положень відносно співпраці, що містяться в багатосторонніх або двосторонніх документах, відсутність зобов'язання представляти відповідь протягом певного терміну, відсутність домовленості про допустимий прямий доступ до екстериторіальних даних, великою кількістю неофіційних мереж правоохоронних органів і відмінності в гарантіях співпраці є серйозні проблеми у справі забезпечення ефективної міжнародного співробітництва в галузі електронних доказів по кримінальних справах [9, с. 5].

У рамках дослідження питання міжнародно-правового регулювання інформаційного тероризму варто згадати проект «Загального договору з питань кібербезпеки та кіберзлочинності», запропонований професором Штайном Шольбергом, який займав посаду голови групи експертів високого рівня з питань кібербезпеки, засновану у 2007 р. задля вивчення можливостей створення загального документа з питань кіберзлочинності в рамках Організації Об'єднаних Націй, та професором Соланж Гернуті-Елі. Автори цього проекту розглядають інформаційний тероризм як один із видів кібератак. Відповідно до положень проекту договору до таких дій належать: публічне підбурювання до вчинення терористичного злочину, пошук та схилення людей для вчинення терористичного акту та проведення терористичних навчань. Також договором передбачено кримінальну відповідальність за такі дії згідно з внутрішнім законодавством держав-членів [10, с. 315].

У рамках ЮНЕСКО була розроблена концепція «Універсальності Інтернету», що відображає позицію організації в межах її мандату щодо питань, пов'язаних з Інтернетом, на період до 2021 року. Вона також

засвідчує роль Інтернету у розбудові суспільств знань та досягнення цілей сталого розвитку ООН. В основу даної концепції покладено чотири ключові принципи, що наразі відомі як принципи R.O.A.M. – орієнтованість на права людини, відкритість, доступність та багатостороння участь [11, с. 82].

Розроблена концепція Конвенції ООН про забезпечення міжнародної інформаційної безпеки. Важливо, що в ст. 4 Конвенції закріплені основні загрози міжнародному миру і безпеки в інформаційному просторі, з яких виділено 11 базових і 4 додаткових. Серед базових названі, наприклад, використання інформаційних технологій і засобів для здійснення ворожих дій і актів агресії; цілеспрямоване деструктивне вплив в інформаційному просторі на критично важливі структури іншої держави; транскордонне поширення інформації, що суперечить принципам і нормам міжнародного права, а також національним законодавствам держав [12, с. 372-373].

Оптимізації процесів надання взаємної правової допомоги, що стосуються електронних доказів, можуть сприяти такі нововведення, як включення модуля по електронним доказам в перероблену Програму складання прохань про надання взаємної правової допомоги Управління Організації Об'єднаних Націй з наркотиків і злочинності (УНП ООН). Разом з тим одночасно з цим правоохоронні органи можуть відчувати зростаючу потребу в знаходженні новаторських методів співпраці в області проведення транснаціональних розслідувань кіберзлочинів [13, с. 109]. Особливо важливим в цьому відношенні може виявитися участь в координації підтримки транснаціональних розслідувань таких структур, як Глобальний інноваційний комплекс Інтерполу і Європейський центр по боротьбі з кіберзлочинністю (ЕЦК) Європейського поліцейського управління (Європол). Інші форми і ініціативи, наприклад Глобальна конференція з кіберпростору, також надають країнам можливість розглядати інноваційні заходи реагування в області міжнародного співпраці в боротьбі з кіберзлочинністю [14, с. 15-16].

Всесвітня організація інтелектуальної власності, у свою чергу, слідкує за дотриманням так званих Інтернет-договорів 1996 року – Договору про авторське право та Договору про виконання та фонограми. Так, обидва договори передбачають обов'язок держав-членів надавати належний рівень правової охорони та ефективні засоби правового захисту, які б унеможливлювали обхід технологічних обмежень, використаних для захисту об'єкту інтелектуальної власності. ВОІВ робила невдалі спроби зафіксувати на нормативному рівні положення щодо веб-мовлення та трансляції в Інтернеті, а також розширення прав телерадіокомпаній у кіберпросторі [15, с. 82-83].

Також необхідно зауважити, що Генеральна Асамблея являється важливим консультативним органом ООН, в зону відповідальності якої входить розгляд важливих аспектів, що стосуються кола інтересів країн-членів та інших країн, зокрема, тих, що стосуються опору кіберзлочинності. Під її егідою встановлений цикл дій, що включають твердження про: врегулювання інформаційного простору; охорону інформативних інфраструктур; надання захищеності користувачів мережу інтернет-послуг; виконання культури кібербезпеки; партнерство країн у протидії кіберзлочинності, в тому числі заміна даними, висококласні збори працівників правоохоронної області, надання конфіденційності, єдності і доступності відомостей комп'ютерних систем від несанкціонованого втручання і так далі. Вона є організатором формування спеціальних експертних компаній з метою дослідження проблематики в галузі протидії кіберзлочинності; погоджує роботу спеціальних органів ООН, зайнятих завданнями протидії кіберзлочинності (Управління ООН з наркотиків і злочинності, Організація Об'єднаних Націй з питань освіти, науки і культури, Конференція ООН з торгівлі і розвитку, Міжнародний союз електрозв'язку тощо) [16]. Водночас, доволі ефективна практика Китаю із побудови «національного інтернету» із практично повним функціоналом «великого інтернету» може спровокувати аналогічні спроби і в інших країнах чи міждержавних об'єднаннях. Не виключено, що ця проблема може зачепити і Україну, якій у відділеному майбутньому доведеться обирати власну позицію щодо такої глобальної сепарації [17].

ЮНОДК як організація, що визначає стандарти в галузі попередження злочинності та кримінального правосуддя, слугуватиме майданчиком для багатосторонніх контактів, центральне місце в яких має належати країнам, що розвиваються. ЮНОДК буде прагнути налагоджувати партнерські зв'язки, мобілізуючи наявний інструментарій та фахівців, в тому числі з боку приватного сектора (і особливо провайдерів інтернет-послуг), з метою вирішення проблеми в тій чи іншій країні або регіоні. Першочергова увага буде приділятися надання технічної допомоги нужденним в ній державам-членам, з тим щоб подолати дефіцит можливостей і експертної підготовки і надати боротьбі з комп'ютерною злочинністю стабільний і довгостроковий характер [18, с. 18].

Міжнародний союз електрозв'язку (МСЕ) як спеціалізована установа в системі Організації Об'єднаних Націй відіграє провідну роль в області стандартизації і розвитку електрозв'язку, а також в питаннях кібербезпеки. Серед іншої діяльності МСЕ є провідною організацією Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства (ВСІС) [19, с. 121].

В Україні враховується міжнародний досвід щодо розбудови мережі ситуаційних центрів кіберзахисту на об'єктах критичної інформаційної інфраструктури та системи ситуаційних центрів кібербезпеки.

Також необхідними змінами законодавства задля протидії протиправним посяганням на електронні інформаційні ресурси має бути закріплення механізму оперативного обмеження (блокування) певного інформаційного ресурсу (інформаційного сервісу) та впровадження особливих умов проведення обшуку і арешту електронних доказів, насамперед закріплення процесуально значимої можливості копіювання інформації, а також імплементація в національне законодавство положень про невідкладне фіксування і подальше зберігання даних операторами, провайдерами телекомунікацій, власниками ресурсу (веб-сайту) із забезпеченням їх цілісності. Отже, ООН та її спеціалізовані установи і організації, мета діяльності яких передбачає забезпечення мирного існування та перевагу дипломатії над воєнним характером відносин, відіграє велику роль у боротьбі із кіберзлочинністю та кібершахрайством. Прийняття низки правових актів спрямовані на підтримку інформаційної безпеки та боротьби і попередження кіберзлочинності.

Список використаних джерел:

1. Конвенція про кіберзлочинність від 23.11.2001 / Верховна Рада України. URL: http://zakon0.rada.gov.ua (дата звернення 30.04.2021р.)

2. Войціховський А. В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. Право і Безпека. 2011. № 4. С. 107-112

3. Шматкова Л. П. Международное сотрудничество в борьбе с киберпреступлениями: состояние и перспективы. Молодой ученый. 2016. № 28. С. 720-723

4. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace / European Comission. High representative of the European Union for foreign affairs and security policy. Brussels, 7.2.2013. Join (2013) URL: http:// www.enisa.europa.eu. (дата звернення 30.04.2021 р.)

5. Кіберзлочинність: проблеми боротьби і прогнози. Антикібер Національне антикорупційне бюро. URL: http:// anticyber.com.ua (дата звернення 30.04.2021р.)

6. Оказание помощи странам в борьбе с киберпреступностью / Управление ООН по наркотикам и преступности. URL: https://www.unodc.org (дата звернення 30.04.2021р.)

7. Забара І. М. Міжнародно-правове регулювання співробітництва держав у боротьбі з інформаційною злочинністю. Часопис Академії адвокатури України. 2012. № 17. С. 1-6

8. Сироїд Т. Л. Діяльність Генеральної Асамблеї ООН у протидії кіберзлочинності. URL: http:// legalactivity.com.ua (дата звернення 30.04.2021р.)

9. Орлов О. В., Онищенко Ю. М. Міжнародна співпраця у сфері боротьби з кіберзлочинністю. Теорія та практика державного управління. 2013. Вип. 4 (43). С. 1-6

10. Грицун О. О. Питання міжнародно-правового регулювання інформаційного тероризму. Часопис Київського університету права. 2014. № 4. С. 312-317

11. Кирилюк О. В. Інституційний механізм міжнародно-правового регулювання глобального інформаційного суспільства. Актуальні проблеми міжнародних відносин. 2015. Випуск 126 (частина ІІ). С. 77-90

12. Якимова Е. М., Нарутто С. В. Международное сотрудничество в борьбе с киберпреступностью. Криминологический журнал Байкальского государственного университета экономики и права. 2016. Т. 10, № 2. С. 369-378

13. Марков В. В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. Право і Безпека. 2015. № 2. С. 107-113

14. Тринадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию: справочный документ. Доха, 12-19 апреля 2015 года. 114 с. https://www.unodc.org (дата звернення 30.04.2021р.)

15.Кирилюк О. В. Інституційний механізм міжнародно-правового регулювання глобального інформаційного суспільства. Актуальні проблеми міжнародних відносин. 2015. Випуск 126 (частина ІІ). С. 77-90

16. Сироїд Т. Л. Діяльність Генеральної Асамблеї ООН у протидії кіберзлочинності. Актуальна юриспруденція. зб. матеріалів інтернет-конференції. Київ. 2018. С.77-80

17. Спроби впровадження міжнародного контролю за діяльністю в Інтернеті під егідою ООН: нові можливості реалізації Україною інформаційного суверенітету: аналітична записка / Національний інститут стратегічних досліджень. URL: http://www.niss.gov.ua/articles/1093/ (дата звернення 30.04.2021р.)

18. Двенадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. Сальвадор, Бразилия. URL: https://www.un.org/ru/conf/crimecongress2010/ (дата звернення 30.04.2021р.)

19. Герке Марко. Понимание киберпреступности: явление, задачи и законодательный ответ. пособие. Женева, 2012. 357 с. URL: https://www.twirpx.com/file/2283591/(дата звернення 30.04.2021р.)