УДК 343.2/.7

Орлеан Андрій Михайлович –
доктор юридичних наук, доцент,
провідний науковий співробітник
юридичного факультету Київського
національного університету імені Тараса Шевченка

Andrii M. Orlean –
doctor of juridical sciences, associate professor,
leading research fellow of the Law Faculty,
Taras Shevchenko National University of Kyiv
(60 Volodymyrska Street, Kyiv, Ukraine)

Адаптація законодавства України у сфері протидії кіберзлочинності до законодавства Європейського Союзу

У статті наведено авторський погляд на проблематику кіберзлочинності. Зокрема її визначення, етапи розвитку та загрози, що несе остання; відзначено її транснаціональний характер та вказано на основоположні міжнародні документи, які регламентують питання боротьби з кіберзлочинами. Розглянуто питання адаптації законодавства України до законодавства Європейського Союзу з урахуванням міжнародного досвіду боротьби з кіберзлочинністю. Вказано на необхідність чіткого нормативного регулювання в Україні правового положення криптовалют та процесу майнінгу (добування криптовалют), а також встановлення кримінальної відповідальності за незаконне заволодіння криптовалютами та визнання їх предметом неправомірної вигоди.

Ключові слова: *законодавство Європейського Союзу, адаптація законодавства, кіберзлочинність, боротьба з кіберзлочинністю, удосконалення законодавства.*

В статье отображен авторский взгляд на проблематику киберпреступности. В частности, приведено ее определение, этапы развития; угрозы, которые она представляет; подчеркнут ее транснациональный характер, а также указаны основоположные международные документы, регламентирующие вопросы борьбы с киберпреступлениями. Рассмотрены вопросы адаптации законодательства Украины к законодательству Европейского Союза с учетом международного опыта борьбы с киберпреступностью. Подчеркнута необходимость четкого правового регулирования в Украине правового положения криптовалют и процесса майнинга (добычи криптовалют), а также установления уголовной ответственности незаконное завладение криптовалютами; признание их предметом неправомерной выгоды.

Ключевые слова: *законодательство Европейского Союза, адаптация законодательства, киберпреступность, борьба с киберпреступностью, усовершенствование законодательства.*

A.M. Orlean Approximation of Ukrainian Legislation on Counteraction to Cyber Crime to Legislation of the European Union

Progress in science and technology in the sphere of informational technologies has brought new types of crimes such as cybercrimes which include unauthorized intrusion in the work of computers, computer systems and telecommunications. Cybercrime refers to one of the most dynamic types of socially dangerous acts. In spite of significant spread of these crimes Ukrainian legislation on counteraction to cybercrimes cannot be considered to comply with realities and European standards.

Dynamic development of cybercrimes requires new research and scientific developments in this sphere to introduce proposals on amendments to effective legislation and draft new legislation for its effective implementation. Besides, Ukraine has not defined a legal status of crypto currency and the process of its receiving (mining) yet. It means that the state does not protect the rights of persons who use crypto currency from illegal activities of those ones who want to possess it. Moreover, miners and owners of crypto currency are beyond the

law in fact. Furthermore, there is no regulation of possibility to bring to liability for theft or other illegal possession of crypto currency as well as for obtaining crypto currency as an illegal profit.

The article provides a definition, stages of development and threats of cybercrimes; its transnational features have been mentioned and basic international documents which regulate fight against cybercrimes have been presented. The issue of approximation of Ukrainian legislation to the legislation of the European Union taking into account international practice of combat cybercrimes has been addressed. Necessity of clear legal regulation of legal status of crypto currency in Ukraine, mining process (obtaining of crypto currency) and establishment of criminal liability for illegal possession of crypto currencies and their recognition as a subject to illegal profit have been highlighted.

Keywords: *legislation of the European Union, approximation of legislation, cybercrimes, fight against cybercrimes, improvement of legislation.*

Постановка проблеми. В сучасному суспільстві управління процесами за допомогою комп'ютерних технологій превалює в широкій палітрі нашого життя. Так, зберігання, доступ і передача інформації у багатьох сферах (проектування, комп'ютерне моделювання, виробництво у різних галузях, обробка інформації та ведення баз даних, технологія блокчейн, розробка та запровадження криптовалют й багато іншого здійснюється у електронній формі.

Науково-технічний прогрес у сфері інформаційних технологій призвів до появи цілої низки злочинів, пов'язаних із несанкціонованим втручанням в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку, тощо. Ці злочини почали називати кіберзлочинністю.

Наразі такі терміни, як «кіберзлочинність», «хакер», «несанкціоноване втручання в базу даних» «комп'ютерний злом», «крадіжка бази даних», «блокчейн», «криптовалюти» «розповсюдження комп'ютерних вірусів», «шахрайство з пластиковими платіжними картками», «крадіжки коштів з банківських рахунків», «боти», «DDoS-атака»[1] та інші перестали бути чимось незвичним як для правоохоронців так і для пересічних громадян у нашій державі.

Кіберзлочинність обґрунтовано відноситься до однієї з найдинамічніших сучасних загроз. Тому добре, що в Україні ще 15 жовтня 2015 року було створено кіберполіцію з метою запобігання та протидії кіберзлочинам, а проблеми протидії злочинам у сфері використання комп'ютерної техніки та мережі Інтернет набули широкого наукового дослідження та обговорення.

Незважаючи на значне поширення таких злочинів, вітчизняне законодавство у сфері протидії кіберзлочинності не можна вважати таким, що повною мірою відповідає викликам сьогодення та європейським стандартам. Адже питання, пов'язані із протидією кіберзлочинності за допомогою кримінально-правових заходів та адаптацією законодавства України до законодавства Європейського Союзу є актуальними на даний час та потребують ретельного наукового дослідження.

Аналіз останніх досліджень і публікацій. Питанням, пов'язаним із кіберзлочинністю увагу в наукових працях приділяли увагу Д.С. Азаров, О.Ю. Амелін, П.Д. Біленчук, А.В. Войцехівський, В.Б. Вєхова, В.О. Голубєв, М.Д. Діхтяренко, С.П. Лапта, А.А. Музика, Є.Д. Скулиш та інші.

Невирішені раніше проблеми. Незважаючи на наявність великої кількості досліджень у цій сфері, динамічний характер розвитку кіберзлочинності вимагає все нових та нових наукових розробок й напрацювань, що мають допомогти зробити вітчизняне законодавство більш ефективним. Зокрема, лавиноподібне поширення в світі та в нашій країні криптовалют, ставить перед нашою країною цілу низку викликів, пов'язаних із необхідністю створення відповідного правового поля для їх безпечного обігу та майнингу.

Мета. Мета статті полягає у дослідженні нових тенденцій кіберзлочинності та з'ясуванні

[1] Атака на комп'ютерну систему з метою довести її до відмови, тобто створити таки умови, при яких легітимні користувачі системи не можуть отримати доступ до надаваних системою ресурсів (серверів або сервісів), або цей доступ ускладнений. Відмова "ворожої" системи може бути як самоціллю (наприклад, зробити недоступним популярний сайт), так і одним із кроків до оволодіння системою) [1]

перспективних напрямів удосконалення національного законодавства та його адаптації до законодавства Європейського Союзу з урахуванням міжнародного досвіду боротьби з кіберзлочинністю

Виклад основного матеріалу. Одночасно із появою та розвитком всесвітньої мережі Інтернет ми отримали неконтрольоване зростання побічних проблем, що згодом почали розглядатись як кіберзлочинність. Сучасні інформаційно-комунікаційні технології продовжують запроваджуватись і розвиватись набагато швидше, ніж можливості законодавчих та правоохоронних органів щодо адекватного реагування на їх збільшення [2].

Як відзначають В.Б. Дзюндзюк та Б.В. Дзюндзюк, у 1970-х роках з'явилися перші комп'ютерні злочинці, яких почали називати «хакерами». Важко точно сказати, хто саме був першим хакером, але в більшості літературних джерел для хакерів і про хакерів як перший професійний кіберзлочинець згадується Джон Дрейпер (John Draper), який також породив першу спеціалізацію хакерів – фрікери (phreaker) скорочене від телефонний хакер phone hacker. В рядах фрікерів у той час були навіть такі знамениті особи як Стів Возняк та Стів Джобс, які в майбутньому заснували «Apple Computers». Вони налагодили виробництво пристроїв для злому телефонних мереж в домашніх умовах [2].

Всього через два десятки років світові засоби масової інформації вперше повідомили про грандіозний міжнародний фінансовий злочин з використанням мережі Інтернет – справу Володимира Льовіна, який проник до електронної системи управляння коштами ньюйоркського «Сітібанку», звідки упродовж 30 червня – 3 жовтня 1994 року несанкціоновано перевів близько 12 млн. USD, які належали корпоративним клієнтам [4].

В літературі називають 4 основні етапи в розвитку цього напряму злочинної діяльності: 1) поява кіберзлочинності і субкультури хакерів; 2) розповсюдження кіберзлочинності, поява спеціалізацій кіберзлочинців і національних груп хакерів; 3) набуття кіберзлочинністю транснаціонального характеру, поява кібертероризму і міжнародних груп хакерів у всіх сферах кіберзлочинності; 4) використання Інтернету в політичних цілях, виникнення таких явищ як інтернет-страйк і інтернет-війна, цілеспрямоване використання кібератак проти урядів окремих держав [2].

Кіберзлочинність традиційно пов'язують із використанням мережі Інтернет для спричинення певної шкоди.

В літературі обґрунтовується думка про те, що сфера вчинення інтернет-злочинів – так званий віртуальний простір, який можна визначити як модельований за допомогою комп'ютера інформаційний простір, де містяться дані про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому вигляді і що перебувають у процесі руху по локальних і глобальних комп'ютерних мережах, або ж відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки і передачі [6].

Враховуючи викладене, існує думка про те, що комп'ютерні злочини слід розглядати суто як злочини у сфері використання комп'ютерних та інформаційних мереж, наслідком яких є протиправне заволодіння даними [7]. Їх також визначають як суспільно небезпечні, протиправні, кримінально карані, винні діяння, які завдають шкоди інформаційним відносинам, засобом забезпечення нормального функціонування яких є ЕОМ, автоматизовані системи, комп'ютерні мережі або мережі електрозв'язку [8].

Проте на наш погляд, кіберзлочинність необхідно розглядати дещо ширше, як це, наприклад, робить Н.В. Савчук, котрий визначає кіберзлочинність як поняття, яке охоплює і комп'ютерну злочинність (де комп'ютер – предмет злочину, а інформаційна безпека – об'єкт злочину) й інші посягання, де комп'ютер є знаряддям а його використання способом вчинення злочинів проти власності, авторських прав, громадської безпеки, моралі тощо [5].

Кіберзлочинність – явище сучасної цифрової доби, доби високих інформаційних технологій. Саме це й робить кіберзлочинців більш небезпечними за звичайних шахраїв. Це люди, які «працюють» за допомогою комп'ютера, ноутбука чи смартфона, і можуть завдати шкоду з будь-якої точки земної кулі. При цьому об'єкти посягань можуть знаходитись за десятки тисяч кілометрів. У багатьох випадках виявити, зафіксувати та вилучити необхідну

інформацію для документування злочинної діяльності в рамках чинного законодавства за допомогою традиційних слідчих (розшукових) дій надзвичайно складно, а подекуди й неможливо. Адже розкриття таких злочинів неможливе без застосування комп'ютерних технологій.

Більше того, кіберзлочинність є транснаціональною, об'єкти її посягання знаходяться в кіберпросторі, який необмежений державними кордонами, і для їх виявлення та розслідування необхідним є залучення правоохоронних органів різних країн, (наприклад, у зв'язку з необхідністю фізичного доступу до комп'ютера злочинця) якщо місцем вчинення злочину є одна країна, а суспільно-небезпечні наслідки настають на території інших.

У зв'язку з цим виникає гостра потреба у розробці та оновленні законодавчих норм, з метою запобігання та протидії кіберзлочинності.

Основоположним документом, який регламентує боротьбу з кіберзлочинами є Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 року, відома ще як «Будапештська Конвенція» ратифікована Законом України № 2824 від 07.09.2005 із застереженнями і заявами [9].

У ній визначено найбільш загальні та разом із тим визначальні принципи щодо забезпечення заходів боротьби із кіберзлочинами на національному та міжнародному рівнях. Конвенція виділяє наступні групи правопорушень у цій сфері:

- злочини у сфері незаконного доступу до інформації: нелегальне перехоплення (ст. 3), втручання у дані (ст. 4), втручання у систему (ст. 5), зловживання пристроями (ст. 6);
- злочини, пов'язані з протиправним використанням комп'ютерів: підробка, пов'язана з комп'ютерами (ст. 7), шахрайство, пов'язане з комп'ютерами (ст. 8);
- злочини, пов'язані зі змістом, до яких відноситься створення, розповсюдження та зберігання дитячої порнографії (ст. 9);
- злочини, пов'язані з порушенням авторських та суміжних прав (ст. 10).

Ст. 8 передбачає, що кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом: a) будь-якого введення, зміни, знищення чи приховування комп'ютерних даних, b) будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи.

Наведені вище положення поряд з іншим свідчать про необхідність віднесення до кримінально караних певного спектру незаконних дій із таким доволі новим фінансовим інструментом як криптовалюти. Йдеться про дії, які можуть призвести до втрати майна іншої особи внаслідок атаки на криптовалютні біржі, крадіжки криптовалют із електронних гаманців власників, тощо.

Криптовалюта – від англійського «cryptocurrency», тобто віртуальна валюта, захищена криптографією. Насамперед, криптовалюта – це швидка і надійна система платежів та грошових переказів – транзакцій, заснована на новітніх технологіях й непідконтрольна жодному уряду. На даний момент в світі існує понад 1600 криптовалют (найвідоміші з яких - Bitcoin, Litecoin, Ethereum, Peercoin). Найбільш відомий серед них в Україні Bitcoin не випускається центральними банками і не залежать від кредитно-грошової політики тієї чи іншої держави. Емісія відбувається тільки в цифровому вигляді. Будь-хто охочий може добувати криптовалюту (займатися майнінгом) за допомогою спеціалізованого обладнання. Bitcoin визнаний фінансовим інструментом у Німеччині. У США Bitcoin є одним із засобів платежів у електронній комерції. В столиці Австрії Відні функціонує перший у в світі Bitcoin банк. У ньому встановлено спеціальні банкомати, які дозволяють обмінювати Bitcoin на євро і навпаки.

Одночасно із розповсюдженням криптовалют, набувають значного поширення і випадки зламу криптовалюних бірж та крадіжки криптовалют з рахунків трейдерів (торговців).

В Україні законодавство не визначає поняття та правовий статус криптовалют, а також майнінгу (процесу їх добування). Це означає, що держава не захищає права осіб, котрі використовують криптовалюту від протиправних дій інших осіб, спрямованих на заволодіння нею.

Майнери та власники криптовалют фактично знаходяться поза законом. Очевидно, що в суспільстві назріває потреба у визначенні на законодавчому рівні правового статусу криптовалют та їх майнінгу, і відповідно встановлення кримінально-правової заборони на протиправне заволодіння криптовалютами.

Крім того, все частіше і частіше ми зустрічаємось із повідомленнями засобів масової інформації про намагання посадових осіб, уповноважених на виконання функцій держави отримувати неправомірну вигоду у криптовалютах [10].

Також збільшується й кількість загальнокримінальних злочинів, спрямованих на заволодіння криптовалютою. Наприклад, нещодавно мало місце повідомлення про викрадення осіб та тримання їх в заручниках з метою отримання викупу в Біткоїнах у сумі, еквівалентній 5 млн. доларів США [11].

Проте зважаючи на невизначеність правового статусу криптовалюти Україні, виникає питання наявності складу відповідних злочинів, оскільки криптовалюта не є ані засобом платежу ані електронними грошовими коштами, ані чимось іншим. Відсутні методики та порядок обчислення, визначення розміру шкоди у грошовому еквіваленті криптовалюти до грошової одиниці гривні згідно з курсом Національного Банку України.

Світовий досвід показує ймовірність спричинення величезної фінансової шкоди через незаконне заволодіння криптовалютою. Так, одна з найбільших у Японії бірж цифрових валют Coincheck повідомила про втрату 28.01.2018 року криптовалюти вартістю приблизно у $534 млн через хакерську атаку на свою мережу. У 2014 році інша біржа з Токіо MtGox рухнула, коли визнала, що з мережі викрали $400 мільйонів [12].

У Особливій частині КК України міститься Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Проте закріплені тут кримінально-правові заборони не призначені для притягнення до відповідальності за незаконне заволодіння криптовалютами, навіть якщо його вчинено з використанням комп'ютерів та мережі Інтернет. Для цього мають використовуватись норми з класичного Розділу VI «Злочини проти власності». Як справедливо відзначають А.А. Музика та Д.С. Азаров, застосування комп'ютерів для вчинення названих діянь є лише певним способом вчинення злочину, який зазвичай не включається до обов'язкових ознак об'єктивної сторони складу злочину. За наявності певних фактичних обставин ці злочини можуть кваліфікуватись за сукупністю зі злочинами передбаченими Розділом XVI Особливої частини КК України [13].

Проте у випадку із незаконним заволодінням криптовалютами необхідно враховувати, що для надання правової оцінки їх викраденню необхідним є визначення їх правового становища, і вже потім вирішення питання щодо кваліфікації як злочину проти власності, службового чи іншого злочину, поєднаних із комп'ютерним злочином.

Першочергова необхідність вирішення проблем протидії кіберзлочинності та співробітництва у цій сфері обумовлюється й обов'язками України щодо виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. Зокрема, пунктом f) ч. 1 ст. 22 цього документу розглядуваний напрям віднесено до кола найважливіших в рамках боротьби з кримінальною та незаконною організованою чи іншою діяльністю [14].

У зв'язку з необхідністю боротьби з кіберзлочинністю на загальноєвропейському рівні, під егідою Європейського поліцейського відомства (Європолу) в Гаазі (Нідерланди), з початку 2013 року розпочав діяльність Європейський центр боротьби із кіберзлочинністю (European Cyber Crime Centre (EC3)). Серед пріоритетів Центру – розслідування шахрайства через онлайн-мережі, зокрема у системі електронного банкінгу та інших видів фінансової діяльності, протидія сексуальній експлуатації дітей через Інтернет, а також розслідування інших злочинів, що посягають на безпеку важливої інфраструктури та інформаційних систем ЄС [15].

До перших масштабних здобутків центру можна віднести викриття одної з найбільших шахрайських комп'ютерних мереж та арешт 11 членів злочинної організації. Дана мережа

приносила своїм засновникам близько мільйона євро щорічно. Вони використовували комп'ютери, що знаходилися у 33 країнах світу, у тому числі в 22 країнах Європи. Гроші «відмивалися» злочинцями з використанням інформаційних систем – різноманітних ігрових порталів, електронних платежів, шлюзів та віртуальних грошей [16].

Поряд з іншим, на європейському рівні питання, пов'язані з кібербезпекою регулюються прийнятою Європарламентом Директивою ЄС 2016/1148 від 6 липня 2016 року (NIS Directive) про заходи для забезпечення високого рівня безпеки мережевих та інформаційних систем [17].

Зазначеною Директивою передбачено вимоги безпеки в таких критично важливих сферах як банківська, енергетики, транспорту, охорони здоров'я, інфраструктури, фінансового ринку та цифрової інфраструктури, а також вимоги безпеки у сферах онлайн-послуг (торгових майданчиків, пошукових систем, хмарних технологій та ін.)

Характерною особливістю кіберзлочинів є те, що суб'єктами їх вчинення можуть бути особи різних вікових категорій – як повнолітні так і неповнолітні. Наприклад, у 1998 році 12-річний хакер проник у комп'ютерну систему, що контролює паводкові шлюзи греблі Т. Рузвельта в Арізоні й поставив під загрозу затоплення два міста з населенням 1 млн. чоловік [18].

Тому актуальними у цьому контексті видаються доводи науковців, котрі піднімають проблеми розширення сфери дії кримінального законодавства спрямованого на протидію кормпютерним злочинам [19].

Висновки. Підсумовуючи викладене, слід відзначити, що для успішної протидії кіберзлочинності, яка надзвичайно динамічно прогресує, держава має не лише створювати, готувати й забезпечувати відповідним технічним оснащенням спеціальні поліцейські підрозділи, а й своєчасно надавати їм нові сучасні правові інструменти для притягнення винних до кримінальної відповідальності.

Подальшої ґрунтовної уваги та вирішення потребує проблема створення відповідного правового поля для майнингу, використання та обігу криптовалют в Україні. Відповідно має бути створеною правова база, що забезпечуватиме притягнення до кримінальної відповідальності за викрадення чи інше незаконне привласнення криптовалют. Використання останньої в якості неправомірної вигоди також має охоплюватись відповідними кримінально-правовими заборонами.

Вказані питання потребують ґрунтовних наукових досліджень, для чого на державному рівні мають бути задіяні групи науковців, які спільно з ІТ фахівцями повинні систематично працювати над оновленням законодавства, спрямованого на боротьбу з кіберзлочинністю. При цьому має бути врахований міжнародний досвід боротьби з кіберзлочинністю та забезпечена відповідність вітчизняного законодавства законодавству ЄС.

Список використаних джерел:

1. Kavun S. V. Enterprise Insider Detection as an Integer Programming Problem. Intelligent Decision Technologies / S. V. Kavun, I. V. Sorbat, V. V. Kalashnikov // Smart Innovation, Systems and Technologies. – 2012. – No. 16 (2). – Pp. 281–289.

2. Лісайчук А. А. Проблеми боротьби із кіберзлочинністю на міжнародному рівні [Електронний ресурс]. – Режим доступу : https://internationalconference2014.wordpress.com/2014/ 10/09.

3. Дзюндзюк В. Б. Поява і розвиток кіберзлочинності / В. Б. Дзюндзюк, Б. В. Дзюндзюк // Державне будівництво. – 2013. – № 1 [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/UJRN/DeBu_2013_1_3.

4. «Дело Левина»: как все было: Компьютерная газета [Електронний ресурс]. – Режим доступу : http://www.nestor.minsk.by/kg/2003/36/kg33614.html.

5. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби [Електронний ресурс] / Н. В. Савчук // Теоретичні та прикладні питання економіки. – Вип. 19. – 2009. – С. 338–342. – С. 338 – Режим доступу : http://archive.nbuv.gov.ua/portal/Soc_Gum/Tppe/2009_19/Zb19_48.pdf.

6. Кіпа О. О. Правопорушення в мережі Інтернет / О. О. Кіпа // Часопис Київського університету права. – 2010. – № 4. – С. 346–349.

7. Біленчук Д. П. Кібрешахраї – хто вони? / Д. П. Біленчук // Міліція України. – 1999. – № 7-8. – С. 32-34.

8. Амелін О. Визначення кіберзлочинів у національному законодавстві / О. Амелін // Науковий часопис Національної академії прокуратури України. – 2016. – № 3. – С. 1–10 [Електронний ресурс]. – Режим доступу : http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/11-2016/amelin.pdf.

9. Конвенція про кіберзлочинність : Закон України від 7 вересня 2005 поку № 2824-IB [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/994_575.

10. На Полтавщині затримали прокурора при отриманні хабара в три біткойни [Електронний ресурс]. – Режим доступу : http://uareview.com/bitcoin-habar.

11. У Києві двох заручників кілька місяців тримали в полоні заради викупу в $5 млн у біткоїнах [Електронний ресурс]. – Режим доступу : https://espreso.tv/news/2018/01/26/u_kyyevi_dvokh_zaruchnykiv_kilka_misyaciv_trymaly_v_poloni_zarady_vykupu_v_5_mln_u_bitkoyinakh.

12. У Японії відбулася найбільша в історії крадіжка цифрової валюти [Електронний ресурс]. – Режим доступу : http://www.bbc.com/ukrainian/news-42847803.

13. Музика А. А. Законодавство України про кримінальну відповідальність за комп'ютерні злочини: науково-практичний коментар і шляхи вдосконалення / А. А. Музика, Д. С. Азаров. — К. : Вид-во Паливода А. В., 2005.

14. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : ратифікована Законом України № 1678-BII від 16 вересня 2014 року [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/984_011.

15. Євросоюз відкрив центр по боротьбі з кіберзлочинністю. Дзеркало тижня. Україна [Електронний ресурс]. – Режим доступу : http://dt.ua/TECHNOLOGIES/evrosoyuz_vidkriv_tsentr_po_borotbi_z_kiberzlochinnistyu.html.

16. Европейский центр по борьбе с киберпреступностью демонстрирует свои первые результаты // Europa. Новости с европейским акцентом [Електронний ресурс]. – Режим доступу : http://euroua.com/europe/eu/1762.

17. Директива ЄС 2016/1148 від 6 липня 2016 року (NIS Directive) [Електронний ресурс]. – Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG.

18. Гнатюк С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / Ukrainian Scientific Journal of Information Security, 2013, vol. 19, issue 2 [Електронний ресурс]. – Режим доступу : http://ecobio.nau.edu.ua/index.php/Infosecurity/article/viewFile/4884/4985.

19. Баранова А. В., Уткіна М. Правова відповідальність за хакерство згідно законодавства України [Електронний ресурс] / А. В. Баранова, М. Уткіна. – Режим доступу : https://core.ac.uk/download/pdf/14060465.pdf.

References:

1. S. V. Kavun, Enterprise Insider Detection as an Integer Programming Problem. Intelligent Decision Technologies / S. V. Kavun, I. V. Sorbat, V. V. Kalashnikov // Smart Innovation, Systems and Technologies. – 2012. – No. 16 (2). – Pp. 281–289.

2. A. A. Lisaichuk, Problemy borotby iz kiberzlochynnistiu na mizhnarodnomu rivni [Elektronnyi resurs]. – Rezhym dostupu : https://internationalconference2014.wordpress.com/2014/ 10/09.

3. V. B. Dziundziuk, Poiava i rozvytok kiberzlochynnosti / V. B. Dziundziuk, B. V. Dziundziuk // Derzhavne budivnytstvo. – 2013. – No. 1 [Elektronnyi resurs]. – Rezhym dostupu : http://nbuv.gov.ua/UJRN/DeBu_2013_1_3.

4. "Delo Levina": kak vse bilo: Kompyuternaya gazeta [Elektronnyi resurs]. – Rezhym dostupu : http://www.nestor.minsk.by/kg/2003/36/kg33614.html.

5. N. V. Savchuk, Kiberzlochynnist: zmist ta metody borotby [Elektronnyi resurs] / N. V. Savchuk // Teoretychni ta prykladni pytannia ekonomiky. – Vyp. 19. – 2009. – Pp. 338–342. – P. 338 – Rezhym dostupu : http://archive.nbuv.gov.ua/portal/Soc_Gum/Tppe/2009_19/Zb19_48.pdf.

6. O. O. Kipa, Pravoporushennia v merezhi Internet / O. O. Kipa // Chasopys Kyivskoho universytetu prava. – 2010. – No. 4. – Pp. 346–349.

7. D. P. Bilenchuk, Kibreshakhrai – khto vony? / D. P. Bilenchuk // Militsiia Ukrainy. – 1999. – No. 7-8. – Pp. 32-34.

8. O. Amelin, Vyznachennia kiberzlochyniv u natsionalnomu zakonodavstvi / O. Amelin // Naukovyi chasopys Natsionalnoi akademii prokuratury Ukrainy. – 2016. – No. 3. – Pp. 1–10 [Elektronnyi resurs]. – Rezhym dostupu : http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/11-2016/amelin.pdf.

9. Konventsiia pro kiberzlochynnist : Zakon Ukrainy vid 7 veresnia 2005 poku No. 2824-IV [Elektronnyi resurs]. – Rezhym dostupu : http://zakon0.rada.gov.ua/laws/show/994_575.

10. Na Poltavshchyni zatrymaly prokurora pry otrymanni khabara v try bitkoiny [Elektronnyi resurs]. – Rezhym dostupu : http://uareview.com/bitcoin-habar.

11. U Kyievi dvokh zaruchnykiv kilka misiatsiv trymaly v poloni zarady vykupu v $5 mln u bitkoinakh [Elektronnyi resurs]. – Rezhym dostupu : https://espreso.tv/news/2018/01/26/u_kyyevi_dvokh_zaruchnykiv_kilka_misyaciv_trymaly_v_poloni_zarady_vykupu_v_5_mln_u_bitkoyinakh.

12. U Yaponii vidbulasia naibilsha v istorii kradizhka tsyfrovoi valiuty [Elektronnyi resurs]. – Rezhym dostupu : http://www.bbc.com/ukrainian/news-42847803.

13. A. A. Muzyka, Zakonodavstvo Ukrainy pro kryminalnu vidpovidalnist za komp'iuterni zlochyny: naukovo-praktychnyi komentar i shliakhy vdoskonalennia / A. A. Muzyka, D. S. Azarov. — K. : Vyd-vo Palyvoda A. V., 2005. – kilkist storinok???

14. Uhoda pro asotsiatsiiu mizh Ukrainoiu, z odniiei storony, ta Yevropeiskym Soiuzom, Yevropeiskym spivtovarystvom z atomnoi enerhii i yikhnimy derzhavamy-chlenamy, z inshoi storony : ratyfikovana Zakonom Ukrainy No. 1678-VII vid 16 veresnia 2014 roku [Elektronnyi resurs]. – Rezhym dostupu : http://zakon3.rada.gov.ua/laws/show/984_011.

15. Yevrosoiuz vidkryv tsentr po borotbi z kiberzlochynnistiu. Dzerkalo tyzhnia. Ukraina [Elektronnyi resurs]. – Rezhym dostupu : http://dt.ua/TECHNOLOGIES/evrosoyuz_vidkriv_tsentr_po_borotbi_z_kiberzlochinnistyu.html.

16. Evropeiskyi tsentr po borbe s kyberprestupnostiu demonstryruet svoi pervie rezultati // Europa. Novosty s evropeiskym aktsentom [Elektronnyi resurs]. – Rezhym dostupu : http://euroua.com/europe/eu/1762.

17. Dyrektyva YeS 2016/1148 vid 6 lypnia 2016 roku (NIS Directive) [Elektronnyi resurs]. – Rezhym dostupu : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG.

18. S. O. Hnatiuk, Kiberteroryzm: istoriia rozvytku, suchasni tendentsii ta kontrzakhody / Ukrainian Scientific Journal of Information Security, 2013, vol. 19, issue 2 [Elektronnyi resurs]. – Rezhym dostupu : http://ecobio.nau.edu.ua/index.php/Infosecurity/article/viewFile/4884/4985.

19. A. V. Baranova, M. Utkina, Pravova vidpovidalnist za khakerstvo zghidno zakonodavstva Ukrainy [Elektronnyi resurs]. – Rezhym dostupu : https://core.ac.uk/download/pdf/14060465.pdf.