можливість самостійно визначати вартість. Все це потребує належного правового регламентування. На жаль, в українському законодавстві немає норм, які б регулювали подібні відносини чи хоча б встановили правовий статус криптовалюти.

Натомість наприкінці 2014 року НБУ у своєму листі вказав, що вважає біткоїн грошовим сурогатом. На даний момент він не є заборонений, адже хоч НБУ і закликало утримуватись від використання криптовалюти, цей заклик носить лише рекомендаційний характер, тому згідно до принципу «дозволено все, що не заборонено» біткоїн широко використовується українцями і набирає все більшої популярності, що не є дивним з огляду на його переваги.

Криптовалюта являє собою апогей платіжних технологій і особливо ефективна для міжнародних транзакцій. Але поки в українському законодавстві не буде чітко прописано відповідні норми, які б регулювали порядок руху біткоїну та здійснення платежів з їх допомогою, економіний розвиток буде призупинено і подальший поступ буде неможливим. Відсутність норм гальмує розвиток торгівлі біткоїнами, яка принесла б чималий дохід, що, в свою чергу, міг би бути визнаний таким, що оподатковується. Також варто зазначити, що врегульована платформа привабила б на український ринок чимало інвесторів, що знову ж таки значно посприяло розвитку економіки. Тому чим швидше в Україні врегулюється питання правового статусу криптовалюти, тим швидше ми зможемо йти в ногу з передовими країнами світу.

Цезар А.Р.
студент,
Науковий керівник: **Діордіца І.В.**
кандидат юридичних наук, доцент,
Навчально-науковий юридичний інститут,
Національний авіаційний університет

АКТУАЛЬНІ ПИТАННЯ ПРАВОРОЗУМІННЯ «КІБЕРБЕЗПЕКИ» В УКРАЇНІ

Нині Україна знаходиться на тому етапі розвитку, коли усе суспільство не уявляє свого життя без інформації. Саме тому, на наше переконання, даний етап характеризується максимальною інформатизацією всіх сфер її життєдіяльності. Більшість процесів, в тому числі процеси, пов`язані з фінансовою, банківською та іншими важливими для існування країни сферами, були перенесені у так званий кіберпростір, і це тягне за собою одночасно і позитивні, і негативні наслідки. Наявність всієї інформації у

єдиному просторі, до якого можна отримати доступ в будь-який момент, робить більшість процесів простішими, але в той же час така система характеризується уразливістю цих процесів перед численними кіберзагрозами. Забезпечення безпеки у кіберпросторі нині є вкрай актуальним для нашої держави з огляду на те, що проти неї ведеться гібридна війна, одним з проявів якої є кібератаки на українські державні органи та установи.

Сьогоднішнє існування людства важко уявити без використання комп'ютерних та телекомунікаційних технологій. Розвиток інформаційного суспільства щодня набуває нових форм, які у підсумку впливають на формування думок, світогляду, звичок. Віртуальний світ стає буквально всеохоплюючим. Саме він здатен спрощувати те, що ще вчора було занадто складним. Завдяки єдиній інформаційній системі легшою та швидшою стала робота державних установ, промисловості, сфери послуг та інших важливих сфер для української держави. Все частіше у своєму житті новітні інформаційні технології використовують і звичайні громадяни, для яких той же Інтернет став невід'ємною частиною їхнього повсякденного життя, тому наше суспільство все більше залежать від безперешкодного функціонування окремого простору – кіберпростору, під яким прийнято розглядати сукупність взаємопов'язаних інформаційних ресурсів, програмного забезпечення, баз та банків даних, що обробляються в комп'ютерних мережах і пов'язаній з ними інфраструктурі, разом з об'єктами, що підпадають під їх контроль та управління. Захист інтересів держав та громадян в кіберпросторі стає життєво важливим завданням, яке перетворює безперешкодне використання ІТ-мереж на питання безпеки й оборони. Потенційна небезпека може загрожувати системам державного та військового управління, економіки та промисловості [1].

Забезпечення належного рівня кібернетичної безпеки є необхідною умовою розвитку інформаційного суспільства. Правову основу кібернетичної безпеки України становлять Конституція України, закони України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» та інші закони, Конвенція Ради Європи про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, Доктрина інформаційної безпеки України, а також видані на виконання законів інші нормативно-правові акти. Водночас, аналіз чинного законодавства дозволяє визначити як основну проблему правового забезпечення системи кібернетичної безпеки України відсутність розробленого та нормативно закріпленого понятійного апарата у сфері кібернетичної безпеки [2].

Різні аспекти правового забезпечення протидії кіберзагрозам досліджували В. М. Бутузов, В. Д. Гавловский, В. О. Голубєв, Д. В. Дубов, В. А. Номоконов, Н. А. Ожеван, М. А. Погорецький. Е. В. Рижков, К. В. Тітуніна, Т. Л. Тропіна та інші науковці. Проте, наукова розробка

проблем правового забезпечення системи кібернетичної безпеки до теперішнього часу не носила системного характеру, розглядалися в основному питання, пов'язані з протидією правової кіберзлочинності та кібертероризму.

Під кібернетичною безпекою взагалі розуміють стан захищеності життєво важливих прав та інтересів людини, суспільства, держави у кіберпросторі від внутрішніх і зовнішніх протиправних посягань та загроз таких посягань [3, с. 176].

Серед основних принципів забезпечення кібернетичної безпеки варто визначити такі, як: своєчасність і адекватність заходів кібернетичного захисту життєво важливих інтересів людини і громадянина, суспільства і держави реальним і потенційним кіберзагрозам; чітке розмежування повноважень і взаємодію органів державної влади у забезпеченні кібернетичної безпеки; використання в інтересах України міжнародних механізмів забезпечення кібернетичної безпеки.

Характерними ознаками, які нині уособлюють поняття кібербезпеки є сукупність активних захисних і розвідувальних дій, що в процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугрупувань розгортаються навколо інформаційного ресурсу (ІР), інформаційно-комунікаційних технологій (ІКТ) та інформаційно-телекомунікаційних систем (ІТС), які спрямовані на досягнення і утримання потенційними протиборчими сторонами переваги у протидії новим загрозам безпеці для власних об'єктів критично важливої інформаційної і кіберінфраструктури [4].

Кібербезпека є дуже важливим аспектом в сучасному світі. Захист інформації передбачає досягнення та збереження властивостей безпеки в ресурсах користувачів, що спрямовані на запобігання відповідним кіберзагрозам. Україна посіла п'яте місце в світі (і перше в Європі) за ризиками зіткнення з веб-загрозами в 2016 році. Третина (33,7%) українських користувачів мережі зіткнулися з загрозами, що поширюються через інтернет, що і є дуже важливим показником для актуальності кібербезпеки, її правового закріплення та практичної реалізації [5].

Підсумовуючи зазначене вище можна сказати, що кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації.

Немає сумнівів, що нині відбуваються формування та інституалізація Національної системи кібербезпеки, створюється її нормативно-правове забезпечення. Побудова дієвої системи кібернетичної безпеки України

вимагає чіткого визначення державної політики у цій сфері та випереджального правового реагування на динамічні зміни, що відбуваються у кіберпросторі.

Список використаних джерел:

1. Діордіца І. В. Поняття та зміст національної системи кібербезпеки [Електронний ресурс] / Ігор Володимирович Діордіца. – 2016. – Режим доступу до ресурсу: http://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/.

2. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / Володимир Петрович Шеломенцев. // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 107. – С. 312-320.

3. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) / В. М. Бутузов. – Київ: Кит, 2010. – С. 408.

4. Бурячок В. Л. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу / В. Л. Бурячок, О. Г. Корченко, В. О. Хорошко. – 2013. – С. 5-12.

5. Стратегія кібербезпеки України від 15.03.2016 р. [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/96/2016.