Деревянко Богдан Володимирович,
доктор юридичних наук, професор,
головний науковий співробітник відділу міжнародного приватного права
та правових проблем євроінтеграції
Науково-дослідного інституту приватного права і підприємництва
імені академіка Ф.Г. Бурчака НАПрН України;
провідний науковий співробітник
відділу господарсько-правових досліджень проблем економічної безпеки
Державної установи «Інститут економіко-правових досліджень імені В.К. Мамутова Національної академії наук України»

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВІЙНИ

Життя держави у стані війни дуже відрізняється від життя самої цієї та інших держав у звичайному стані. Громадяни і суб'єкти господарювання у своїй діяльності повинні переорієнтовуватися на потреби збройних сил. Значна частина державних витрат спрямовується на її захист, а не на розвиток соціальних, культурних, гуманітарних проєктів. Зрозуміло, що зовсім за іншими правилами мають працювати політики, культурні і громадські діячі, представники ЗМІ, блогери та інші публічні і медійні особи. Так, інформація, яка поширюється через ЗМІ, має бути перевіреною, а дозвіл на передачу стратегічно важливої інформації має узгоджуватися із компетентними підрозділами ЗСУ (наприклад, Головним управлінням розвідки) або СБУ. На початку повномасштабного вторгнення московської федерації в Україну у першій половині 2022 року неперевірена інформація про військові дії та пересування військових підрозділів часто була приводом для паніки серед окремих верств мирного населення. Натомість своєчасно і вірно подана інформація неодноразово дозволяла впливати на моральний дух ворога й отримувати локальні перемоги, брати у полон окремі підрозділи ворога тощо. Можна пригадати одну із перших таких операцій, проведених американськими військовими стосовно німецько-фашистських субмарин, без бою захоплених у полон через поширення в аргентинських ЗМІ неправдивої інформації про завершення війни і програш країн осі.

Сьогодні завдяки застосуванню сучасних цифрових технологій можна спілкуватися майже із кожною точкою планети, здійснювати банківські операції, укладати договори міжнародної купівлі-продажу та інші договори, вираховувати і привласнювати одиниці криптовалюти та здійснювати багато інших операцій. Цифрові технології активно застосовуються у

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Деревянко Б.В. Ризики здійснення операцій з криптовалютою (біткойнами) громадян і суб'єктів господарювання України. Форум права. 2017. № 3. С. 33–39. URL: https://repository.ndippp.gov.ua/handle/765432198/269.

воєнних цілях. В частині забезпечення цифрової та інформаційної безпеки важливе значення має те, хто виготовляє прилади, за посередництва яких здійснюються різноманітні операції, а також хто розробляє, обслуговує та є власником програмного забезпечення (іншими словами – того самого цифрового забезпечення), за допомогою якого здійснюються різноманітні операції. Сьогодні Україна не є розробником жодної відомої марки чи моделі мобільного телефону. Так само, розробники і власники найбільш відомих, поширених та ефективних комп'ютерних програм знаходяться за межами України. Це говорить про те, що інформація із електронних пристроїв українців може надходити на сервери до виробників цих пристроїв та до власників програмного забезпечення до них. Зрозуміло, що через це українці не повинні відмовлятися від використання сучасних технологій, проте мають дотримуватися певних безпекових правил.

В умовах війни різноманітні шахраї, хакери, «рейдери» та інші потенційні і реальні правопорушники і злочинці тільки активізувалися. Часто телефонні дзвінки українцям з метою отримання у них особистих даних та паролів від банківських карток і рахунків надходять від шахраїв із тимчасово окупованих територій та території московської федерації. Через неможливість правоохоронних органів України у поточний момент мати фізичний доступ до зловмисників, останні надмірно активізувалися. Така ситуація вимагає від держави та комерційних банків активніше проводити роботу з інформування населення про дотримання правил безпеки у поводженні із банківськими картками і рахунками. Також українці мають звертати увагу на громадянство власників комунікаційних мереж та місцезнаходження їх центральних компаній, зокрема багатоплатформового месенджеру «Телеграм» із власниками - громадянами московської федерації та місцезнаходженням серверів в еміраті Дубай. Це не означає, що українцям слід відмовитися від користування названим месенджером та іншими месенджерами і мережами. Навпаки, через ці мережі можна доводити правду до осіб, обмежених у користуванні іншими мережами (осіб з тимчасово окупованих територій та підданих московської федерації). Проте будь-яку персональну інформацію, особливо інших осіб, будь-які стратегічно важливі відомості передаватися такими мережами не повинні. Такі месенджери можна застосовувати спеціальними службами для проведення спеціальних операцій.

У сфері обігу криптовалют хакери можуть під'єднатися до комп'ютера у мережі інтернет і заволодіти ID-гаманця криптовалюти та паролем від нього. Значна кількість атак на комп'ютерні мережі, крадіжок криптовалюти та інших злочинів у сфері цифрових технологій відбувається з різноманітних офшорних зон, а в значній кількості випадків із держави-агресора. Раніше нами вказувалося, що фахівці зі сфери комп'ютерних технологій не радять зберігати «ID гаманця» і особливо пароль у пам'яті підключеного до мережі інтернет комп'ютеру. Найкращим вважається зберігання на паперовому носії або «холодне зберігання», тобто зберігання у пам'яті комп'ютера, не підключеного до мережі інтернет. Цей ризик має технологічну природу. Загрозу для власника гаманця біткойнів становлять дії третіх осіб [1, с. 36]. Для запобігання таким ризикам держава через фінансові установи має організувати консультування населення і суб'єктів господарювання України.