УДК 343.345

Максим Гребенюк,
канд. юрид. наук, доцент, заслужений юрист України, керівник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України

Андрій Черняк,
докт. юрид. наук, головний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України

ПРОБЛЕМИ ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ У СФЕРІ ЦИФРОВОЇ ЕКОНОМІКИ

Цифрова економіка стрімко розвивається у глобальних масштабах, виступаючи акселератором інновацій, конкурентоздатності та економічного зростання у світових масштабах. Більшість передових країн світу, таких як США, Канада, Японія, Німеччина, розвивають цифрову економіку та визначають впровадження цифрових технологій у своїх суспільствах як стратегічну мету, що у перспективі повинна стати рушійною силою інноваційного технологічного розвитку, у тому числі й для української економіки. Визначено загрозливі тенденції та фактори уразливості окремих сегментів сучасної цифрової економіки від злочинних посягань. Досліджено актуальні питання протидії організованій злочинності у важливих сферах цифрової економіки. Проведено аналіз стану криміногенної ситуації у сфері цифрової економіки, за результатами якого деталізовано шляхи вдосконалення правоохоронної діяльності з метою побудови ефективної системи боротьби зі злочинністю в сучасних умовах. Регламентовано пріоритетні напрями прогнозування та попередження «цифрової» злочинності.

Ключові слова: протидія, організована злочинність, кіберзлочинність, цифрова економіка, цифрові технології, інформаційно-комунікаційні технології, правоохоронна діяльність, кіберзлочинність, злочини економічної спрямованості.

Постановка проблеми. Сьогодні, з огляду на стрімке поширення у глобальному вимірі інформаційних та телекомунікаційних мереж, техніко-технологічний розвиток, актуальним є питання розвитку цифрової економіки. Тобто завдання, яке ставить цифрова економіка, – це запровадження цифрових технологій у промислове виробництво, освіту, медицину та інші сфери. Загальновідомо, що сектори економіки, що використовують цифрові технології, зростають швидше та якісніше. Сфери життєдіяльності, зокрема освіта, медицина, транспорт, сільське господарство, що модернізуються завдяки цифровим технологіям, стають набагато ефективнішими та створюють нову цінність і якість. Важливим складником формування інформатизованого суспільства є використання можливостей сучасних ІКТ з метою створення інформації, нових сучасних знань, товарів та електронних послуг, ефективного інформаційного обміну й, отже, сприяння стабільному розвитку країни. Застосування ІКТ в умовах інтенсивного розвитку ринкових відносин залишається одним із важливих елементів ефективного управління.

Аналіз останніх досліджень та публікацій. Наукова проблематика, винесена в заголовок статті, з різних точок зору вивчається багатьма вченими. Окремі аспекти цього наукового напряму розглядалися у фундаментальних працях таких науковців, як: В.М. Бутузов, С.В. Демедюк, В.В. Марков, О.В. Орлов, С.М. Рогозін, В.С. Цимбалюк, та інших.

Метою статті є дослідження сучасного стану нормативного та організаційного забезпечення протидії організованій злочинності у сфері цифрової економіки, виходячи з аналізу новел сучасного законодавства.

Виклад основного матеріалу. Розвиток цифрової економіки в Україні полягає у створенні ринкових стимулів, формуванні потреб щодо використання цифрових технологій, продуктів і послуг серед українських секторів промисловості, сфер життєдіяльності, бізнесу та суспільства для їх ефективності, конкурентоздатності та національного розвитку, зростання обсягів виробництва високотехнологічної продукції та благополуччя населення. Тобто цифрова

© М. Гребенюк, А. Черняк, 2019

трансформація – процес, який повинен бути одним із пріоритетів сучасного розвитку [1].

Україна робить дієві кроки з метою інтеграції до світового діджітал середовища. Так, 17 січня 2018 року своїм розпорядженням Уряд схвалив Концепцію розвитку цифрової економіки та суспільства України на 2018-2020 роки [1] і затвердив план заходів щодо її реалізації. У її положеннях деталізовано напрями цифрового розвитку нашої країни, якими є: подолання цифрового розриву шляхом розвитку цифрових інфраструктур; розвиток цифрових компетенцій; цифровізація реального сектору економіки, реалізація проектів цифрових трансформацій, громадська безпека, електронна демократія тощо. Тобто головні напрями розвитку цифрової економіки України доцільніше визначати у відповідній національній програмі. 5 липня 2018 року при Міністерстві економічного розвитку і торгівлі України почала роботу Координаційна рада з розвитку цифрової економіки в Україні [2]. Метою її діяльності є забезпечення виконання Концепції та Плану розвитку цифрової економіки та суспільства України до 2020 року. Невипадково протягом останніх десятиріч спостерігається глобальний перехід від промислового до інформаційного (цифрового) капіталу. Усе більші масштаби використання цифрового капіталу призводять до зростання цифрової ренти, коли прибутки генеруються за рахунок використання «великих даних». Наприклад, фактично «Google» чи «Facebook» вже зараз отримують цифрову ренту.

При цьому цифрові платформи стають осередками концентрації інформаційного (цифрового) капіталу, знижуючи транзакційні видатки для своїх користувачів, а також вирішуючи певною мірою проблему асиметрії інформації. Виходячи з міжнародного досвіду, оцінкою вартості інформаційного (цифрового) капіталу може бути ринкова капіталізація цифрових платформ, які поступово впроваджуються в Україні. Специфічними для цифрових платформ елементами регулювання є: інклюзивність (правила доступу користувачів до цифрових платформ), безпека особистих даних, збір великих масивів даних, дистанційна праця.

Слід зазначити, що у 2018 році в ЄС була документально оформлена революційна ідея створення спільного цифрового ринку: 22 країни підписали спільну декларацію про створення Європейського блокчейн-партнерства. Цей європейський проект передбачає обмін інформацією та технологіями між державами і приватним сектором. Зазначена декларація побудована на трьох основних принципах: безперешкодний доступ до цифрових продуктів та послуг; створення адекватного середовища для динамічного розвитку мережевих і цифрових технологій; використання можливостей цифрового ринку як важливого потенціалу для прискорення зростання економіки. Очікується, що практична реалізація цієї декларації на теренах ЄС дасть змогу запровадити єдину технічну стандартизацію з метою полегшення здійснення міжнародної електронної торгівлі, поступово зняти бар'єри в питаннях торгівлі діджитал-продуктами, покращити стан цифрової безпеки та приватності; відповідної інформаційної інфраструктури тощо. За задумом мають бути остаточно усунені «національні сегменти» таким чином, щоб цифрові платформи не були здатні блокувати доступ до продуктів та послуг за географічним принципом; спрощені питання інтернаціональної доставки товарів під час їх придбання з використанням мережі Інтернет; запроваджено надійний захист прав споживачів незалежно від того, в якій країні ЄС були придбані товари або послуги з використанням засобів електронної комерції.

Сучасні процеси цифрової трансформації економіки пов'язані з розвитком бізнес-моделей, які використовують цифрові платформи. Фактично протягом останнього десятиріччя відбувається революція платформ. Особливістю цифрових платформ є об'єднання різних груп споживачів, виробників, власників ресурсів на одному віртуальному майданчику. Вітчизняний цифровий капітал перебуває на стадії формування, але вже спостерігається велика кількість позитивних прикладів, оскільки можливості розвитку цифрової економіки в Україні пов'язані з розширенням використання цифрових платформ, які є точками зростання сучасної інформаційної економіки, при цьому перспективним напрямом розвитку цифрових платформ виступає технологія блокчейн [4].

Загальнопоширеним у світі є визначення цифрової економіки як електронної комерції, що здійснюється за допомогою сучасних інформаційних і комунікаційних технологій. Адже суцільний розвиток цифрових технологій також є однією з причин збільшення масштабів тіньової економіки, оскільки поряд із розвитком сучасних технологій виникають нові можливості для зростання «цифрової злочинності». Оцінка впливу «цифрової економіки» на національну та світову економіку, а також неминуче на всю соціальну сферу дуже важлива, з огляду на зростаючі проблеми поширення транснаціональної злочинності у віртуальному просторі, яка також модернізується на перманентній основі.

Організована кіберзлочинність може бути асоційована не тільки з проблемами інформаційної безпеки, але й із загрозами для державної безпеки, військово-промислового і виробничого комплексів, інфраструктури життєзабезпечення. Характеризуючи стан організованої злочинності у сфері економіки, доцільно виділяти її в окрему категорію для вивчення злочинності саме у сфері «цифрової економіки». Оцінка впливу цифрової економіки на національну та світову економіку дозволяє констатувати, що актуальним залишається суцільна модернізація злочинності, яка постійно вдосконалюється у рамках активної суцільної електронізації та цифровізації суспільства.

Практичні здобутки та надбання цифрової економіки активно використовуються транснаціональними організованими злочинними угрупованнями з метою отримання надприбутків шляхом вчинення злочинів економічної спрямованості на території однієї або декількох держав з використанням кіберпростору та його можливостей. Викладене зумовлює розкриття нагальних проблем протидії організованій злочинності у сфері цифрової економіки.

Як зазначено в доповіді Європолу «Оцінка загроз організованої кіберзлочинності (IOCTA)» (2018) [5], забезпечення правопорядку у кіберпросторі потребує активізації роботи з ідентифікації, локалізації окремих злочинців і злочинних груп, які є складовими елементами сучасної європейської кримінальної субкультури. Це передбачає насамперед створення національних і міжнародних баз даних про кіберзлочинність та її кримінологічний стан. У Стратегічному звіті «IOCTA» надаються основні рекомендації правоохоронним органам, політикам та регуляторним органам, щоб вони мали змогу ефективно та узгоджено реагувати на кіберзлочинність та протистояти їй. Акцентовано, що велике значення для успішної боротьби правоохоронних органів з кіберзлочинністю мають такі складники, як виділення достатніх ресурсів для дослідження шкідливого програмного забезпечення і нових бізнес-моделей кіберзлочинності, а також проведення стрес-тестів і аудиту безпеки державних органів і населення. Правоохоронні органи повинні мати інструменти, методи і досвід для боротьби зі злочинним зловживанням методами шифрування й анонімності.

Натепер профілактичні кампанії у сфері кіберзлочинності спрямовані в основному на громадян і бізнес, тобто потенційних жертв кіберзлочинності. Крім того, необхідно також активізувати профілактичну роботу з потенційними кіберзлочинцями, насамперед підлітками та молоддю, що володіють необхідними програмними навичками, а також працівниками у сфері ІТ. Основний акцент у проведенні профілактичної роботи повинен бути зроблений на роз'ясненні наслідків протиправної діяльності для самих злочинців. Варто зазначити, що національні профілактичні кампанії повинні бути скоординовані з міжнародними і громадськими організаціями. У рамках профілактичної діяльності особливу увагу необхідно приділити мобільним гаджетам та сучасним електронним пристроям як джерелам найбільшої небезпеки для їх власників і проникнення злочинців у приватні і корпоративні мережі. Правоохоронні органи спільно з некомерційними організаціями і приватним сектором повинні брати активну участь в інформаційно-просвітницьких заходах серед населення та громадськості.

Одним із головних завдань правоохоронних органів є боротьба з постачальниками кримінальних послуг та спеціалізованих інструментів, які є основою програмних, апаратних і кадрових структур європейської кіберзлочинності. До такого роду спеціалізованих інструментів належать: шкідливе програмне забезпечення, включаючи програми-вимагачі паролів, програми-шпигуни і банківські трояни, а також, відповідно, їх розробники, постачальники і покупці, провайдери, організатори і виконавці DDoS-атак як послуг; виробники ботнетів, особливо тих їх модифікацій, які використовуються для поширення інших шкідливих програм; здійснення DDoS-атак, а також злочинних маніпуляцій шляхом спотворення і «зашумлення» інформаційного простору.

З огляду на викладене, пріоритетними напрямами, на яких доцільно зосередити профілактичні зусилля правоохоронних органів, є:

1) платіжні шахрайства: шкідливі програми, які порушують цілісність платіжних систем, ускладнюють або блокують роботу банківських терміналів; системи «софт», що застосовуються для отримання готівкових коштів або конфіденційних даних під час користування кредитними картками, безконтактними картками і банківськими терміналами; системи «софт», що використовуються для крадіжки даних громадян, які перебувають у розпорядженні фінансових інституцій; системи «софт», що використовуються для викрадення грошових коштів і шахрайства у сфері електронної комерції і насамперед на транспорті, у роздрібних мережах і туристичному бізнесі;

2) сексуальна експлуатація дітей та підлітків он-лайн: боротьба з каналами

потокового відео, пов'язаного із сексуальним насильством щодо дітей та підлітків; припинення діяльності груп, що спеціалізуються на виготовленні та розповсюдженні злочинного контенту, пов'язаного з педофілією, і його поширенні в мережах DarkNet; виявлення за допомогою цифрових засобів конкретних жертв сексуального насильства й експлуатації та проведення операцій з їх порятунку;

3) наскрізна «цифрова злочинність»: вендори, покупці й адміністратори нелегальних торгових сайтів у DarkNet; кримінальні провайдери послуг із незаконної анонімізації і прихованого хостингу; «грошові мули» і «конверт центр» на території не тільки країн ЄС, а й тих, що обслуговують громадян ЄС; експерти, розробники і програмісти, що сприяють використанню біткоїнів і інших віртуальних валют з метою кримінальних обмінних операцій, відмивання грошей і платіжних операцій, пов'язаних із будь-якими видами фінансування тероризму.

Більшість кримінальних інструментів і послуг може бути використана в найрізноманітніших сферах злочинної діяльності. Відповідно, викриття і припинення діяльності злочинних мереж, що займаються виготовленням програмних інструментів і надають послуги з їх використанням в інтересах інших злочинних груп, дасть змогу протидіяти кіберзлочинності.

Аналіз стану криміногенної ситуації у сфері цифрової економіки. Сьогодні транснаціональні організовані злочинні угрупування поширюють свою протиправну діяльність не тільки у кримінальній економіці, але й у легальному секторі, особливо фінансовому. У світі відбувається поступове зрощення криміналу та економіки, зокрема, є численні приклади такого роду симбіозу кримінальної та легальної економік, який стає все більш характерним. Також це реалізація контрафактних товарів, продаж на легальних ринках об'єктів права інтелектуальної власності, здобутої кримінальним шляхом, використання інсайдерської інформації в операціях на фондових ринках тощо. Чим далі, тим більше зрощення кримінальної та легальної економік формує ландшафт для транснаціональної організованої злочинності.

Загалом, кримінальні мережі і групи хакерів постійно прагнуть використовувати новітні технічні розробки, такі як криптовалюта й анонімні (безконтактні) способи оплати. Швидка обробка транзакцій і поширення ефективних інструментів анонімізації ускладнюють діяльність правоохоронних органів щодо доказової ідентифікації реальних бенефіціарів доходів, одержаних злочинним шляхом. Зростаюча кількість онлайн платформ і додатків пропонують нові способи переказу грошей. Вони не регулюються тією ж мірою, що й традиційні постачальники фінансових послуг, що робить їх привабливими для злочинців. Крім того, за даними Європолу, існує ймовірність, що деякі поширені платіжні системи на основі блокчейна через компанії-«метелики» можуть контролюватися міжнародним криміналом. Онлайн-банкінг також полегшує життя злочинцям. За даними Європолу, на «чорному» ринку активно продаються спеціальні програми, що дозволяють обійти біометричну ідентифікацію власників рахунків фізичних та юридичних осіб.

Ще одним напрямом транснаціональної злочинної діяльності є встановлення все більш тісних зв'язків з представниками корпоративного сектору в деяких країнах ЄС. Така взаємодія будується за трьома напрямами. По-перше, бізнес-структури, іноді навіть найбільші корпорації замовляють послуги у кіберзлочинців. Найбільшою мірою це стосується кіберзлочинності і пов'язане з крадіжкою інтелектуальної власності та компрометуючої конкурентів документації. По-друге, ОЗУ намагаються інвестувати злочинні прибутки в легальний бізнес. Особливий інтерес ОЗУ проявляють до: будівництва, прибирання міського сміття та проблем екології. Також злочинність інвестує в ІТ-індустрію, особливо у фінансові технології, виготовлення відеоігор і різного роду мобільних додатків, які передбачають отримання від клієнтів персональних даних. Слід вказати, що значна частина адвокатських, консультативних та реєстраційних бюро, пов'язаних із податковим плануванням і трансфертом коштів в офшорні зони, якими користується легальний бізнес, перебуває під контролем міжнародних ОЗУ.

Сучасною типовою рисою останніх років стала пильна увага злочинців до найбільших європейських транспортних вузлів і магістралей, які активно використовуються з метою глобального розподілу товарних потоків. Натепер найбільші темпи динаміки злочинності припадають на локації, які характеризуються декількома факторами, включаючи наявність ефективної та розгалуженої транспортної інфраструктури, близькість або зв'язок із країнами джерелами товарів, послуг або мігрантів, доступ до інвестиційних можливостей, а також попит на незаконні товари та послуги.

На цьому тлі збільшується кількість злочинів економічної спрямованості у кіберпросторі, у зв'язку з чим бізнес і держава змушені нести масштабні збитки, які обчислюються мільярдами доларів США. Отже,

викладене вище зумовлює зробити такі висновки. **По-перше,** традиційна правоохоронна діяльність організаційно повинна бути істотно переформатована шляхом посилення оперативного інформаційного співробітництва та взаємодії між різними правоохоронними органами за умов розширення механізмів координуючого управління такими органами. **По-друге,** є нагальна потреба у формуванні відомчих і міжвідомчих правоохоронних інформаційних мереж для спільних дій, погоджених за цілями, а не за результатами. **По-третє,** доцільно розвивати застосування в правоохоронній діяльності цифрових джерел доказів, загальних (мережевих) цифрових джерел оперативної інформації, інформаційних реєстрів. **По-четверте,** доцільно переглянути підходи до регламентації конфіденційності інформації про оперативну обстановку, відкривши до неї мережевий розподілений узгоджений доступ різних правоохоронних органів, які у рамках компетенції здійснюють боротьбу зі злочинністю у сфері цифрової економіки.

Слушно вказує В.П. Поїзд, що декриміналізація мережі Інтернет, у тому числі мінімізація можливостей її використання як складника інфраструктури злочинності, вимагає формування правової основи здійснення фінансових, податкових та господарських операцій через мережу Інтернет; розроблення інституційної основи контролю за національним сегментом мережі Інтернет; розроблення принципів, тактичних прийомів та належне кадрове забезпечення оперативного обслуговування національного сегменту мережі [9, с. 309].

На цьому тлі О. Вінник об'єктивно зазначає, що формування цифрової економіки та її соціальне спрямування вимагає адекватного правового регулювання, важливою частиною якого є визначення понять, що її характеризують (суб'єкти, об'єкти, засоби, зв'язки тощо), насамперед потребує вирішення проблема уніфікації термінів, притаманних цифровій економіці, їх закріплення в кодифікованому акті, яким може бути навіть Закон «Про цифрову економіку» [10, с.165].

Враховуючи викладене, ефективними шляхами щодо удосконалення системної протидії організованій злочинності у сферах цифрової економіки мають стати: технічна антивірусна підтримка правоохоронців, яка включає регулярне оновлення ліцензованого програмного забезпечення, криміналістичної техніки; залучення нових ІТ-спеціалістів до підрозділів відповідних правоохоронних органів; міжнародна цифрова інтеграція, унормування на правовій основі інформаційного обміну, узгодження понятійного апарату щодо цифрової економіки та її складників; узагальнення та практичне забезпечення поширення кращих практик європейського досвіду у країнах з розвинутою цифровою економікою у сфері протидії злочинності у цій площині; управління ризиками цифрової безпеки в економічній сфері на рівні світової інтеграції, держави, окремих галузей, приватного сектора, підприємств, які мають стратегічне значення для держави.

Висновки

Цифрова економіка активно працює майже у всіх сферах життєдіяльності, зокрема у хмарних технологіях, Інтернет-банкінгу, у сфері придбання товарів з використанням смартфону, он-лайн консультації тощо. Наявна нормативна база не може забезпечити належний рівень протидії технологічним злочинам. На цьому тлі чисельність скоєних злочинів у сфері ІТ-технологій постійно зростає. Враховуючи викладене, видається доцільним сконцентрувати увагу на таких актуальних питаннях комплексної протидії організованій злочинності у сфері цифрової економіки. Спільний характер проблем протидії злочинності у сфері цифрової економіки як в Україні, так і за кордоном дозволяє зробити висновок про необхідність акумуляції та аналізу позитивного досвіду зарубіжних країн у цій площині. Злочинність у сфері цифрової економіки має транскордонний характер, а тому заходи щодо протидії такій злочинності передбачають налагодження, перш за все, ефективного міжнародного співробітництва організаційно-правового та технічного характеру.

До ефективних засобів протидії злочинності у сфері цифрової економіки можна віднести: перманентну модернізацію програмного забезпечення комп'ютерних систем правоохоронних органів; суцільну інтеграцію заходів посилення інформаційної безпеки на основі новітніх розробок та впровадження сучасних систем захисту інформації; створення відповідної нормативно-правової бази, здатної забезпечити протидію сучасним кіберзагрозам.

По-перше, як на міжнародному, так і на національному рівнях доцільно розробити універсальні підходи до нормативного врегулювання цифрової економіки, оскільки різні країни світу на власний розсуд тлумачать базові поняття та їх ознаки (блокчейн, криптовалюта тощо). Наприклад, у сучасному світі існує понад 3 тисячі різноманітних криптовалют, проте відсутнє єдине їх розуміння, не визначено статус відповідних криптобірж, де вони продаються та купуються.

По-друге, доцільно використовувати можливості блокчейн-технологій для

розслідування злочинів в Інтернет просторі, що передбачає налагодження конструктивного діалогу між правоохоронними органами та криптовалютними кампаніями з метою запобігання та протидії злочинній діяльності у блокчейн-платформах. Встановлення причетності використання блокчейн-технологій під час скоєння злочинів певними особами можливо лише за умов вилучення правоохоронцями комп'ютерної техніки або мобільних телефонів, на які встановлено відповідне програмне забезпечення.

По-третє, повинні активно впроваджуватися принципи електронного документообігу, що передбачає утворення єдиного середовища довіри з метою забезпечення учасників цифрової економіки засобами довірених цифрових дистанційних комунікацій. Крім того, з метою стимулювання впровадження цифрової економіки у сфері інтелектуальної власності має бути розроблено порядок цифрового обігу об'єктів інтелектуальної власності у тому числі з метою боротьби з «патентними тролями».

По-четверте, у нашій країні працює 4 тисячі IT-компаній і понад 110 R&D центрів всесвітньо відомих міжнародних компаній. Оскільки ключовою метою діяльності правоохоронних органів є боротьба з постачальниками кримінальних цифрових послуг та відповідних інструментів, то доцільним є створення відповідного реєстру таких постачальників, які мають сумнівну репутацію, зокрема IT-компаній, інших суб'єктів господарювання, що дасть змогу певним чином контролювати ситуацію у цій сфері.

Список використаних джерел:

1. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації : Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80

2. В Україні запрацювала Координаційна рада з розвитку цифрової економіки та суспільства. URL: https://www.ukrinform.ua/rubric-economy/2493487-v-ukraini-zapracuvala-koordinacijna-rada-z-rozvitku-cifrovoi-ekonomiki.html.

3. Оцінка загроз організованої кіберзлочинності (IOCTA) 2018. URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.

4. ЄС працює над посиленням боротьби з відмиванням грошей-FT. URL: https://www.unn.com.ua/uk/news/1751338-yes-pratsyuye-nad-posilennyam-borotbi-z-vidmivannyam-groshey-ft.

5. Ляшенко В.І., Вишневський О.С. Цифрова модернізація економіки України як можливість проривного розвитку : монографія. Київ, 2018. 252 с.

6. Генасамблея ООН ухвалила резолюцію щодо кібербезпеки. URL: https://www.unn.com.ua/uk/news/1768487-genasambleya-oon-ukhvalila.

7. Про схвалення Концепції розвитку електронного урядування в Україні : Розпорядження Кабінету Міністрів України від 20 вересня 2017 р. № 649-р / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80.

8. Про затвердження Плану заходів з реалізації Концепції розвитку електронного урядування в Україні : Розпорядження Кабінету Міністрів України від 22 серпня 2018 р. № 617-р / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/617-2018-%D1%80.

9. Поїзд В. П. Високі інформаційні технології як складова сучасної економічної злочинності. *Форум права*. 2013. № 4. С. 306-310. URL: http://nbuv.gov.ua/j-pdf/FP_index.htm_2013_4_53.pdf.

10. Вінник О. Регулювання відносин у сфері цифрової економіки: проблеми термінології. *Підприємництво, господарство і право*. 2017. № 11. С. 163-166.

Цифровая экономика стремительно развивается в глобальных масштабах, являясь акселератором инноваций, конкурентоспособности и экономического роста в мировых масштабах. Большинство передовых стран мира, таких как США, Канада, Япония, Германия, развивают цифровую экономику и считают внедрение цифровых технологий в своих обществах стратегической целью, что в перспективе должно стать движущей силой инновационного технологического развития, в том числе и для украинской экономики. Определены угрожающие тенденции и факторы незащищенности отдельных сегментов современной цифровой экономики от преступных посягательств. Исследованы актуальные вопросы противодействия организованной преступности в важных сферах цифровой экономики. Проведен анализ криминогенной ситуации в сфере цифровой экономики, по результатам которого детализированы пути совершенствования правоохранительной деятельности с целью построения эффективной системы борьбы с преступностью в современных условиях. Регламентированы приоритетные направления прогнозирования и предупреждения «цифровой» преступности.

Ключевые слова: противодействие, организованная преступность, киберпреступность, цифровая экономика, цифровые технологии, информационно-коммуникационные технологии, правоохранительная деятельность, киберпреступность, преступления экономической направленности.

The digital economy is developing globally at a fast pace, acting as an innovation accelerator, competitiveness and economic growth on a global scale. Most of the advanced countries of the world, such as the USA, Canada, Japan, and Germany, are developing the digital economy and introducing digital technologies in their societies as a strategic goal, which in the long term should be the driving force of innovative technological development, including for the Ukrainian economy. Threatening trends and vulnerabilities of certain segments of the modern digital economy from criminal attacks are determined. Actual issues of countering organized crime in important areas of the digital economy are investigated. The analysis of the state of the criminal situation in the digital economy was carried out. Based on its results, the ways of improving law enforcement activity were detailed in order to build an effective crime control system in modern conditions. Priority directions for predicting and preventing "digital" crime have been regulated.

Key words: counteraction, organized crime, cybercrime, digital economy, digital technologies, information and communication technologies, law enforcement activity, crimes of economic orientation.