УДК 343.37
https://orcid.org/0000-0002-3077-4942
DOI https://doi.org/10.32703/2663-6352/2021-2-10-120-127
Топчій Ганна Сергіївна,
кандидат педагогічних наук,
старший викладач кафедри соціально-гуманітарних дисциплін
Київського інституту Національної гвардії України,
м. Київ, Україна

ПРАВОВІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З МЕТОЮ ПРОТИДІЇ ЗЛОЧИННОСТІ

Анотація: *Стаття є дослідженням актуальних аспектів інформаційної безпеки в контексті протидії злочинності. Проведено аналіз дефініції «інформація» та «інформаційна безпека» згідно чинних нормативно-правових актів. Визначено чинники та основні завдання забезпечення інформаційної безпеки в контексті протидії злочинності. Також продемонстровано особливості протиправних діянь у окремих напрямках життєдіяльності суспільства, в яких значення інформаційної безпеки в контексті протидії злочинності надзвичайно актуальне, а саме: продаж наркотичних та психотропних засобів, крадіжки грошей та відмивання тіньового капіталу, промислове шпигунство, доведення до самогубства. Саме тому, зважаючи на рівень і темпи зростання злочинності суспільство вимагає від державних органів адекватного реагування та забезпечення інформаційної безпеки, у тому числі і на законодавчому рівні.*

Ключові слова: *інформація, інформаційна безпека, протидія злочинності, забезпечення інформаційної безпеки.*

Abstract: *The article is a study of current aspects of information security in the context of combating crime. It is noted that the problem of protection of information and information systems is now one of the most pressing in Ukraine and in the world. New opportunities provided by information technologies, their widespread use and accessibility make this area extremely attractive to criminals, and the dynamic development of telecommunications networks, the creation of numerous information resources and databases, the development of better devices create conditions that facilitate crime in this area, the number of which is increasing in Ukraine. An analysis of the definition of «information» and «information security» according to current regulations. The factors and main tasks of information security in the context of combating crime are identified. It is emphasized that cybercrime is not limited to crimes committed in the global information network, it applies to all types of crimes committed in the information and telecommunications sector, where information, information resources, information technology can be the subject of criminal encroachment, the environment in which offenses occur and means or an instrument of crime. The peculiarities of illegal actions in certain areas of society are demonstrated, in which the importance of information security in the context of combating crime is extremely relevant, namely: sale of drugs and psychotropic drugs, theft of money and money laundering, industrial espionage, suicide. It is noted that one of the main problems why information technology crimes have a low level of disclosure is that people lack special knowledge. Due to the fact that the rapid development of*

information technology methods of forensic examination of these objects require constant updating and refinement. It was also found that the state authorities are directly involved in solving issues related to information security. That is why, given the level and rate of growth of crime, society requires public authorities to respond adequately and ensure information security, including at the legislative level.

***Keywords**: information, information security, crime prevention, information security.*

Постановка проблеми. Розвиток системи кримінального права підтверджує, що в різні історичні періоди об'єктом правової захисту ставали лише ті суспільні відносини, які на даному історичному етапі є значущими для держави, суспільства і людини. Проблематика захисту інформації, зараз є однією з найактуальніших в Україні і в світі. Нові можливості, які надають інформаційні технології, їх широка поширеність і доступність роблять цю галузь надзвичайно привабливою для представників криміналітету, а динамічний розвиток телекомунікаційних мереж, створення численних інформаційних ресурсів і баз даних, розробка більш досконалих пристроїв створюють умови, які полегшують вчинення злочинів у цій сфері, число яких в Україні збільшується. Про актуальність проблеми забезпечення інформаційної безпеки засвідчують об'єктивні дані статистики МВС та Генеральної Прокуратури України. Так, у 2005–2009 рр. спостерігалася загальна тенденція до збільшення кількості злочинів у сфері високих інформаційних технологій: у 2005 р. їх було виявлено 615, а у 2009 р. – 707. З 2010 р. ведеться статистика злочинів у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. У 2010 р. їх було зареєстровано 190, у 2011 р. – 131, а у 2017 р. – вже 2573 [10].

Аналіз останніх досліджень і публікацій. Проблематика інформаційної безпеки складна і багатоаспектна, що зумовлює необхідність вивчення й узагальнення наукових праць представників різних галузей юридичної науки. Окремі аспекти правового регулювання інформаційної сфери стали об'єктом наукового аналізу в працях українських і зарубіжних дослідників, зокрема І. Арістової, І. Бачило, Р. Калюжного, Т. Костецької, О. Кохановської, Е. Макаренко, В. Цимбалюка. Ключовими для вивчення проблеми забезпечення інформаційної безпеки стали дослідження В. Гурковського, О. Золотар, В. Копилова, Б. Кормича, В. Ліпкана, В. Настюка, Н. Нижник, М. Швеця, А. Селіванова.

Мета дослідження полягає в аналізі сутності головного поняття теми дослідження, розкритті об'єкту, завдань та основних напрямків життєдіяльності суспільства, в яких значення інформаційної безпеки в контексті протидії злочинності надзвичайно актуальне.

Виклад основного матеріалу. У контексті нашого дослідження необхідно звернути увагу на зміст категорії «безпека», котра у житті людини відіграє роль орієнтиру, навколо якого групуються цінності людського існування. Це поняття багатопланове, з цього приводу в науці існує багато думок. У буквальному розумінні безпека означає відсутність небезпеки. Потреба безпеки належить до числа базових мотиваційних механізмів у життєдіяльності людини, і в цьому відношенні людина мало чим відрізняється від будь-кого з інших живих істот. Крім того, безпека

становить безсумнівну цінність, що має універсальний характер, оскільки визнається всіма людьми незалежно від їхньої расової, національної чи соціальної належності. Законодавче визначення інформаційної безпеки зафіксоване в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.» в якому говориться, що інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації (п. 13 Закону) [2]. Про важливість захисту інформаційної безпеки наголошується в Конституції України: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» (ст. 17) [1].

Інформаційна безпека також є важливою складовою протидії злочинності, яка набула поширення у сучасному Інтернет суспільстві. Так, кіберзлочинність не обмежується рамками злочинів вчинених у глобальній інформаційній мережі, вона поширюється на всі види злочинів вчинених в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть виступати предметом злочинних посягань, середовищем, в якому відбуваються правопорушення і засобом або знаряддям злочину. Це і порнографія, шахрайства, виготовлення та поширення шкідливих програм, викрадення ідентифікаційних даних осіб та багато інших. 23 листопада 2001 року в Будапешті було підписано Конвенцію Ради Європи про кіберзлочинність, в якій йде мова про протидію комп'ютерним злочинам та співробітництво й координацію діяльності правоохоронних органів різних держав. На сьогодні її ратифіковано у 18 країнах та підписано 25 країнами, серед яких і Україною [3].

Головною ознакою стану захищеності в інформаційній сфері (інформаційної безпеки) є оптимальне співвідношення інтересів людини, суспільства й держави. Чинниками забезпечення інформаційної безпеки держави є гарантування:

- захищеності особи, суспільства й держави від шкідливого впливу певних видів інформації (в даному разі йдеться не про інформацію, віднесену до категорій з обмеженим доступом, а про такі її види, котрі здатні зашкодити вказаним суб'єктам інформаційних відносин);
- конфіденційності інформації з обмеженим доступом;
- безпеки інформації загального доступу, мереж зв'язку, інформаційно-телекомунікаційних систем, технічних та програмних засобів виконання маніпуляцій з інформацією, доступу до інформації [6, с. 89].

Разом з тим протидія злочинності – це особливий інтегрований, багаторівневий об'єкт соціального управління, що являє собою різноманітну за формами діяльність відповідних суб'єктів (державних і недержавних органів та установ, громадських формувань та окремих громадян), які взаємодіють у вигляді системи різнорідних заходів, спрямованих на пошук шляхів, засобів та інших можливостей ефективного впливу на злочинність із метою зниження інтенсивності

процесів детермінації злочинності на всіх рівнях, нейтралізації дії її причин та умов для обмеження кількості злочинних проявів до певного рівня [8, с. 277].

Проте, механізми контролю, запобігання та розслідування злочинів у кіберпросторі дуже обмежені соціально і технологічно. Анонімність мережі Інтернет, вразливість бездротового доступу і використання проксі-серверів істотно ускладнюють виявлення злочинців: для вчинення злочину може використовуватися «ланцюжок» серверів, злочини можуть бути вчинені шляхом виходу в Інтернет через точки загального доступу, такі, як Інтернет-кафе, технології дозволяють також «зламати» доступ в чужу бездротову мережу Wi-Fi. Отже, існує достатньо способів ускладнити припинення і розслідування злочинів. Боротьба з кіберзлочинністю неможлива без глибокого розуміння і правових проблем регулювання інформаційних мереж. Саме аналіз взаємозв'язку між технічними характеристиками мережі і зумовленими цими характеристиками правовими і соціальними труднощами, з якими стикаються законодавці та правоохоронні органи, є першим кроком до можливого вироблення механізмів адекватного реагування на розвиток і зростання кіберзлочинності [7, с. 101].

Такою ситуацією активно користуються кримінальні угрупування для розповсюдження наркотичних засобів через мобільні месенджери Viber, WhatsApp та Telegram, які можна встановлювати на смартфони. Основною особливістю більшості програм месенджерів є те що вся інформація або розмови, що ведуться через месенджер піддаються шифруванню. Тобто забезпечується так званий принцип анонімності. Дуже корисна функція для абонентів у якій на жаль є зворотна сторона. Якщо абонент вирішить чинити протиправні дії, то встановити його особистість практично неможливо.

Механізм такого злочину, на перший погляд, дуже простий. Як що хтось вирішив придбати наркотичні речовини, йому не потрібно особисто шукати розповсюджувачів «зілля», виходити з ними на зв'язок, домовлятися про зустріч. Досить зайти на вказаний прямо на стіні анонімний канал Telegram (месенджер для смартфонів) або спеціалізований сайт, зробити замовлення, оплатити на банківську картку або поповнити рахунок телефону. Після цього клієнту надсилають фото «закладки» – місця, де на вулиці захований пакет з наркотиками. Залишається лише підібрати його. Онлайн-торговці ховаються за анонімними ніками та значно активізувалися в останні роки. Так, у 2016 році МВС зафіксувало 1,9 тис фактів збуту наркотиків, у 2017–3,6 тис. І якщо раніше наркопродажами в Мережі займалося 26 груп, то у 2018 році поліцейські розкрили 108 подібних структур [9, с. 140]. А протягом 2020 р. було ліквідовано більше 100 інтернет-крамниць, через які щодоби збувалося близько 50 тисяч доз наркотиків.

Криміналістична особливість кіберзлочинів у тому, що їх припинення та розслідування неможливе без використання комп'ютерних технологій. Оперативний пошук має включати низку заходів, які фактично є оперативно-розшуковими (оперативно-пошукові заходи із забезпечення оперативної закупівлі та (або) контрольованого постачання товарів, заборонених для відкритого обігу; оперативне впровадження у віртуальні соціальні групи, що мають деструктивні цілі, з метою отримання інформації про їх персональний склад, місця зустрічей, плани та засоби, що використовуються в деструктивній

діяльності; оперативно-аналітичні заходи, спрямовані на прогноз розвитку ситуації, розробки заходів з утримання її під контролем, заходи оперативно-технічного характеру) і проводитись він має лише тими правоохоронними органами, до компетенції яких віднесено проведення оперативних операцій [12, с. 279].

Ще одним пріоритетним напрямом протидії злочинності є боротьба з комп'ютерними злочинами у сфері економіки. Серед основних завдань на цьому напрямку діяльності необхідно назвати протидію легалізації тіньових доходів. Аналіз схем відмивання коштів свідчить про значну зацікавленість організованої злочинності у використанні можливостей електронних платіжних систем, які дозволяють здійснювати миттєві перекази коштів із забезпеченням практично повної анонімності контрагентів. Особливий інтерес у світлі проблеми становить і те, що електронні платіжні системи не належать до розряду суб'єктів первинного фінансового моніторингу, а тому не зобов'язані інформувати наглядові органи про виявлення підозрілих транзакцій, зберігати відомості про транзакції, а також дані, що дозволяють ідентифікувати клієнта.

Необхідно зазначити, що фінансовий сектор економіки, тобто банки та їх послуги, вважається одним із найбільш уразливих до кіберзлочинів. Так, за оцінками експертів, в останні місяці тільки в м. Києві фіксується до двадцяти випадків крадіжки грошей через клієнт банк в місяць. Суми становлять від 20 тис до 40 млн грн. Однак подібні факти замовчуються, повідомлень в ЗМІ про них практично немає. Ні потерпілим, ні банкам не вигідний галас навколо того, що відбувається. У ряді випадків бувають ситуації, коли такі шахрайські схеми реалізуються організованими групами, у які входять представники банків [5].

Варто зазначити, що банки і платіжні системи намагаються не показувати реальних збитків понесених від хакерських атак з метою збереження довіри клієнтів. Достовірний обсяг злочинності такого типу, на сьогоднішній день, оцінити достатньо важко оскільки фінансові установи скривають від правоохоронних органів більшість фактів кібератак на свої установи, піклуючись про свою репутацію серед клієнтів; за умови незначних фінансових втрат, фінансові установи не проводять навіть внутрішніх розслідувань з огляду на те, що людські, фінансові та інші затрати на таке їх проведення значно перевищують втрати.

Важливе місце у забезпеченні інформаційної безпеки в контексті протидії злочинності посідає інформаційна безпека підприємницької діяльності. Необхідно зазначити, що в Україні широко поширений такий вид злочинів пов'язаний з підприємницькою діяльністю як промислове шпигунство, яке здійснюється як прийнятний спосіб ведення бізнесу, без наявності ефективного чинного законодавства для запобігання цьому. Очевидно, що у сфері бізнесу інформація є більш цінною, ніж будь-коли. Кожне підприємство є вразливим до крадіжки інформації. Близько 85% випадків промислового шпигунства здійснюються співробітниками підприємств, безпека котрих стосується, насамперед, захисту від зовнішніх загроз, незважаючи на витік інформації через внутрішні елементи. Законодавство, однак, не завжди захищає від протиправних дій, учинених промисловим шпигуном, що підлягає цивільному або кримінальному переслідуванню. Особливості конфіденційної інформації, що є вкраденою, широко

оприлюднюються в ході судового процесу, у результаті чого її значення нівелюється [4, с. 26].

Також, останнім часом в Україні постала нова, дуже серйозна загроза інформаційної безпеки, яка стрімко поширилася серед молоді. Це створення таких інтернет-банд як «Синій кит», «Тихий дім», «Кити пливуть Вгору», «Море китів», «Біжи або помри», «Розбуди мене в 4.20», F57, F58, FF33, D28 тощо. Метою таких сайтів є пропаганда самогубства серед дітей та підлітків. Слід зазначити, що жертвами стають діти, в яких є проблеми з батьками, з друзями в школі, тобто особливо вразливі діти, які не отримують необхідної уваги, підтримки від дорослих, любові та відчуття захищеності у родині [11, с. 139].

Однією з головних проблем, чому злочини в сфері інформаційних технологій мають низький рівень розкриття, є те, що людям не вистачає спеціальних знань. У зв'язку з тим, що бурхливий розвиток інформаційних технологій методики судово-експертного дослідження даних об'єктів вимагають постійного оновлення та доопрацювання. А щодо наукової експертизи, то він повністю залежить від рівня професійної підготовки експертних кадрів. У світі досить ретельно підходять до проблеми боротьби з кіберзлочинами, і до її вирішення безпосередньо залучається державна влада. Адже ту кількість інформації, яка протікає по мережі Інтернет щоденно, просто нереально контролювати самостійно. Тому, починаючи з 2009 року, влада США розпочала створення власних кібервійськ – Агентство національної безпеки, яке також опікується питаннями інформаційної війни. У ЄС функціонує Агентство з мережевої та інформаційної безпеки, у НАТО створений комітет з кібернетичної оборони, а також Спільний центр з кібернетичної оборони.

Сьогодні рівень і темпи зростання кіберзлочинності вимагають адекватного реагування, у тому числі і на законодавчому рівні. А тому, потребують змін положення законодавства про порядок і підстави виконання запитів, отриманих від правоохоронних органів у рамках виконання зобов'язань України, узятих у зв'язку з ратифікацією «Конвенції про кіберзлочинність». Як наслідок, одним із пріоритетних напрямків є організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою.

Висновки. Проведене дослідження дозволяє зробити висновки про те, що інформаційна безпека є важливою складовою протидії злочинності, оскільки забезпечує захист від всіх видів злочинів, що вчиняються в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть виступати предметом злочинних посягань, середовищем, в якому відбуваються правопорушення і засобом або знаряддям злочину. Розкрито зміст поняття «інформація» та «інформаційна безпека» згідно діючим нормативно-правових актів та наголошено на значенні міжнародного співробітництва у цій сфері. Також продемонстровано особливості протиправних діянь у окремих напрямках життєдіяльності суспільства, в яких значення інформаційної безпеки в контексті протидії злочинності надзвичайно актуальне, а саме: продаж наркотичних та психотропних засобів, крадіжки грошей та відмивання тіньового капіталу, промислове шпигунство, доведення до самогубства. Наголошено, що

без належної взаємодії поліції з населенням, яка включає в себе просвітницьку роботу з питань інформаційної безпеки, неможливо казати про якісну протидію злочинності.

Література:

1. Конституція України від 28 червня 1996 р. URL: http: // zakon5. rada. gov. ua / laws / show / 254к / 96-вр (дата звернення: 30.09.2021).
2. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.: Закон України від 09 січня 2007 р. № 537-V. URL: http: // zakon. rada. gov. ua / laws / show / 537–16? find=1&text=%E1% E5% E7% E. (дата звернення: 30.09.2021).
3. Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи: Закон України від 21 липня 2006 р. № 23-V. URL: https: // zakon. rada. gov. ua / laws / show / 23–16#Text. (дата звернення: 30.09.2021).
4. Березіна Л. М., Братанов Б. В. Характерні особливості конкурентної розвідки та промислового шпигунства підприємств // Інтелект XXI. 2020. № 2. С. 22–27.
5.Довбиш Н. Кіберзлочинність в Україні. Science-community 2013. URL: https: // www. science-community. org / ru / node / 16132. (дата звернення: 30.09.2021).
6.Довгань О. Д., Ткачук Т. Ю. Концептуальні засади законодавчого забезпечення інформаційної безпеки України // Інформація і право. 2019. № 1 (28). С. 86–99.
7.Информационная безопасность: Учебное пособие / Ясенев В. Н., Дорожкин А. В., Сочков А. Л., Ясенев О. В. Нижний Новгород: Нижегородский госуниверситет им. Н. И. Лобачевского, 2017. 198 с.
8.Кримінологічний довідник: довідкове видання / за наук. ред. д-ра юрид. наук, проф., акад. НАПрН України Бандурки О. М.; за заг. ред. д-ра юрид. наук, проф. Джужі О. М. і д-ра юрид. наук, проф. Литвинова О. М. Харків: Золота миля, 2013. 412 с.
9.Махницький О. В. Розповсюдження наркотичних речовин за допомогою месенджерів // Економічна та інформаційна безпека: проблеми та перспективи: матеріали Міжнар. наук. – практ. конф. (м. Дніпро, 27 квіт. 2018 р.). Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. С. 139–141.
10.Статистична інформація про стан злочинності та результати прокурсько-слідчої діяльності. URL: https: // www. gp. gov. ua / ua / statinfo. html. (дата звернення: 30.09.2021).
11.Хоменко В. М., Савченко В. О. Косиченко О. О. Проблеми латентності кіберзлочинності // Використання сучасних інформаційних технологій в діяльності національної поліції України: матеріали Всеукраїнського науково-практичного семінару (23 листопада 2018 р., м. Дніпро). Дніпро: Дніпропетровський державний університет внутрішніх справ, 2018. С. 136–141.
12.Шраго А. Міжнародний досвід протидії обігу порнографічних предметів мережею інтернет та його використання в діяльності оперативних та слідчих підрозділів національної поліції України // Knowledge, Education, Law, Management. 2020. № 3 (31), vol. 2. С. 276–282.