УДК 343.85
DOI https://doi.org/10.24144/2307-3322.2022.75.2.13

ЗАПОБІГАННЯ ЗЛОЧИННОСТІ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

Бодунова О.М.,
кандидат юридичних наук, доцент,
завідувач кафедри правничої лінгвістики
Державного податкового університету,
https://orcid.org/0000-0001-9179-5985

Бодунова О.М. Запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану в Україні.

У статті розглянуто напрями запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану. Зазначено, що в процесі науково-технічного прогресу та активного впровадження інтернет-технологій у всі сфери життєдіяльності суспільства, розвивається й злочинність.

Особливо це питання є актуальним сьогодні в Україні, адже в умовах воєнного стану кіберзлочинців активно залучають до зламу урядових серверів, дезінформування населення, використання при цьому фейкових профілів у соцмережах тощо. Поширеним на сьогодні є кібершахрайство, при якому злочинці під виглядом різноманітних виплат мають намір дізнатися банківські реквізити громадян з метою заволодіння коштами.

Відмічено що, сьогодні війна в інформаційному просторі завдає не меншої шкоди, аніж війна на полі бою. У зв'язку з цим, в Україні вже розпочато процес щодо вдосконалення чинного кримінального та кримінального процесуального законодавства щодо притягнення до відповідальності кіберзлочинців. Так, після повномасштабного вторгнення росії на територію України кількість кримінальних правопорушень у сфені інформаційних технологій різко збільшилась. Країна-агресор використовує інтернет-технології задля дезінформації щодо вторгнення в Україну, пропаганди ворожих ідей тощо. У зв'язку з цим, Верховна Рада України здійснила оптимізацію кримінального та кримінального процесуального законодавства, удосконаливши підстави та процесуальні механізми притягнення до кримінальної відповідальності злочинців.

Визначено, що законодавча база України не містить окремого спеціального акту, який би врегульовував питання запобігання злочинності у сфері інформаційних технологій. Натомість в українському законодавстві є декілька правових актів, які регулюють дане питання.

Зроблено висновок, що задля побудови ефективної системи запобігання злочинності у сфері інформаційних технологій доцільно не лише посилювати відповідальність за вчинені кримінальні правопорушення, а й розробити соціально-економічні, організаційно-управлінські та морально-психологічні напрями, спрямовані на нейтралізацію чинників, що зумовлюють вчинення кримінальних правопорушень.

Ключові слова: кіберзлочинність, кібершахрайство, воєнний стан, злочинність у сфері інформаційних технологій, запобігання

Bodunova O.M. Prevention of crime in the field of information technologies in the conditions of martial law in Ukraine.

The article examines the directions of crime prevention in the field of information technologies in the conditions of martial law. It is noted that in the process of scientific and technical progress and the active introduction of Internet technologies into all areas of society, crime is also developing.

This issue is especially relevant today in Ukraine, because in the conditions of martial law, cybercriminals are actively involved in hacking government servers, disinforming the population, using fake profiles in social networks, etc. Today, cyber fraud is widespread, in which criminals intend to learn bank details of citizens under the guise of various payments in order to take possession of funds.

It is noted that today the war in the information space causes no less damage than the war on the battlefield. In this regard, the process of improving the current criminal and criminal procedural legislation regarding

the prosecution of cybercriminals has already begun in Ukraine. Thus, after the full-scale invasion of Russia on the territory of Ukraine, the number of criminal offenses in the field of information technology increased dramatically. The aggressor country uses Internet technologies for disinformation about the invasion of Ukraine, propaganda of hostile ideas, etc. In this regard, the Verkhovna Rada of Ukraine optimized the criminal and criminal procedural legislation, improving the grounds and procedural mechanisms for bringing criminals to criminal responsibility.

It was determined that the legislative framework of Ukraine does not contain a separate special act that would regulate the issue of crime prevention in the field of information technologies. Instead, there are several legal acts in Ukrainian legislation that regulate this issue.

It was concluded that in order to build an effective system of crime prevention in the field of information technology, it is advisable not only to strengthen responsibility for committed criminal offenses, but also to develop socio-economic, organizational-management and moral-psychological directions aimed at neutralizing the factors that lead to the commission of criminal offenses .

Key words: cybercrime, cyberfraud, martial law, crime in the field of information technologies, prevention

Постановка проблеми. Сьогодні майже кожна особа використовує інтернет-технології в повсякденному житті, державні органи і приватні підприємства вводять електронний документообіг, банківські установи функціонують за допомогою автоматизованих електронних систем, залізничне сполучення теж неможливе без електронних засобів зв'язку. Інтернет-комунікації значно полегшують повсякденне життя кожної людини, покращують роботу державних органів, органів місцевого самоврядування, підприємств, установ, організацій.

Проте в процесі науково-технічного прогресу та активного впровадження інтернет-технологій у всі сфери життєдіяльності суспільства, розвивається й злочинність. Відповідно до офіційної статистики Офісу Генерального прокурора, лише за останні 8 років кількість виявлених кіберзлочинів збільшилась майже у 8 разів [1]. При цьому у статистиці не враховано використання інформаційних технологій як способу вчинення традиційних кримінальних правопорушень, хоча частка таких на сьогодні є надзвичайно великою. Все це свідчить про необхідність вивчення, узагальнення і розробки новітніх напрямів запобігання таким кримінальним правопорушенням.

Особливо це питання є актуальним сьогодні в Україні, адже в умовах воєнного стану кіберзлочинців активно залучають до зламу урядових серверів, дезінформування населення, використання при цьому фейкових профілів у соцмережах тощо. Поширеним на сьогодні є кібершахрайство, при якому злочинці під виглядом різноманітних виплат мають намір дізнатися банківські реквізити громадян з метою заволодіння коштами.

Отже, сьогодні війна в інформаційному просторі завдає не меншої шкоди, аніж війна на полі бою. У зв'язку з цим, в Україні вже розпочато процес щодо вдосконалення чинного кримінального та кримінального процесуального законодавства щодо притягнення до відповідальності кіберзлочинців. Все це свідчить про актуальність обраної тематики та необхідність дослідження чинного законодавства, судово-слідчої практики та наукових джерел з цього питання.

Стан опрацювання цієї проблематики. Питання боротьби з кіберзлочинністю розглядалися багатьма науковцями. Зазначеним питанням приділяли увагу такі дослідники як О.М. Бандурка, В.В. Василевич, В.В. Голіна, Б.М. Головкін, А.П. Закалюк, О.М. Литвинов, В.В. Марков, М.І. Сащенко, В.І. Трапезніков, В.О. Туляков, І.В. Жук, Я.В. Левківська та інші. Проте проблема запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану є такою, що не знайшла достатнього наукового аналізу та вивчення.

Метою наукової статті є аналіз та вивчення законодавчих джерел та практики його застосування щодо боротьби зі злочинністю у сфері інформаційних технологій в умовах воєнного стану в Україні.

Виклад основного матеріалу. Слід розпочати з того, що законодавча база України не містить окремого спеціального акту, який би врегульовував питання запобігання злочинності у сфері інформаційних технологій. Натомість в українському законодавстві є декілька правових актів, які регулюють дане питання.

Одним із основних правових джерел щодо запобігання злочинності у сфері інформаційних технологій є Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року». Відповідно до цього нормативно-правового акту, кіберзлочин (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність (ККУ) та/або яке визнано злочином

міжнародними договорами України. Мета таких дій – розкрадання або руйнування інформації в інформаційних системах і мережах [2]. В умовах війни кіберзлочини можуть здійснюватися з метою дестабілізації ситуації в країні, крадіжки необхідних (конфіденційних) даних, виведення з ладу державних інституцій, техніки, завдання іншої матеріальної шкоди.

Ці положення деталізовані у Стартегії кібербезпеки України, яка введена в дію Указом Президента України № 446/2021.

У Кримінальному кодексі України кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку визначені в Розділі 16 [3]. Деякі норми щодо превенції містяться в Конституції України, в Кримінальному процесуальному кодексі України, проте вони є більш декларативними і потребують подальшого опрацювання та вдосконалення. По-друге, оскільки кіберзлочинність зазвичай має міжнародний характер і може вчинюватися особами різних національностей і з території різних держав, дуже важливого значення набуває міжнародне співробітництво. Європейським Союзом, крім раніше названих, прийняті інші акти, що регулюють питання боротьби з кіберзлочинністю – Директива про боротьбу із сексуальною експлуатацією дітей в Інтернеті та дитячою порнографією (2011 рік), Пропозиція про тимчасове регулювання обробки персональних та інших даних з метою боротьби із сексуальним насильством над дітьми (2020 рік) та інші. Крім того, з метою об'єднання європейської експертизи в галузі кіберзлочинності для підтримки розслідувань з питань кіберзлочинності Європолом був створений ключовий орган боротьби з кіберзло чинністю в ЄС – Європейський центр з кіберзлочинності. Незважаючи на те, що Україною було ратифіковано низку міжнародних договорів, що гарантують співробітництво у боротьбі з кіберзлочинністю, на практиці – взаємодія з іншими країнами тягне за собою велику кількість бюрократичних процедур, які значно уповільнюють процес запобігання кіберзлочинам [4, с. 18].

Після повномасштабного вторгнення росії на територію України кількість кримінальних правопорушень у сфені інформаційних технологій різко збільшилась. Країна-агресор використовує інтернет-технології задля дезінформації щодо вторгнення в Україну, пропаганди ворожих ідей тощо. У зв'язку з цим, Верховна Рада України здійснила оптимізацію кримінального та кримінального процесуального законодавства, удосконаливши підстави та процесуальні механізми притягнення до кримінальної відповідальності злочинців.

Так, було внесено зміни до відповідних законів: «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» з питання підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» № 2137-IX від 15 березня 2022 року та «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» «2149-IX від 24 березня 2022 року [5; 6].

Відповідні зміни стосувались посилення кримінальної відповідальності за кримінальні правопорушення у сфері інформаційних технологій та розширення меж правоохоронних органів щодо виявлення таких кримінально протиправних діянь.

Справді, враховуючи показники діяльності правоохоронних органів після внесення відповідних змін до законодавства, прослідковується підвищення ефективності боротьби зі злочинністю у сфері інформаційних технологій за допомогою якраз посилення відповідальності за наведені кримінальні правопорушення. Проте залишається недослідженим питання щодо вивчення соціальних, економічних, політичних, демографічних, організаційних та інших причин кібершахрайства, адже на сьогодні для формування системи запобігання злочинності у сфері інформаційних технологій використовуються лише результати судово-слідчої практики.

Необхідність у посиленні кримінальної відповідальності за кримінальні правопорушення у сфері інформаційних технологій назріла давно. Зміни до законодавства стосуються збільшення повноважень правоохоронних органів щодо розслідування кіберзлочинів, передбачених статями 361, 361-1 КК України. Посилення санкцій та додаткова криміналізація окремих діянь здатні частково стримати потенційних злочинців від вчинення нових кримінальних проавопорушень.

Важливим, на нашу думку, є запровадження відповідальності за вищевказані кримінальні правопорушення, вчинені під час воєнного стану. Суворі санкції за такі протиправні діяння зумовлена ситуацією в країні, адже особа, яка завдає шкоди національним інтересам України у кіберпросторі, тим самим допомагаючи агресору у цій війні, не може нести відповідальності меншої, ніж військові злочинці.

Варто зазначити, що сфера використання інтернет-технологій давно потребувала більшого захисту. Вторгнення росії стимулювало вдосконалення чинного законодавства та гарантій безпеки у сучасному інформаційному середовищі.

Адже від початку війни стало відомо про велику кількість кібератак на Україну. Так, сучасним в Україні видом кібершахрайства є пенсійні афери, або ж допомога пенсіонерам від держави, соціальні виплати та допомога від європейських організацій. Ці шахрайства пов'язані зі злочинцями, які пропонують людям помилкові фінансові можливості, обіцяють багато коштів і гарантовані високі допомоги від фондів. У соціальній мережі Facebook активізувалися шахраї, які спекулюють на темі грошових виплат українцям, про це повідомляє Державна служба спеціального зв'язку та захисту: «Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, яка діє при Держспецзв'язку, попереджає про зростання кількості шахрайських сторінок у соціальній мережі Facebook. Зловмисники використовують тематику грошових компенсацій, фінансової допомоги від ООН, Європейського суду з прав людини, Товариства Червоного Хреста тощо» [7].

Зокрема, шахраї обіцяють виплати «за рахунок конфіскованих активів рф», посилаються на нечинні рішення різних органів влади України. Повідомляється, що в оголошеннях пропонують перейти за посиланням, яке веде на фішингову сторінку так званого «Єдиного Компенсаційного Центру повернення невиплачених грошових коштів». На цьому сайті користувачам пропонують отримати виплату за умови надання персональної інформації та здійснення додаткового платежу. В результаті дані банківської картки будуть скомпрометовані [7].

Варто зазначити, що таких злочинних схем в Україні наразі багато. Боротьба з таким видом злочинності на сьогодні ускладнюється через використання інтернет-ресурсів, через що важко відслідкувати кібершахраїв. Окрім цього, кібершахрайство виходить на міжнародний рівень, що також ускладнює виявлення та запобігання злочинності вказаного виду. А це – лише один із видів кримінальних правопорушень у сфері інформаційних технологій.

Висновки. Ми вважаємо, що задля побудови ефективної системи запобігання злочинності у сфері інформаційних технологій доцільно не лише посилювати відповідальність за вчинені кримінальні правопорушення, а й розробити соціально-економічні, організаційно-управлінські та морально-психологічні напрями, спрямовані на нейтралізацію чинників, що зумовлюють вчинення кримінальних правопорушень.

Погоджуємося з думкою вчених про доцільність розробки заходів запобігання кібершахрайству, які може реалізувати кожен орган державної влади, місцевого самоврядування, приватні підприємства або ж окремі особи. До таких віднесено:

1) до діяльності органів державної влади, приватних підприємств обов'язково залучати технічного спеціаліста або спеціалізованої компанії, що суттєво підвищить рівень кібербезпеки. Професіонали здатні ускладнити роботу ворогу через запровадження в компанії необхідних алгоритмів захисту, в тому числі організаційних. Варто відповідно проінструктувати працівників, які залучені до роботи із відповідними системами та мережами, адже багато атак досягають цілі лише через непродумані й необережні дії працівників.

2) особам, які перебувають в зоні кіберризику, варто слідкувати за відповідними повідомленнями на офіційних ресурсах Держспецзв'язку та CERT-UA, иадже органи публікують офіційні попередження не лише про можливі кіберзагрози, а й про те, як мінімізувати ризики [8].

3) якщо особа стала жертвою кібератаки, потрібно повідомити про це тих, на кого така атака може поширитися - інші співробітники, клієнти та контрагенти або ж родичі чи друзі.

4) у разі кібератаки потрібно обов'язково інформувати офіційні суб'єкти забезпечення кібербезпеки України, CERT-UA та кіберполіцію. Це дозволить не лише притягти до відповідальності винних, а й вжити невідкладних заходів з блокування та нейтралізації шкідливих вебресурсів.

Список використаних джерел:

1. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування: офіційний сайт Офісу Генерального прокурора. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.
2. Про основні засади забезпечення кібербезпеки України: закон України від 5 жовтня 2017 року 2163-VIII https://zakon.rada.gov.ua/laws/show/2163-19.
3. Кримінальний кодекс України: Закон України від 05.04.2001 No 2341-III / Верховна Рада Украї-

ни. URL: https://zakon.rada.gov.ua/go/2341-14 (дата звернення: 05.01.2023).
4. Сащенко М.І. Проблемні аспекти запобігання кіберзлочинності в Україні. *«Young Scientist»*. 2022. No 1 (101). С. 17–20.
5. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану від 24.02.2022 No 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text (дата звернення: 20.11.2022).
6. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24 берез. 2022 No 2149-IX: URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text (дата звернення: 20.11.2022).
7. Стережіться «виплат»: ПриватБанк попереджає про нову схему шахрайства. *УНІАН*. URL: https://www.unian.ua/economics/finance/shahraystvo-z-bankivskimi-kartkami-privatbank-poperedzhaye-pro-novu-shemu-mahinaciy-novini-ukrajina-11895471.html.
8. Ярема М., Борисенко А. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix.