DOI: https://doi.org/10.33994/kndise.2020.65.27
УДК 343.346

Михайло Олександрович Думчиков
кандидат юридичних наук,
асистент кафедри
кримінально-правових дисциплін та судочинства

E-mail: Misha.dumchikov23@gmail.com

Володимир Васильович Пахомов
доктор юридичних наук, професор,
завідувач кафедри
кримінально-правових дисциплін та судочинства

E-mail: v.pakhomov @yur.sumdu.edu.ua

Ольга Сергіївна Бондаренко
кандидат юридичних наук,
старший викладач кафедри
кримінально-правових дисциплін та судочинства

E-mail: o.bondarenko@yur.sumdu.edu.ua

Навчально-науковий інститут права
Сумський державний Університет

КРИМІНАЛІСТИЧНІ ПРОБЛЕМНІ АСПЕКТИ БОРОТЬБИ ЗІ ЗЛОЧИНАМИ В КІБЕРСФЕРІ

У статті досліджується головні криміналістичні проблеми щодо боротьби з кіберзлочинністю, як нової загрози сучасному суспільству. Наведена статистика скоєння кіберзлочинів й актуальність даної проблеми для України та інших країн світу. Розглядаються проблеми застосування поняття комп'ютерного злочину і необхідності внесення змін в правову базу.

Ключові слова: *кіберзлочинність, кіберзлочини, кіберпростір, комп'ютерний злочин, мережа Інтернет, кібербезпека.*

Сьогодні в результаті швидкого розвитку комп’ютерних технологій і активного розширення їх застосування в різних сферах життя людство увійшло в нову еру інформатизації, коли комп’ютер є необхідним інструментом в різноманітних сферах діяльності людини. Ми можемо, наприклад, елементарно спілкуватися або здійснювати багатомільйонні грошові операції з людьми з іншого боку планети та робити це швидко та з мінімальними витратами. Постійне збільшення кількості персональних комп’ютерів, вільний доступ до мережі Інтернет та динамічний розвиток

ринку нових комунікаційних пристроїв змінили як способи проведення дозвілля, так і методи ведення бізнесу.

Проте доступність глобальних цифрових технологій відкрила нові можливості й злочинного співтовариства. Щодня злочинці, які володіють достатніми комп'ютерними знаннями та навичками, незаконно отримують величезні кошти. Разом з цим, глобальні комп'ютерні мережі також використовуються з метою розпалювання національної ворожнечі, сприяють посиленню екстремізму, сепаратизму, досить часто застосовуються для координації та здійснення терористичних актів. На превеликий жаль, у багатьох випадках правоохоронні органи відстають від злочинців, у результаті нестачі як технічних засобів, так і, що особливо важливо, кваліфікованого персоналу для відображення нової і швидкозростаючої загрози кіберзлочинності.

Метою статті є визначення основ розвитку злочинності у кіберпросторі та криміналістичних проблемних аспектів щодо боротьби з кіберзлочинами, а також головних проблем, які заважають оперативно запобігати та протидіяти подібним видам злочинів.

Поняття «кіберзлочини» і «кіберпростір» в даний час використовуються досить широко, у зв'язку з тим, що XXI ст. вважається століттям інформаційних технологій, які стали невід'ємною частиною всіх сфер життєдіяльності людини. Згідно з даними Звіту ООН по «Стану широкосмугового зв'язку» за 2015 року, в даний час доступ в Інтернет мають близько 4 млрд. осіб, що становить близько 60 % всього світового населення. Сфера застосування мережі Інтернет є багатогранною – це пошук і обмін інформацією, пошук людей і нових знайомих для спілкування, розваги, місце проведення валютних операцій, ведення бізнесу та роботи тощо [4].

У міру зростання Інтернет-користувачів, зростає і кількість осіб, якими досить легко маніпулювати, які нездатні відмовитися від «привабливих пропозицій» злочинців. Такі дії використовуються будь-де: веб-сайти, електронна пошта, платіжна система, соцмережі тощо.

У вітчизняних і зарубіжних наукових працях злочини, що здійснюються в кіберпросторі називаються по-різному: комп'ютерні злочини, злочини у сфері безпеки поводження з комп'ютерною інформацією, злочини в сфері інформаційних технологій, інформаційні злочини, кіберзлочини, злочини у сфері комп'ютерної інформації тощо.

Українське законодавство має поняття кіберзлочинності, у відповідності до Закону України «Про основні засади забезпечення кібербезпеки України» [3], проте у Кримінальному кодексі України такого поняття не існує, при цьому наявний розділ, що передбачає кримінальну відповідальність за відповідні суспільно небезпечні діяння:

– Розділ 16. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку [6].

Кіберзлочинність по своїй семантиці і по суті набагато ширше поняття «комп'ютерна злочинність» і охоплює цілий спектр протиправних діянь. Останнє дає підставу охарактеризувати кіберзлочини з точки зору

криміналістики і визнати його суспільно небезпечним діянням, що здійснюються в кіберпросторі, і які посягають, з одного боку, на громадську безпеку, власність, права людини, інші охоронювані законом відносини, а з іншого – необхідним елементом механізму підготовки, здійснення і приховування злочину, відображенням якого є комп'ютерна інформація, яка виступає в ролі предмета або засобу злочину.

Основна проблема українського законодавства у сфері інформаційних технологій не в тому, що воно слабо розвинена, а в тому, що вона розвивається повільно.

Міжнародна спільнота визначила класифікацію кіберзлочинів в залежності від об'єкта, предмета посягання та від способів скоєння, яка ґрунтується відповідно до Конвенції Ради Європи про кіберзлочинність [5], що поділяє їх на 5 груп:

1) злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему;

2) злочини, які пов'язані з використанням комп'ютера як засобу скоєння злочинів (комп'ютерне шахрайство та комп'ютерна підробка);

3) злочини, пов'язані з утриманням даних, розміщених в комп'ютерних мережах;

4) злочини, пов'язані з порушенням авторського права і суміжних прав;

5) злочини, пов'язані з актами расизму і ксенофобії, вчинені за допомогою комп'ютерних мереж.

Це дозволяє більш ефективно регулювати дану сферу, тому виникає необхідність у кодифікації міжнародно-правових актів, задля створення необхідної правової бази щодо контролю даної сфери.

Відсутність такого регулювання, а також відповідної діяльності правоохоронних органів призводить до виникнення все більше нових видів кіберзлочинності. Беручи до уваги статистичні дані Генеральної прокуратури України за 2019 рік було виявлено 6264 злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, але при цьому тільки 660 проваджень було закрито, у тому числі 531 за ч. 1 п. п. 1, 2, 4, 6 ст. 284 КПК України [2].

До недавнього часу дослідженню феномена кіберзлочинності і наслідків його поширення в світі не приділялося особливої уваги. У багатьох випадках у співробітників правоохоронних органів не було інструментів, необхідних для вирішення цієї проблеми. Старі закони недостатньо відповідали сучасному стану таких злочинів, а нові не могли вирішити такі проблеми, у зв'язку з прискореним науково-технічним прогресом. І, нарешті, однією з найважливіших проблем була відсутність ефективної взаємодії між двома найбільш важливими учасниками процесу боротьби з кіберзлочинністю – співробітниками правоохоронних органів і IT-професіоналами. Однак в останні роки ситуація почала змінюватися в кращий бік. Наприклад, у 2013 р.в Гаазі відкрився Європейський центр по боротьбі з кіберзлочинністю [1]. На сьогоднішній день існують ще дві великі міжнародні організації, які активно працюють в цьому напрямку – підрозділ

по боротьбі з тероризмом (Action Against Terrorism Unit) ОБСЄ, а також Інтерпол, який має у своїй структурі відділення по боротьбі з кіберзлочинністю.

У багатьох країнах зараз вже створені особливі групи реагування на комп'ютерні інциденти (Computer Emergency Response Teams) і прийняті спеціальні закони щодо протидії кіберзлочинності. Однак, очевидно, що в наші дні завдання по боротьбі з кіберзлочинністю не можуть ефективно вирішуватися будь-якої окремою організацією. Злочини такого роду мають практично необмежену сферу дії, а їх жертвами можуть стати користувачі в будь-якій частині світу, а органи попередження та протидії таким загрозам мають досить обмежену юрисдикцію і не можуть самостійно проводити розслідування на території інших держав. Тому організація ефективної співпраці на міжнародному рівні є важливо необхідною.

Як приклад, можна навести взаємодію «Лабораторії Касперського» з Інтерполом і міжнародною організацією багатостороннього співробітництва проти кіберзагроз, яка є підрозділом Міжнародного союзу електрозв'язку ООН. Перша надає найбільш актуальні технічні дані про широко поширені або небезпечні шкідливі програми, які за сприяння міжнародних організацій можуть бути використані в ході поточних розслідувань або для порушення нових справ [8].

Тому правоохоронні органи повинні заручатися підтримкою спеціалістів із різних сфер діяльності, оскільки це є вкрай важливим в умовах глобальної комп'ютеризації суспільства, що створює нові види кіберзагроз.

Ще одним прикладом існуючого взаємодії правоохоронних органів і IT-компаній може служити відкритий корпорацією Microsoft Центр по боротьбі зі світовою кіберзлочинністю. Його робота спрямована на протидію комп'ютерним злочинам, поширенню шкідливих програм, порушення прав інтелектуальної власності тощо.

Розміри збитку, що заподіюється кіберзлочинами, збільшується з кожним днем, доходи від подібного тіньового бізнесу в мережі «Інтернет» можуть зрівнятися з прибутком від незаконної торгівлі наркотиками. Щорічні втрати світової економіки від економічних злочинів, що здійснюються в кіберпросторі, становлять близько 500 млрд дол. Тенденція зростання кіберзлочинів є і в Україні, де щодня відбувається розкрадання з систем дистанційно-банківського обслуговування. Більш того, згідно зі статистичними даними Європолу за 2013-2014 рр., більшість хакерів і кіберзлочинців в Європі – це громадяни України і країн СНД. Це відбувається тому, що російські закони, що регулюють питання кіберпростору і злочинних посягань, слабо розроблені [1].

На ефективність протидії кіберзлочинів негативно впливає дуже високий рівень латентності, як економічних злочинів, що здійснюються в кіберпросторі, так і злочинів у сфері комп'ютерної інформації.

Відділення Центру використовують всі технології Microsoft, що дозволяють боротися з глобальними кіберзагрозами в режимі реального часу. Наприклад, технологія SitePrint допоможе відстежити місцезнаходження кіберзлочинців, програма PhotoDNA дозволить захистити дитину від заборонених сайтів в Мережі. У Центрі є окремий

департамент для роботи зі сторонніми партнерами, який дає можливість співробітникам правоохоронних органів і експертам з кібербезпеки з усього світу взаємодіяти з фахівцями Microsoft в режимі реального часу [7].

У боротьбі з кіберзлочинністю на рівні держави досвід приватних компаній, таких як Microsoft, має велике значення – він дозволяє ефективніше захищати громадян від злочинів в інтернеті.

В умовах сьогодення відсутня ідеальна статистика, яка дозволить всебічно проаналізувати дані, що відображають реальний стан злочинів у кіберпросторі, також відсутні надійні методи збору таких даних, тому не можна достовірно стверджувати щодо втрат, які спричинені подібними злочинними діяннями.

Аналіз результатів досліджень, наведений американським Центром стратегічних і міжнародних досліджень та компанією McAfee, показує, що щорічні втрати світової економіки від кіберзлочинів і їх наслідків досягають близько 500 млрд доларів. Необхідно зазначити, що види кіберзлочинності помітно різниться в залежності від характеру і рівня розвитку комп'ютерних технологій, поширення мережі Інтернет, використання веб-ресурсів та сервісів, електронна торгівля, у різних країнах світу. Наприклад, в США 44 % такого роду злочинів становлять крадіжки грошей з електронних рахунків, 16 % – пошкодження програмного забезпечення, стільки ж – викрадення секретної інформації, 12 % – фальсифікація інформації, 10 % – замовлення послуг за чужий рахунок [9, с. 548-589].

Отже, розслідування злочинів, скоєних в кіберпросторі, вимагає, як технічного, так і теоретичного удосконалення. Виникає необхідність обґрунтування єдиного поняття кіберпростору у всьому національному законодавстві, с точки зору криміналістики, що сприятиме поглибленню і розширенню термінології теоретичної бази комп'ютерної криміналістики. А для успішного виявлення, швидкого і повного розслідування цих злочинів необхідні нові підходи, засновані на більш масштабному використанні досягнень науки та техніки. Наведені факти ще раз доводять необхідність забезпечення правоохоронних органів висококваліфікованими спеціалістами в області інформаційних технологій. Комплексна боротьба з цією проблемою також вимагає спільних зусиль держави, громадян, співробітництва з міжнародними організаціями, вітчизняними та іноземними компаніями, які ведуть свою діяльність у кіберсфері.

Перелік посилань

1. *European Cybercrime Centre* URL: https://www.europol.europa.eu/ec3.

2. *Єдиний звіт Генеральної прокуратури України* про кримінальні правопорушення по державі за січень-жовтень 2019 року. URL*:* https://old.gp.gov.ua/ua/stst2011.html?dir_id=113897&libid=100820&c=edit&_c=fo.

References

1. *European Cybercrime Centre*. Retrieved from https://www.europol.europa.eu/ec3. (In English).

2. *The Unified Prosecutor General's Report* on criminal offenses by state for January-October 2019. Retrieved from https://old.gp.gov.ua/en/stst2011.html?dir_id=113897&libid=100820&c= edit & _c = fo. (In Ukrainian).

3. *Про основні засади забезпечення кібербезпеки України:* Закон України. *Відомості Верховної Ради (ВВР).* 2017. № 45. Ст. 403.
URL*:* https://zakon.rada.gov.ua/laws/show/2163-19.

4. Зверянская Л. П. Интернет-зависимость как основная причина развития киберпреступности*. Фундаментальные и прикладные исследования: проблемы и результаты*. 2015. № 17. С. 239–243.

5. Конвенція про кіберзлочинність: від 23.11.2001. URL*:* http://zakon.rada.gov.ua/laws/show/994_575.

6. Кримінальний кодекс України: від 07.03.2018. URL*:* http://zakon3.rada.gov.ua/laws/show/2341-14/page6.

7. Офіційний сайт американського Центра стратегічних та міжнародних досліджень. URL: https://www.csis.org/8.

8. Офіційний сайт «Лабораторії Касперського». URL: www.kaspersky.ru.

9. Развитие российского общества: социально-экономические и правовые исследования*:* моногр. */* под ред. М. А. Винокурова и др. Москва: Наука*,* 2014. 622 с.

3. *On the Fundamental Principles of Cyber Security of Ukraine:* Law of Ukraine*. Bulletin of theVerkhovna Rada of Ukraine (BBR),* 2017, No. 45, Article 403. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19. (In Ukrainian).

4. *Zverianskaia*, *L. P.* (2015). Internet addiction as the main reason for the development of cybercrime*. Fundamental and applied research: problems and results*. No. 17. P. 239–243. (In Russian).

5. *Cybercrime Convention: of 23.11.2001. Ret*rieved from http://zakon.rada.gov.ua/laws/show/994_575. (In Ukrainian).

6. *Criminal Code of Ukraine* dated 07.03.2018. Retrieved from *http://zakon3.rada.gov.ua/laws/show/2341-14/page6.* (In Ukrainian).

7. *Official Website* of the US Center for Strategic and International Studies Retrieved from https://www.csis.org/8. (In English).

8. Kaspersky Lab's official website Retrieved from www.kaspersky.ru. (In Russian).

9. Vinokurova, M. A. (Ed.). (2014). The development of the Russian community*:* socio-economic and legal studies: monograph. Moscow: Nauka. 622 p. (In Russian).

КРИМИНАЛИСТИЧЕСКИЕ ПРОБЛЕМНЫЕ АСПЕКТЫ ПО БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В КИБЕРПРОСТРАНСТВЕ

М. О. Думчиков
В. В. Пахомов
О. С. Бондаренко

В статье исследуется главные криминалистические проблемы по борьбе с киберпреступностью, как новой угрозы современному обществу. Приведена статистика совершения киберпреступлений и актуальность данной проблемы для Украины и других стран мира. Рассматриваются проблемы применения понятия компьютерного преступления и необходимости внесения изменений в правовую базу, а также привлечение помощи международных организаций, компаний и специалистов в сфере информационных технологий. Анализируется стремительное увеличение киберпреступности в условиях современности. Рассматривается толкование понятий, связанных с преступлениями в киберпространстве, как в национальном, так и

международном законодательстве. При рассмотрении проблемы борьбы с киберпреступностью, были проанализированы работы таких ученых как Л. П. Зверянская, М. А. Винокурова, А. П. Киреенко, С. В. Чупрова.

Определены главные проблемы, которые возникают при исследовании подобных преступлений:

– отсутствие согласованной теоретической базы, а как следствие страдает законодательное регулирование;

– отсутствие специалистов в сфере информационных технологий в правоохранительных органах;

Исследуются вопросы по предупреждению и противодействию киберпреступности, и решение указанных проблем. Определены главные меры по борьбе и минимизации существующих проблем, а конкретно:

– техническое и теоретическое совершенствование: необходимость обоснования единого понятия киберпространства, во всём национальном законодательстве, с точки зрения криминалистики, что разрешит законодательно по-новому регулировать эту сферу;

– новые подходы, основанные на более масштабном использовании достижений научно-технического прогресса, которые помогут успешно выявить, расследовать подобные преступления;

– необходимость обеспечения правоохранительных органов высококвалифицированными специалистами в области информационных технологий;

– привлечения международной поддержки, в виде международных организаций, компаний и специалистов.

Ключевые слова: киберпреступность, киберпреступления, киберпространство, компьютерное преступление, сеть Интернет, кибербезопасность.

FORENSIC PROBLEMATIC ASPECTS OF COMBATING CRIMES IN CYBERSPACE

M. Dumchykov
V. Pakhomov
O. Bondarenko

The article deals with the main forensic issues in the fight against cybercrime, as a new threat to modern society. The statistics of cybercrime and the relevance of this problem in Ukraine and other countries of the world are given. The problems of applying the concept of computer crime and the need to amend the legal framework, as well as attracting the help of international organizations, companies and specialists in the field of information technology is examined. It analyzes the rapid increase in cybercrime in modern conditions. The interpretation of concepts related to crimes in cyberspace, both in national and international legislation, is considered. When considering the problem of combating cybercrime, the works of such scientists as L.P. Zverianskaia, M.A. Vinokurova, A.P. Kireenko, S.V. Chuprova.

The main problems that arise in the study of such crimes are identified:

– the lack of an agreed theoretical base, and as a result, legislative regulation suffers;

– lack of specialists in the field of information technology in law enforcement agencies;

The issues of prevention and combating cybercrime, and the solution of these problems are investigated. The main measures to combat and minimize existing problems, namely:

– technical and theoretical improvement: the need to justify a single concept of cyberspace in all national legislation, from the point of view of forensics, which will allow a new legislative regulation of this area;

– new approaches based on a wider use of the achievements of scientific and technological progress that will help to successfully identify and investigate such crimes;

– the need to provide law enforcement with highly qualified specialists in the field of information technology;

– attracting international support in the form of international organizations, companies and specialists.

Keywords: cybercrimes, cyberspace, cybercrime, computer crime, Internet network, cybersecurity.

DOI: https://doi.org/10.33994/kndise.2020.65.28
УДК 343.346

Катерина Дмитрівна Янішевська
кандидат юридичних наук, доцент
старший викладач кафедри
кримінально-правових дисциплін та судочинства

E-mail: mailto:k.yanishevska@yur.sumdu.edu.ua

Навчально-науковий інститут права
Сумський державний Університет

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ НЕНАЛЕЖНОГО ВИКОНАННЯ ПРОФЕСІЙНИХ ОБОВ'ЯЗКІВ МЕДИЧНИМИ ТА ФАРМАЦЕВТИЧНИМИ ПРАЦІВНИКАМИ

Стаття присвячена актуальним питанням та особливостям розслідування неналежного виконання професійних обов'язків медичним або фармацевтичним працівником. Так як останнім часом сфера надання медичної допомоги все більше потерпає від великої кількості злочинних посягань, а результати розслідування та доведення вини суб'єктів злочину потребують більш високої результативності, то було б доречно звернути увагу на проблеми, які сьогодні стоять перед правоохоронними органами щодо розслідування вказаної категорії злочинних посягань. Зазначаються основні пропозиції щодо процесу розслідування неналежного виконання професійних обов'язків медичними працівниками.

Ключові слова: *медична допомога, невиконання професійних обов'язків, неналежне виконання професійних обов'язків, автоматизація ведення обліку медичних послуг, методика розслідування злочинів*