КРИМІНАЛЬНЕ ПРАВО ТА ПРОЦЕС

УДК 343.3

Н. М. Гузела
магістрант Навчально-наукового інституту права,
психології та інноваційної освіти
й Інституту комп'ютерних наук
та інформаційних технологій
Національного університету "Львівська політехніка"

М. В. Гузела
кандидат юридичних наук, доцент,
доцент кафедри кримінального права і процесу
Навчально-наукового інституту права,
психології та інноваційної освіти
Національного університету "Львівська політехніка"

ПРОБЛЕМА ЗАПОБІГАННЯ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ В ІНФОРМАЦІЙНІЙ СФЕРІ

Розглянуто проблему кримінальних правопорушень в інформаційній сфері, зокрема нові способи злочинної діяльності, які названо кіберзлочинністю. З огляду на це, дослідження досвіду вирішення проблеми запобігання кримінальним правопорушенням в інформаційній сфері, насамперед зарубіжного, є сьогодні доволі важливим завданням для вітчизняної правової науки.

На основі дослідження наукових позицій окремих вчених та аналізу чинного законодавства України, міжнародно-правових актів зроблено висновок, що Україні в особі органів, що ведуть боротьбу зі злочинністю, слід гармонізувати вітчизняне законодавство із законодавством Європейського Союзу, упровадити світовий досвід у національну практику, вчасно реагувати на появу нових загроз, спрямованих на доступ до персональних даних, працювати над створенням надійніших форм захисту конфіденційної інформації, а також внести зміни до КК України, посиливши відповідальність за злочини у сфері комп'ютерних та інформаційних технологій.

Ключові слова: кримінальне правопорушення; кримінальне правопорушення в інформаційній сфері; кіберзлочинність.

Н. М. Гузела, М. В. Гузела

ПРОБЛЕМА ПРЕДОТВРАЩЕНИЯ УГОЛОВНЫХ ПРАВОНАРУШЕНИЙ В ИНФОРМАЦИОННОЙ СФЕРЕ

Рассмотрено проблему уголовных правонарушений в информационной сфере, в частности новые способы преступной деятельности, именующейся киберпреступностью. Учитывая это, исследование опыта решения проблемы предотвращения уголовных правонарушений в информационной сфере, прежде всего зарубежного, является сегодня достаточно важной задачей для отечественной правовой науки.

На основе исследования научных позиций отдельных ученых и анализа действующего законодательства Украины, международно-правовых актов сделан вывод, что Украине в лице органов, ведущих борьбу с преступностью, следует гармонизировать отечественное законодательство с законодательством Европейского Союза, привлечь мировой опыт в национальную практику, своевременно реагировать на появление новых угроз, направленных на доступ к персональным данным, работать над созданием более надежных форм защиты конфиденциальной информации, а также

внести изменения в УК Украины в части усиления ответственности за преступления в сфере компьютерных и информационных технологий.

Ключевые слова: уголовное преступление; уголовное правонарушение в информационной сфере; киберпреступность.

N. M. Huzela
Institute of jurisprudence, psychology and innovative education,
Institute of computer science and information technology
Lviv Polytechnic National University
student of magistracy

M. V. Huzela
Institute of jurisprudence, psychology and innovative education
Lviv Polytechnic National University
department of criminal law and procedure
Ph. D., Assoc. Prof

THE PROBLEM OF PREVENTION OF CRIMINAL OFFENSES IN THE INFORMATION SPHERE

The article deals with the problem of criminal offenses in the information sphere, in particular new ways of criminal activity, called cybercrime. Against this background, research, first of all, on foreign experience in solving the problem of preventing criminal offenses in the informational sphere is currently quite a significant task for the national legal science.

Based on the research of the scientific positions of individual scientists and the analysis of the current legislation of Ukraine, international legal acts conclude that Ukraine, in the form of bodies dealing with crime, should harmonize domestic legislation with the legislation of the European Union, integrate world experience in national practice, respond in a timely manner to appearance of new threats aimed at access to personal data, work on creation of more reliable forms of protection of confidential information, as well as to amend the Criminal Code of Ukraine style of increasing responsibility for crimes in the field of computer and information technologies.

Key words: criminal offense; criminal offense in information sphere; cybercrime.

Постановка проблеми. Оскільки ми живемо в епоху становлення кримінального та кримінального процесуального законодавства України, серед основних проблем правової науки сьогодні на одне з чільних місць виходить проблема запобігання кримінальним правопорушенням в інформаційній сфері. Багато науковців сходяться на тому, що вже наприкінці XX ст. у світі розпочався бурхливий науково-технічний розвиток, який отримав назву інформаційної революції, найбільшим досягненням якої стала поява мережі Інтернет. На сучасному етапі розвитку інформаційного суспільства наявністю різноманітних комп'ютерів, інтернет-провайдерів вже нікого не здивуєш. Тому з'явились і нові способи злочинної діяльності, так званої кіберзлочинності. З огляду на це, дослідження досвіду вирішення проблеми запобігання кримінальним правопорушенням в інформаційній сфері, насамперед, зарубіжного, є сьогодні доволі вагомим завданням для вітчизняної правової науки.

Аналіз дослідження проблеми. Враховуючи новизну та специфіку проблематики, дослідженням проблеми запобігання кримінальним правопорушенням в інформаційній сфері займається ціла низка науковців, зокрема, О. С. Бондаренко, Д. А. Рєпін, Н. Міщук, О. Ю. Іванченко та ін.

Мета статті – спираючись на законодавство України та міжнародно-правові акти, вивчити вітчизняний та зарубіжний досвід запобігання кримінальним правопорушенням в інформаційній сфері.

Виклад основного матеріалу. Сьогодні кіберзлочинність зростає, а нормативне регулювання інформаційної сфери в Україні недосконале, що загострює проблему інформаційних злочинів. За даними Генеральної прокуратури України, упродовж 2017 р. в Україні зареєстровано 3178 кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж електрозв'язку та виявлено 168 осіб, які вчинили такі кримінальні правопорушення [11, с. 186]. В Україні діє низка нормативно-правових актів, якими встановлено законодавчі основи протидії кіберзлочинності. Правову основу забезпечення кібербезпеки України становлять Конституція України, Закони України "Про інформацію", "Про державну таємницю", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про основи національної безпеки України", Указ Президента України "Про Національний координаційний центр кібербезпеки", Конвенція про кіберзлочинність та інші нормативно-правові акти. 15 березня 2016 року Указом Президента України затверджено Стратегію кібербезпеки України. Метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Для досягнення цієї мети необхідні: створення національної системи кібербезпеки; посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері; забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимогу щодо захисту якої встановлено законом, а також інформаційної інфраструктури, яка перебуватиме під юрисдикцією України та порушення сталого функціонування якої негативно впливатиме на стан національної безпеки і оборони України (критична інформаційна інфраструктура) [1, 11].

З 5.10.2017 р. набрав чинності Закон України "Про основні засади забезпечення кібербезпеки України". Відповідно до положень цього закону національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

Необхідно зазначити, що основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних сил України, розвідувальні органи, Національний банк України, які виконують в установленому порядку завдання відповідно до Конституції і законів України [2]. Крім цього, відповідно до рішення Ради національної безпеки і оборони України від 27.01.2016 р. "Про Стратегію кібербезпеки України" утворено Національний координаційний центр кібербезпеки, що є робочим органом Ради національної безпеки і оборони України [3].

У нормах загальної частини чинного Кримінального кодексу України встановлена відповідальність за "злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку" [4]. І навіть більше, у вересні 2005 р. Україна ратифікувала Конвенцію про кіберзлочинність з деякими застереженнями і заявами, чим підтвердила необхідність співробітництва між державами для боротьби з кіберзлочинністю і необхідність захисту законних інтересів у ході використання і розвитку інформаційних технологій [5].

В Європі за координації Європолу створено Європейський центр боротьби із кіберзлочинністю, який розпочав свою діяльність з січня 2013 р. в Гаазі (Нідерланди) [6, с. 177].

Для боротьби з кіберзлочинністю в країнах світу створено спеціалізовані підрозділи, які займаються виявленням, розслідуванням кіберзлочинів та збиранням іншої інформації з цього питання на національному рівні. Такі спеціалізовані підрозділи вже створені й діють тривалий час у

США, Канаді, Великобританії, Німеччині, Швеції, Швейцарії, Бельгії, Португалії, Австрії, Польщі та багатьох інших країнах [7, с. 174]. Наприкінці серпня 2018 р. Уряд Німеччини схвалив рішення про створення нової структури з кібербезпеки для посилення захисту країни – Агентства з питань інновацій у сфері кібербезпеки. У створенні відомства Німеччина орієнтується на відповідні державні агентства США та Ізраїлю [8]. В Естонії 1 серпня 2018 р. розпочав роботу підрозділ кіберкомандування, який буде боротися із хакерськими атаками, спрямованими проти країни. Новий підрозділ складається із 300 осіб і повноцінно запрацює у 2023 р. Буде створено близько 60 нових посад, а решта працівників залучено з наявних ресурсів Міноборони [9; 11].

Вважаємо, що цілком слушно О. С. Бондаренко та Д. А. Рєпін визначають чинники, які пов'язані з діяльністю правоохоронних органів й істотно впливають на функціонування та розвиток кіберзлочинності в Україні. Серед таких чинників: недостатнє забезпечення правоохоронних органів спеціальними технічними засобами, що допомагають виявити та розслідувати кіберзлочини; технічна складність відстеження інформаційних загроз; відсутність належної взаємодії правоохоронних органів та приватного бізнесу з питань захисту комп'ютерних мереж, надання необхідної інформації щодо порушень у віртуальному просторі; недосконаліть чинного кримінального та кримінально-процесуального законодавства; слабка скоординованість у боротьбі з кіберзлочинністю, а також відсутність ефективної міжнародної співпраці в цій сфері, що є необхідним складником розкриття таких злочинів [10, с. 247].

Висновки. Зважаючи на те, що персональні дані є конфіденційною інформацією, надання надійного захисту цих даних – це важлива гарантія реалізації прав людини, закріплених у статті 31 та 32 Конституції України. Тому Україні в особі її органів державної влади необхідно гармонізувати вітчизняне законодавство із законодавством Європейського Союзу, упровадити світовий досвід у національну практику, вчасно реагувати на появу нових загроз, спрямованих на доступ до персональних даних, працювати над створенням надійніших форм захисту конфіденційної інформації, а також внести зміни до КК України в частині посилення відповідальності за злочини у сфері комп'ютерних та інформаційних технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Стратегія кібербезпеки України: указ Президента України від 15 березня 2016 року № 96/2016 [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/laws/show/96/2016. 2.Закон України "Про основні засади забезпечення кібербезпеки України" від 5 жовтня 2017 року № 2163-VIII [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/laws/show/2163-19. 3. Положення про Національний координаційний центр кібербезпеки: указ Президента України від 7 червня 2016 року № 242/2016 [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/laws/show/242/2016. 4. Кримінальний кодекс України: Закон України від 5 квітня 2001 р. [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua. 5. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7 вересня 2005 р. № 2824-IV. *Відомості Верховної Ради України*. 2006. № 5–6. Ст. 71. 6. Міщук Н. Кіберзлочинність як загроза інформаційному суспільству. *Вісник Львівського університету*. Серія економічна. 2014. Вип. 51. С. 173–179. 7. Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. *Актуальні проблеми вітчизняної юриспруденції*. 2016. Вип. 3. С. 172–177. 8. Уряд Німеччини схвалив створення нового агентства з кібербезпеки [Електронний ресурс]. Режим доступу: https://www.eurointegration.com.ua/news/2018/09/3/7086389/. 9. Defence Forces cyber command takes up operations [Електронний ресурс]. Режим доступу: https://news.err.ee/850719/defence-forces-cyber-command-takes-up-operations 10. Бондаренко О. С., Рєпін Д. А. Кіберзлочинність в Україні: причини, ознаки та заходи протидії. *Порівняльно-аналітичне право*. 2018. № 1. С. 246–248. 11. Гей К., Ортинський В. Л. Деякі питання запобігання злочинам у інформаційній сфері: український та зарубіжний досвід. Наукове забезпечення захисту прав та свобод громадян України в умовах інтеграції в Європейський простір: матеріали Міжн. конф. (Львів, 25.10.2018 р). Львів: Сполом, 2018. С. 186–189.

REFERENCES

1. ***Stratehiia kiberbezpeky Ukrainy: ukaz Prezydenta Ukrainy vid 15 bereznia 2016 roku No. 96/2016*** [Ukraine's Cybersecurity Strategy: Presidential Decree No. 96/2016 of March 15, 2016][Elektronnyi resurs]: Rezhym dostupu: http://zakon.rada.gov.ua/laws/show/96/2016. 2. ***Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy" vid 5 zhovtnia 2017 roku No. 2163-VIII*** [The Law of Ukraine "On the Fundamental Principles of Cybersecurity of Ukraine" of October 5, 2017 No. 2163-VIII][Elektronnyi resurs]/ Rezhym dostupu: http://zakon.rada.gov.ua/laws/show/2163-19. 3. ***Polozhennia pro Natsionalnyi koordynatsiinyi tsentr kiberbezpeky*** [Regulation on the National Cybersecurity Coordination Center: Presidential Decree No. 242/2016 of June 7, 2016]: ukaz Prezydenta Ukrainy vid 7 chervnia 2016 roku No. 242/2016 [Elektronnyi resurs]. Rezhym dostupu: http://zakon.rada.gov.ua/laws/show/242/2016. 4. ***Kryminalnyi kodeks Ukrainy*** [Criminal Code of Ukraine]: Zakon Ukrainy vid 5 kvitnia 2001 r. [Elektronnyi resurs]. Rezhym dostupu: http://zakon2.rada.gov.ua. 5. ***Pro ratyfikatsiiu Konventsii pro kiberzlochynnist: Zakon Ukrainy vid 7 veresnia 2005 r. No. 2824-IV*** [On ratification of the Convention on Cybercrime: Law of Ukraine of September 7, 2005 No. 2824-IV]. Vidomosti Verkhovnoi Rady Ukrainy. 2006. No. 5–6. P. 71. 6. Mishchuk N. ***Kiberzlochynnist yak zahroza informatsiinomu suspilstvu*** [Cybercrime as a Threat to the Information Society]. Visnyk Lvivskoho universytetu. Seriia ekonomichna. 2014. Vyp. 51. P. 173–179. 7. Ivanchenko O. Yu. ***Kryminolohichna kharakterystyka kiberzlochynnosti, zapobihannia kiberzlochynnosti na natsionalnomu rivni*** [Criminological characteristics of cybercrime, prevention of cybercrime at the national level]. Aktualni problemy vitchyznianoi yurysprudentsii. 2016. Vyp. 3. P. 172–177. 8.***Uriad Nimechchyny skhvalyv stvorennia novoho ahentstva z kiberbezpeky*** [The German Government has approved the creation of a new cybersecurity agency][Elektronnyi resurs]. Rezhym dostupu: https://www.eurointegration.com.ua/news/2018/09/3/7086389/. 9. ***Defence Forces cyber command takes up operations*** [Defence Forces cyber command takes up operations][Elektronnyi resurs]. Rezhym dostupu: https://news.err.ee/850719/defence-forces-cyber-command-takes-up-operations 10. Bondarenko O. S., Riepin D. A. ***Kiberzlochynnist v Ukraini*** [Cybercrime in Ukraine]: prychyny, oznaky ta zakhody protydii. Porivnialno-analitychne pravo. 2018. No. 1. P. 246–248. 11. Hei K., Ortynskyi V. L. ***Deiaki pytannia zapobihannia zlochynam u informatsiinii sferi: ukrainskyi ta zarubizhnyi dosvid*** [Some Issues of Crime Prevention in the Information Sphere: Ukrainian and Foreign Experience]. Naukove zabezpechennia zakhystu prav ta svobod hromadian Ukrainy v umovakh intehratsii v Yevropeiskyi prostir: materialy Mizhn. konf. (Lviv, 25.10.2018 r). Lviv: Spolom, 2018. P. 186–189.

Дата надходження: 04.11.2019 р.