ECLI:CE:ECHR:2016:1004JUD003746209.

5. Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 04.09.1950.

6. Ferdinandusse W.N. Direct application of international criminal law in national courts. Amsterdam Center for International Law, PhD thesis. 2005. P. 225-270.

7. Kempen P.H., and Bemelmans J. EU Protection of the Substantive Criminal Law Principles of Guilt and Ne Bis in Idem under the Charter of Fundamental Rights: Underdevelopment and Overdevelopment in an Incomplete Criminal Justice Framework. New Journal of European Criminal Law. 2018. No 2. P. 247-264.

8. Murphy Cian C. The Principle of Legality in Criminal Law Under the ECHR. European Human Rights Law Review. 2010. P. 1-45.

9. Sanz-Caballero S. The Principle of Nulla Poena Sine Lege Revisited: The Retrospective Application of Criminal Law in the Eyes of the European Court of Human Rights. European Journal of International Law. 2017. No 3. P. 787-817.

УДК 343.9(043.2)

Грекова Л.Ю., асистент,
Колісніченко Л.А., студентка,
Національний авіаційний університет, м. Київ, Україна

МІЖНАРОДНІ ОРГАНІЗАЦІЇ З ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Розповсюдження та використання новітніх технологій як у приватному, так і в державному секторі зумовлює питання, які потребують вирішення проблем інформаційної безпеки та захисту мережі від несанкціонованого доступу до інформації. Прогресивні системи мають свої недоліки, зокрема, незахищеність серверів, де знаходяться бази даних, які можуть бути знищені або модифіковані зловмисниками. Розвиток техніки зумовлює не тільки позитивні зміни в економіці, але й негативні тенденції появи нових форм і видів злочинних посягань. Це проявляється, насамперед, в тому, що за допомогою інформаційних технологій відбувається розповсюдження комп'ютерних вірусів, порнографічних матеріалів, шахрайство з пластиковими картками, розкрадання банківських рахунків тощо.

Злочини у сфері інформаційно-комп'ютерних технологій (ІКТ) з кожним роком набувають все більш глобального масштабу, вони є загрозою для всієї міжнародної інформаційної безпеки. Розвиток та поширення комп'ютерних злочинів, що мають транснаціональний характер, свідчить про те, що окрема держава не може самотужки боротися з даним явищем. Цей факт є причиною створення міжнародної системи організацій та співробітництва країн у боротьбі з кіберзлочинністю.

Починаючи з кінця XX ст. держави почали будувати фундамент міжнародної співпраці та протидіяти кіберзлочинності. Центральне місце серед всіх організацій займає Організація Об'єднаних Націй (ООН) та її спеціалізовані установи. Зокрема, Управління ООН з наркотиків та злочинності (United Nations Office on Drugs and Crime), у рамках якого втілюється Глобальна програма з питань кіберзлочинності (Global Program on Cybercrime) [1], а також проводяться засідання Міжурядової експертної групи з питань кіберзлочинності (Open-ended Intergovernmental Expert Group on Cybercrime) [2]. Основними завданнями Управління, які визначені в програмі, є підвищення ефективності та результативності розкриття кіберзлочинів, посилення міжнародної комунікації, співробітництво національних органів, приватних структур та ознайомлення суспільства щодо небезпеки кіберзлочинності.

Провідну роль у питаннях кібербезпеки займає ще одна спеціалізована установа системи ООН - Міжнародний союз електрозв'язку (International Telecommunication Union – ITU). З 2007 року було розпочато Глобальну програму кібербезпеки ITU (Global Cyber security Agenda – GCA) [3]. Дана програма зазначає основні напрямки роботи Міжнародного союзу електрозв'язку у сфері протидії кіберзлочинності: юридичні заходи, технічні та процедурні заходи, організаційні структури, нарощування потенціалу та міжнародне співробітництво. Крім цього, під керівництвом ITU розробляються регіональні кібернетичні підрозділи ALERT (Applied Learning for Emergency Response Teams) [4], які є своєрідними центрами обміну інформацією та обговорення питань кібербезпеки, а також забезпечують практичні заходи для національних груп з реагування на комп'ютерні інциденти.

Серед глобальних регіональних організацій, які сприяють міжнародному співробітництву держав проти кіберзлочинності слід виокремити Раду Європи (РЄ). Боротьба з високотехнологічною злочинністю як напрям діяльності РЄ здійснюється ще з 1976 р., а в 1995 р. Європейським комітетом з проблем злочинності було створено Комітет по боротьбі з кіберзлочинністю. Разом з ухваленням Конвенції Ради Європи про кіберзлочинність було утворено Комітет з питань Конвенції про кіберзлочинність [5].

В лютому 2013 р. була ухвалена стратегія кібербезпеки Європейського Союзу, метою якої є нарощування потужностей для попередження кіберзагроз, включаючи кіберзлочинність та кібертероризм. В тому ж році Європейським поліцейським управлінням (Європол) був створений Європейський центр боротьби з кіберзлочинністю, головним завданням якого є посилення реакції правоохоронних органів на кіберзлочинність в ЄС і захист європейських громадян, бізнесу та урядів. Щорічно Центр видає Оцінку загрози організованої злочинності в Інтернеті (Internet Organised Crime Threat Assessment) [6], організовує діяльність Об'єднаної

робочої групи з боротьби проти кіберзлочинності (Joint Cybercrime Action Task force). Місія цієї групи полягає в керівництві інтегрованими та узгодженими діями проти основних загроз створюваних кіберзлочинами за допомогою транскордонних розслідувань та операцій з боку своїх партнерів.

Найбільш відома своєю міжнародною співпрацею щодо боротьби зі злочинністю (в тому числі з кіберзлочинами) є Міжнародна організація кримінальної поліції (International Criminal Police Organization – INTERPOL) [7]. Вона не тільки використовує у своїй діяльності різноманітні заходи для підтримки держав-учасниць у боротьбі з кіберзлочинністю, а й надає технічну допомогу, створює спеціальні рекомендації щодо застосування корисного практичного досвіду, та навіть проводить тренування. Підхід Інтерполу до боротьби з кіберзлочинністю полягає в тому, щоб використовувати досвід його членів у боротьбі зі злочинами у сфері інформаційних технологій шляхом функціонування робочих груп або експертних груп. Робочі групи створюються для вивчення регіонального досвіду та існують в Європі, Азії, Африці, Північній і Південній Америці [8].

Серед завдань, що постають перед світовою спільнотою та міжнародними організаціями, діяльність яких направлена на протидію та запобігання кіберзлочинності, найважливішим є необхідність імплементації міжнародних нормативних актів до національного законодавства кожної держави. Крім того, нагальною є потреба з налагодження цілісної мережі спеціальних установ в кожному регіоні з протидії злочинам в інформаційній сфері, вжиття необхідних технічних заходів, нормотворчості у міжнародному законодавстві. Вважаємо за необхідне звернути увагу на побудування дієвої, гнучкої міжнародної співпраці організацій, судів, правоохоронних органів різних країн, створення єдиного простору щодо обміну інформацією, транснаціональних баз даних з правом доступу до них кожної країни, що дозволить позбутися проблеми несанкціонованої кіберзлочинності.

Література

1. Global Programme on Cybercrime. 2020. URL: https://www.unodc.org/ unodc/ en/ cybercrime/global-programme-cybercrime.html

2. Open-ended intergovernmental expert group meeting on cybercrime. 2020. URL: https://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-meeting-on-cybercrime.html

3. Global Cybersecurity Agenda (GCA). 2020. URL: https://www.itu.int/ en/ action/cybersecurity/Pages/gca.aspx

4. ITU ALERT (Applied Learning for Emergency Response Teams). 2020. URL: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2018/ CYBDRILL/ITU-ALERT-Cyber-drill.aspx

5. Конвенція про кіберзлочинність: Конвенція від 23.11.2001. Ратифіковано

із застереженнями і заявами Законом № 2824-IV (2824-15) від 07.09.2005. *Відомості Верховної Ради України*. 2006. № 5-6. Ст. 71.

6. INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2019. 2020. URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

7. INTERPOL: Cybercrime. 2020. URL: https://www.interpol.int/Crimes/Cybercrime

8. Орлов О.В., Онищенко Ю.М. Організаційні та нормативно-правові засади боротьби з кіберзлочинністю. 2020. URL: http://www.dy.nayka.com.ua/?op= 1&z=715

УДК 343.352(043.2)

Лисько Т.Д., к.ю.н.,
Вовканич Д., студентка,
Національний авіаційний університет, м. Київ, Україна

ХАРАКТЕРИСТИКА КОРУПЦІЙНИХ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ СЛУЖБОВОГО СТАНОВИЩА

Протягом кількох десятиріч корупція є однією з головних проблем у світі, адже це правопорушення є суттєвою перепоною розвитку міжнародних економічних зв'язків, загрожує правопорядку, демократії та правам людини, руйнує державне управління.

Україна вже протягом тривалого часу за даними міжнародної організації Transparency International знаходиться в числі країн з високим рівнем корупції. У нашій державі корупція (хабарництво) особливо процвітає у сфері управління державою, тому створює загрозу національній безпеці України та ставить під загрозу політичну стабільність і сталий розвиток країни.

Хабарництво спотворює авторитет державного апарату, породжує уявлення стосовно можливості досягнення бажаного шляхом підкупу службових (посадових) осіб. Для службових (посадових) осіб хабарництво є джерелом додаткового незаконного доходу. В результаті грубо порушуються права і законні інтереси громадян, підриваються гарантії реалізації конституційних прав. Врешті, небезпечність хабарництва полягає і в тому, що воно нерідко поєднується з іншими злочинами, зокрема, з привласненням, розтратою або заволодінням майном через зловживання службовим становищем, владою, службовим підробленням та іншими злочинами у сфері службової діяльності та професійної діяльності, пов'язаної з наданням публічних послуг.

У кримінальному кодексі України поняття «хабар» не застосовується. У ст. 368 КК України «Прийняття пропозиції, обіцянки або одержання *неправомірної вигоди* службовою особою», тобто це злочин у сфері