в мережі Інтернет. Тому напрямами наших наступних наукових розвідок стануть різні аспекти зазначеної теми.

Список використаних джерел:

1. Основные услуги и тарифы на рынке киберпреступности в странах СНГ. URL: http://www.interface.ru.
2. Єдиний звіт про кримінальні правопорушення по державі: офіційний сайт Генеральної прокуратури України URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=104402
3. Комаров А. А. Криминологические аспекты мошенничества в глобальной сети Интернет: дис. на соискание ученой степени канд. юрид. наук: спец. 12. 00. 08. Саратов, 2011. 262 с.

Ключові слова: шахрайство, шахрайство в мережі Інтернет, попередження шахрайства.

Ключевые слова: мошенничество, мошенничество в сети Интернет, предупреждение мошенничества.

Keywords: fraud, Internet fraud, fraud prevention.

***Науковий керівник**: к.ю.н., доцент Дикий О. В.*

Флюнт Мар'яна Орестівна

Національний університет «Одеська юридична академія»,
аспірантка кафедри кримінології та кримінально-виконавчого права

КІБЕРЗЛОЧИН ТА КІБЕРЗЛОЧИННІСТЬ У КРИМІНОЛОГІЧНИХ ДОСЛІДЖЕННЯХ: СУЧАСНІ ПІДХОДИ ТА ПРОБЛЕМАТИКА

Формування актуальної кібербезпекової політики та забезпечення ефективності її реалізації, функціонування безпечного кіберпростору, а також попередження та протидія кіберзлочинності є одними з найбільш актуальних завдань та викликів для держав і міжнародної спільноти на сучасному етапі розвитку суспільства. Саме тому дослідження окремих питань забезпечення кібербезпеки є об'єктом дослідження науковців різних сфер.

У кримінології кібербезпека розглядається як взаємодія окремих складових, – державної політики щодо забезпечення

кібербезпеки; суб'єктів забезпечення кібербезпеки; засобів, способів і методів забезпечення кібербезпеки. Однією з ключових загроз кібербезпеці є, зокрема, кіберзлочинність.

Не зважаючи на те, що кіберзлочини та кіберзлочинність є предметом вивчення все більшої кількості сучасних науковців, існують деякі труднощі дослідження даного соціального явища, що, своєю чергою, уповільнює функціонування системи забезпечення кібербезпеки як на національному, так і на міжнародному рівнях, оскільки остання формується на основі теоретичних досліджень. Розгляньмо деякі проблемні моменти.

По-перше, *відсутній єдиний підхід до термінології у правовій доктрині та роботах вітчизняних та закордонних науковців.* Так, у сучасних дослідженнях активно застосовують поняття «комп'ютерні злочини», «кіберзлочини», «віртуальні злочини», «інформаційні злочини», «цифрові злочини», «високотехнологічні злочини», «злочини, пов'язані з використанням мережі Інтернет», «злочини, пов'язані з використанням телекомунікаційних систем», «електронні злочини» тощо. Зазначені терміни по-різному описуються, тлумачаться один через одного, крім того, то розмежовуються, то ототожнюються різними дослідниками.

Неоднаковим є застосування термінології й у чинному законодавстві. Так, Кримінальний кодекс України (далі – КК України) оперує поняттям «кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», жодного разу не згадуючи поняття «кіберзлочин», а Закон України «Про основні засади забезпечення кібербезпеки» застосовує іншу термінологію, – «кіберзлочин» і «комп'ютерний злочин», фактично ототожнюючи зазначені поняття та визначаючи їх як «…суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України» [1].

Варто зазначити, що термін «кіберзлочин» є найбільш вживаним у побутовому спілкуванні, політиці та публіцистиці, в порівнянні з іншими (суміжними) категоріями. У буденному розумінні, – кіберзлочин це загальне поняття, яке охоплює усі злочини, що вчиняються у мережі інтернет та/або з використанням комп'ютерів та/або сучасних інформаційних комунікаційних технологій. Така неоднозначність у термінології спричиняє плутанину та помилкову взаємопідміну понять, що своїм результатом має отримання помилкових даних, а отже й неревалентність дослідження.

По-друге, *невідповідність чинного законодавства міжнародним стандартам.*

У вересні 2005 року Україною було ратифіковано (із застереженням) Конвенцію Ради Європи про кіберзлочинність (так звану Будапештську конвенцію). Конвенцією сформовано новий міжнародний стандарт – злочин міжнародного характеру – кіберзлочин, що за своєю правовою конструкцією є збірним поняттям, яке включає декілька різнопланових протиправних посягань [2].

Так, у Конвенції перелічено основні види кіберзлочинів, схарактеризовано окремі процесуальні заходи та описано загальні принципи міжнародного співробітництва у сфері протидії кіберзлочинам. Зокрема, Конвенцією передбачено чотири основні групи кіберзлочинів [3]: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, – незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями; правопорушення, пов'язані з комп'ютерами, – підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами; правопорушення, пов'язані зі змістом, – правопорушення, пов'язані з дитячою порнографією; правопорушення, пов'язані з порушенням авторських і суміжних прав.

Зазначені у Конвенції кіберзлочини частково передбачені КК України. Так, розділом XVI КК України встановлено відповідальність за кримінальні правопорушення у сфері викорис-

тання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Крім того, для кваліфікації правопорушень, що фактично є кіберзлочинами, з точки зору норм Конвенції, застосовують також статті з інших розділів Особливої частини КК України: ст. 163 – порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер, ст. 176 – порушення авторського права і суміжних прав, ст. 190 ч. 3 – шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки, ст. 301 – ввезення, виготовлення, збут і розповсюдження порнографічних предметів, ст. 359 – незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації.

Відсутність чіткого визначення у кримінальному законі яке діяння є кіберзлочином; «розпорошеність» у КК України статей, якими встановлено відповідальність за правопорушення, що відповідно до норм Конвенції є кіберзлочинами; невключення ряду правопорушень, що є конвенційними кіберзлочинами до кримінального законодавства України зумовлюють неправильну кваліфікацію та необлікування значної кількості вчинених злочинів. Наслідком зазначеного є латентність, помилковість у статистичних даних, а отже й відсутність оцінки реального стану кіберзлочинності у нашій державі.

Необхідність чіткого нормативного визначення та доповнення кримінального закону нормами, що встановлюють відповідальність за конвенційні злочини зумовлена й тим, що кримінальне право є фундаментальною наукою щодо кримінології (як науки кримінального циклу), а остання, будучи теоретико-прикладною наукою одним зі своїх основних предметів дослідження має злочини. Таким чином, некоректним є йменування у кримінологічних дослідженнях «злочином» діянь, що не є криміналізованими, тобто таких, що не є злочином з точки зору закону про кримінальну відповідальність, адже аналогія у цій галузі не застосовується.

По-третє, *обмеженість кримінологічних досліджень способів вчинення кіберзлочинів.*

Формування державної політики та розробка ефективної системи заходів протидії злочинам передбачає попереднє вивчення способів їх вчинення. У кримінології способам вчинення злочинів приділено недостатньо уваги, – зазвичай спосіб розглядається поверхнево та фрагментарно, а їх опис базується на основі статистичних даних (у розрізі звітності Офісу генерального прокурора України, – Форма № 1). Такими ж поверхневими є переважна більшість наявних робіт щодо способів вчинення кіберзлочинів, – дослідження, здійснені на основі вивчення матеріалів слідчої та судової практики є швидше винятком, а не закономірністю. Таким чином, неналежне вивчення злочинів, вчинених у кіберпросторі, зумовлює існування певних кліше щодо сучасної кіберзлочинності, не дозволяє виявити основні тенденції даного виду злочинності та спрогнозувати її подальший розвиток.

Окрім зазначених, проблематичним у дослідженні кіберзлочинності вважаємо: обмеженість методів вивчення кіберзлочинності; незначне врахування результатів досліджень закордонних фахівців та міжнародних наукових спільнот; застарілість та поверхневість наявних досліджень; мала кількість судової практики щодо кримінальних справ даної категорії (у співвідношенні до кількості зареєстрованих та облікованих злочинів, визначених, зокрема, Розділом XVI КК України).

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05 жовтня 2017. URL: https://zakon.rada.gov.ua/laws/show/2163–19#Text

2. Гринчак І. В. Кіберзлочинність як злочин міжнародного характеру. URL: http://nbuv.gov.ua/j-pdf/Nivif_2015_12_15.pdf

3. Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

Ключові слова: кіберзлочинність, міжнародний стандарт, криміналізація, спосіб вчинення кіберзлочинів, політика кібербезпеки.
Ключевые слова: киберпреступность, международный стандарт, криминализация, способ совершения киберпреступлений, политика кибербезопастности.
Keywords: cybercrime, international standard, criminalization, method of committing cybercrimes, cybersecurity policy.

***Науковий керівник**: к.ю.н., доцент Дикий О. В.*

Керусов Максим Вікторович
Національний університет «Одеська юридична академія»,
студент 4-го курсу факультету кібербезпеки
та інформаційних технологій

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНТЕРНЕТ ПРОВАЙДЕРІВ

Термін інформаційна безпека в сучасному світі надзвичайно широкий. Вон включає в себе як контроль за непоширенням інформації, яка вважається секретною, так і облік своєчасного, повного і якісного інформування громадян про події в країні і світі, вільний доступ до різних джерел інформації – і в той же час просування цілісності суспільства, підтримання його морального благополуччя, захист від різноманітних несприятливих інформаційних впливів.

Актуальність порушення проблеми захисту інформаційної безпеки обумовлюється зростанням доступу до мереж загального користування окремих категорій негативно настроєних осіб, певною уразливістю окремих мереж, збільшенням спроб злочинних елементів на здобування або руйнування інформації, а також збільшення кількості шахраїв які намагаються вкрасти персональні данні.

Політика інформаційної безпеки являє собою набір обмежень, вимог, рекомендацій, правил, які регламентують порядок інформаційної діяльності в організації і направлені на досягнення і підтримку стану інформаційної безпеки в організації.