передбачає адміністративну відповідальність за гендерно-обумовлене насильство;

– метою юрисдикційної діяльності Національної поліції щодо протидії гендерно-обумовленому насильству є притягнення винного суб'єкта до відповідальності, захист та відновлення прав потерпілої особи від наслідків гендерно-обумовленого насильства, попередження подальших фактів вчинення гендерно-обумовлених насильств, відновлення належного стану правопорядку.

Література:

1. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X. Відомості Верховної Ради Української РСР. 1984. додаток до № 51. Ст. 1122.

2. Комісаров С. А. Особливості адміністративно-юрисдикційної діяльності Національної поліції України. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Юридичні науки. 2018. Т. 29(68), № 2. С. 73-77.

3. Константінов С.Ф., Братель С.Г., Басс В. О. та інші. Адміністративно-юрисдикційна діяльність поліції: навчальний посібник. Київ: «Центр учбової літератури». 2016. 336 с.

4. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII. Відомості Верховної Ради. 2015. № 40-41. Ст. 379.

ТЕНДЕНЦІЇ РОЗВИТКУ ТА ЗАХОДИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Левчишин О. О.
студент 4-го курсу
юридичного факультету
Міжнародного економіко-гуманітарного університету
імені академіка Степана Дем'янчука
м. Рівне, Україна

В умовах сучасного етапу розвитку України особливої уваги потребує система кібернетичної безпеки як ключовий елемент інформаційної, а відтак, і національної безпеки. Всебічне розповсюдження комп'ютерних технологій і комп'ютерної техніки, повсюдне проникнення телекомунікаційних мереж майже в усі сфери життєдіяльності людини одночасно і полегшило (створення та

накопичення баз даних, автоматична обробка інформації, можливість миттєвого передання інформації на дуже великі відстані тощо), але й ускладнило управління, виконання виробничих процесів та особисту комунікацію. Перевагою нових ІТ– технологій є можливість удосконалення функціонування багатьох сфер життєдіяльності, таких як оборона, енергетика, транспорт. Однак в поєднанні із перевагами такої комп'ютеризації виникає ряд негативних, часом незворотніх наслідків, одним з яких є кіберзлочинність, яка своєю діяльністю перешкоджає нормальному розвитку інфраструктури держави та діяльності не тільки людей, але й підприємств, установ, організацій у сфері надання публічних послуг.

На науково-теоретичному, методичному та практичному рівнях вивченням даного питання займалися такі науковці як Д. С. Азарова, Ю. М. Батуріна, П. Д. Біленчука, В. М. Бутузова, В. Б. Вєхова, В. О. Голубєва, О. Ю. Іванченко, М. В. Карчевського, Н. В. Коваленко, А. А. Музики, С. О. Орлова, Д. В. Пашнєва, В. С. Цимбалюка, В. П. Шеломенцева та ін.

Перед тим як перейти до розгляду питання опису статистичних показників та характеристики кіберзлочинності доцільно зазначити, що з приводу визначення поняття й ознак кіберзлочинів і кіберзлочинності в науці кримінального права та кримінології досі триває дискусія, адже на національному рівні це поняття не має нормативного врегулювання (на рівні законодавчого його визначення), проте цим терміном оперує Конвенція про кіберзлочинність (2001 р.) [1].

На думку В.М. Болгова, кіберзлочини – це сукупність передбачених чинним законодавством кримінально караних, суспільно небезпечних діянь (дій чи бездіяльності), що посягають на право захисту від несанкціонованого поширення і використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію [2].

Згідно з Доктриною інформаційної безпеки України, інформаційна безпека визначена невід'ємною складовою національної безпеки і, в той же час, важливою її самостійною сферою, а відповідно до ст. 17 Конституції України вона детермінується як одна із головних функцій держави [3]. На сьогоднішній день активно відбуваються процеси розробки нормативно-правового забезпечення, яке визначає правове підґрунтя державної діяльності у даній сфері.

Відповідно до даних Генеральної прокуратури України щодо рівня вчинення кіберзлочинів за 2015–2018 рр. на території України, станом на грудень 2015 р. органами досудового розслідування зареєстровано

вчинення 523 злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку предбаченими ст. 361, 362 ККУ станом на грудень 2016 р. – 768 злочинів, станом на грудень 2017 р. – 911 злочинів, станом на березень 2018 р. – 1867 злочинів; хочеться підкреслити, що рівень вчинення даного виду злочину станом на березень 2018 р. виріс майже втричі порівняно з 2015 р. Статистичний аналіз географічної поширеності кіберзлочинів в Україні за останні роки виявив залежність від фактору урбанізації. Відповідні географічні особливості вчинення кіберзлочинів в Україні слід розглядати не стільки через призму переважання на мапі кіберзлочинів східних областей порівняно із західними, скільки через призму переважання промислово та фінансово розвинутих областей (центрів).

Спеціалісти Національного інституту стратегічних досліджень при Президентові України у своїй аналітичній доповіді на тему «Кібербезпека: світові тенденції та виклики для України» виділяють три основні, тісно пов'язані проблеми, що ускладнюють боротьбу проти злочинів у кіберсфері: 1) відсутність сформованих визначень ключових понять і термінів: «кібербезпека», «кіберпростір», «кібератака», «кіберзахист», «кібервійна», «кібертероризм», що потенційно можуть ефективно застосовуватись у практиці правоохоронної діяльності; 2) нереформованість чинного нормативно-правового поля у сфері кібербезпеки; 3) відсутність Єдиної загальнодержавної системи протидії кіберзлочинності з необхідним нормативним забезпеченням [4].

Зауважимо що, кіберзлочинність – за своєю природою транскордонне явище, що дозволяє більшості вчених вказувати на те, що для кіберзлочинів є характерним максимальний рівень латентності. Факторами латентності кіберзлочинів виступають такі: 1) складність механізму вчинення кіберзлочинів, поєднана з дуже різноманітними сферою та наслідками їх учинення, а також «комп'ютерна безграмотність» більшості потенційних жертв кіберзлочинів, їх нехтування своєю безпекою; 2) негативна поведінка жертв (очевидців) злочину – незвернення жертви та осіб, яким відомо про злочин, до правоохоронних органів і неповідомлення про факт вчинення кіберзлочину; 3) недоліки в роботі правоохоронних органів стосовно реагування на звернення та повідомлення про кіберзлочини.

Підкреслимо що, саме реалізація загальносоціальних заходів запобігання дає змогу усунути чи мінімізувати вплив криміногенних факторів детермінації кіберзлочинності, запобігти формуванню особистості злочинця. Окремим заходом запобігання вчиненню кіберзлочинів є виявлення та запобігання діяльності кібертерористів, тобто осіб, які використовують комп'ютерну техніку, пристрої та мережі для вчинення терористичних актів [5].

Викладене вище дозволяє дійти висновку, що кіберзлочиність – виходить за межі однієї країни, це явище, яке водночас має ряд переваг, а в той же час характеризується негативним впливом не тільки на охоронювані законом права, інтереси, свободи, суспільні відносини людей, підприємств, установ, організацій, але й на інфраструктуру країни в цілому, що може призвести до ряду негативних наслідків. Аналізуючи тенденції розвитку кіберзлочинності на світовому рівні, Україна повинна продовжувати активні дії в контексті розбудови власної системи кібербезпеки. Таким чином, слід звернути увагу на необхідність створення в системі органів державної влади та місцевого самоврядування, відповідних структур, які б контролювали та наглядали за безпекою, законністю та доцільністю операцій з передачі, обробки та використання інформації для своєчасного, попередження, виявлення, припинення та неупередженого розкриття кіберзлочинів.

Література:

1. Конвенція про кіберзлочинність : міжнародний документ від 23.11.2001 // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 10.09.2018).

2. Болгов В., Гадіон Н., Гладун О. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій: наук.-практ. посіб. К.: Національна академія прокуратури України, 2015. 202 с.

3. Про Доктрину інформаційної безпеки України : Указ Президента України від 8 липня 2009 року № 514/2009 [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=514%2F2009.

4. Кібербезпека: світові тенденції та виклики для України. Аналітична доповідь: [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/content/articles/files/kyber_bezpekaaab17.pdf.

5. Кримінологія. Академічний курс / кол. авт. ; за заг. ред. О. М. Литвинова. Київ : Кондор, 2018. 588 с.