Отже, аналіз законодавства та практики його застосування в діяльності Національної поліції в сфері кібербезпеки в Україні підтверджує, що ці підрозділи, крім заходів захисту інформації, активно використовують новітні технології для протидії комп'ютерній злочинності та кіберзагрозам. Однак у сучасних умовах також критично важливо розробити систему заходів, спрямованих на чітке визначення поняття "дезінформація" у цифровому просторі, а також методи її виявлення та протидії шляхом закріплення цих аспектів у законодавстві.

***Література*:**

1. Боротьба з кіберзлочиннісю в умовах воєнного стану. URL: https://jurliga. ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanuzakon-2149-ix (дата звернення: 10.11.2023).
2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017. № 2163-VIII. Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 10.11.2023).
3. Присяжнюк М.М., Цифра Є.І. Особливості забезпечення кібербезпеки. Реєстрація, зберігання і обробка даних. 2017. Т. 19. № 2. С. 61–68. (дата звернення: 10.11.2023).
4. Ліпкан В.А., Діордіца І.В. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. Підприємництво, господарство і право. 2017. № 5. С. 174–180. (дата звернення: 10.11.2023).
5. Діордіца І.В. Адміністративно-правове регулювання кібербезпеки України : автореф. дис. ... д-ра юрид. наук : 12.00.0; Запорізький нац. ун-т. Запоріжжя, 2018. 32 с. (дата звернення: 10.11.2023).
6. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24.03.2022. № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text (дата звернення: 10.11.2023).

ОСОБЛИВОСТІ ЗМІН КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА КІБЕРЗЛОЧИНИ В УКРАЇНІ

Лучик Василь Єфремович
доктор економічних наук
професор кафедри протидії кіберзлочинності факультету №4
Харківського національного університету внутрішніх справ
Кочин Владислав Дмитрович
Здобувач вищої освіти

З самого початку існування України, як незалежної держави, влада незалежної України боролася із кіберзлочинністю. Аналізуючи [1-3], можна визначити власне поняття кіберзлочину. Кіберзлочин – небезпечні та незаконні діяння, які спрямовані на кіберпростір за допомогою електронно-обчислювальних машин (комп’ютерів), комп’ютерних систем та мереж і мереж електрозв’язку.

Згідно конвенції Ради Європи по боротьбі з кіберзлочинністю виділяють 4 основних типи кіберзлочинів:

- злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем;
- злочини щодо авторських і суміжних прав;
- шахрайство та підробка, пов'язані з використанням комп'ютерів;
- злочини, пов'язані з розміщенням у мережах протиправної інформації [2].

У свою чергу, Рада Європи по боротьбі з кіберзлочинністю [3] ділить кіберзлочини на 10 видів: піратство, скімінг, кардинг**,** фішинг, вішинг, шимінг**,** рефайлінг, мальваре**,** протиправний контент**,** онлайн-шахрайство.

Україна почала боротися із кіберзлочинністю ще з 2001 року, і відповідальність за кіберзлочини з’явилася у XVI розділі Кримінального кодексу України під назвою

«Кримінальні правопорушення у сфері використання електро-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» [4].

Перші зміни XVI розділу ККУ регламентовані 2003 роком змінами до Закону України «Про внесення змін до Кримінального кодексу України щодо відповідальності за незаконне втручання в роботу мереж електрозв'язку» № 908-IV від 05.06.2003 року [5]. Після доповнень розділ став називатися «Кримінальні правопорушення у сфері використання електро-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»

Одне із ключових змін XVI розділу ККУ, були доповнення статей 361 та 363 частинами 361-1, 361-2, 363-1, Закону України «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України» № 2289-IV від 23.12.2004 року [6], ці зміни додали нові частини до ККУ, та розширило список протиправних дій проти *електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.* Доповнення охопило навмисне створення та збут шкідливого програмного забезпечення, навмисне розповсюдження секретної інформації з комп'ютерів та навмисне перешкоджання роботі шляхом розповсюдження повідомлень електрозв'язку, *зміцнило право на захист даних, збережених всередині персональних комп'ютерів, що як слідство допомогло зміцнити внутрішню безпеку України.*

У 2015 році був прийнятий Закон України «Про внесення змін до Кримінального кодексу України щодо вдосконалення інституту спеціальної конфіскації з метою усунення корупційних ризиків при її застосуванні»[7] із зміною статтей 361, 361-1, 361-2, 362, 363-1.

Найпотужніші зміни XVI розділу ККУ відбулися 24.03.2022 року, згідно Закону України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» [8], ним було охоплено більше випадків несанкціонованих втручань в роботу, змін даних комп'ютерів та інших електронних систем, цей закон вже допомагає поліції, СБУ, ДБР та іншим уповноваженим підрозділам боротися із колаборантами, зрадниками та хакерськими атаками під час дії воєнного стану.

Таким чином, аналізуючи зміни XVI розділу ККУ, можемо прийти висновку, що відповідальність за кіберзлочини в України почала охоплювати все більше випадків незаконного втручання в роботу комп'ютерів, несанкціонованих змін даних, та інших протиправних дій стосовно *використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.*

На сьогодні, згідно із чинним законодавством Кримінального кодексу України, передбачений розділ XVI «Кримінальні правопорушення у сфері використання електро-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», який визначає кримінальну відповідальність за кіберзлочини, а саме: ст.361, ст.361-1, ст.361-2, ст. 362, ст. 363, ст. 363-1 Кримінального кодексу України, та карається накладанням штрафу, обмеженням волі або позбавленням волі з позбавленням права обіймати певні посади чи займатися певною діяльністю.

Висновки. Кіберзлочин представляє собою небезпечні та незаконні діяння, за допомогою електронно-обчислювальних машин (комп'ютерів), комп'ютерних систем та мереж, які спрямовані на кіберпростір. Аналізуючи зміни, внесеними в різні роки, було додано нові статті, змінено існуючі, додані нові частини. Усі ці зміни сприяли більш ефективній боротьбі із кіберзлочинами. Останні зміни ККУ у сфері протидії кіберзлочинності були спрямовані на підвищення ефективності боротьби із кіберзлочинами в умовах дії воєнного стану. Чинне законодавство України все ще не є досконалим щодо відповідальності у сфері кіберзлочинності, але згідно історії змін ККУ, найближчим часом наше законодавство буде охоплювати більше випадків у цій сфері.

***Література*:**

1. Кримінальна відповідальність за кіберзлочини. URL: http://surl.li/azxue (20 серпня 2017 року).

2. Інформаційні злочини. URL: http://surl.li/mgodx
3. Конвенція Ради Європи по боротьбі з кіберзлочинністю. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
4. Кримінальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
5. Закон України «Про внесення змін до Кримінального кодексу України щодо відповідальності за незаконне втручання в роботу мереж електрозв'язку» № 908-IV від 05.06.2003. URL: https://zakon.rada.gov.ua/laws/show/908-15#Text
6.Закон України «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України» № 2289-IV від 23.12.2004. URL: https://zakon.rada.gov.ua/laws/show/2289-15#Text
7.Закон України «Про внесення змін до Кримінального кодексу України щодо вдосконалення інституту спеціальної конфіскації з метою усунення корупційних ризиків при її застосуванні» № 770-VIII від 10.11.2015. URL: https://zakon.rada.gov.ua/laws/show/770-19#Text
8.Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану». URL: https://zakon.rada.gov.ua/laws/show/2149-20/

ЗАСТОСУВАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У ФІКСАЦІЇ ВОЄННИХ ЗЛОЧИНІВ

Лучик Світлана Дмитрівна
доктор економічних наук, професор, професор кафедри протидії кіберзлочинності,
Харківський національний університет внутрішніх справ
Столик Денис
курсант спеціальності «Кібербезпека»,
Харківський національний університет внутрішніх справ

Світ безперервно розвивається як в інформаційному плані, так і в плані розвитку військових технологій. З цим на учасників військових конфліктів накладається суворіша відповідальність за використання більш потужної зброї та ведення конфлікту загалом. На жаль, нашій державі доводиться відбивати вторгнення російського агрессору, який переслідує ціль знищення українського народу. Вороже командування порушує міжнародні закони та звичаї війни. Кожного дня рашисти вчиняють воєнні злочини на українській землі. Тому є нагальна потреба фіксувати всі воєнні злочини для притягнення до кримінальної відповідальності агресора на національному і міжнародному рівнях.

Воєнний злочин визначають як порушення законів та звичаїв війни. Воєнні злочини належать до сфери виключно міжнародного кримінального права і повний перелік воєнних злочинів закріплений у Статуті Міжнародного кримінального суду (Римський статут). На жаль, Україна не ратифікувала Римський статут. Для нашої країни це становить певні серйозні бар'єри, зокрема, це є зобов'язанням Украйни за Угодою про асоціацію з ЄС. Тому в довгостроковій перспективі Україна повинна ратифікувати Статут. Чинне національне законодавство не містить визначення поняття «воєнний злочин». Проте, правозахисники стверджують, що попри відсутність законодавчого визначення воєнних злочинів, деякі з тих злочинів, що передбачені Кримінальним кодексом України (ККУ), є саме воєнними, а не військовими, злочинами, а саме:

мародерство (стаття 432 ККУ).

насильство над населенням у районі воєнних дій (стаття 433 ККУ);

погане поводження з військовополоненими (стаття 434 ККУ);

незаконне використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала та зловживання ними (стаття 435 ККУ) [1]. Кримінальний кодекс Украйни також передбачає відповідальність за порушення законів та звичаїв війни (стаття 438 ККУ), геноцид (стаття 442), злочини проти осіб та установ, що мають міжнародний захист (стаття 444) тощо [2].

Росія не ратифікувала Римський статут, тому може не співпрацювати з Міжнародним кримінальним судом. Однак, це не означає, що країна не повинна нести відповідальність за всі ті злочини, що коїть в Україні, вбиваючи і викрадаючи людей, грабуючи і руйнуючи все