Шишацька Юлія Олегівна
студентка IV курс
Інституту кримінальної юстиції
Національного університету «Одеська юридична академія»

КРИМІНАЛЬНО-ПРАВОВІ ЗАСОБИ ПРОТИДІЇ КІБЕРЗЛОЧИННІСТІ В УКРАЇНІ

На сьогоднішній день стан розвитку сучасних інформаційних технологій та комп'ютерної техніки продовжує стрімко рости в умовах відкритого доступу до транснаціональної мережі Інтернет. Входження нашої держави у світовий інформаційний простір відкриває не тільки можливість для обміну інформацією та вільного спілкування, але і для поширення злочинної діяльності. Віртуальний світ багато в чому відображає світ реальний. Так, злочинність, як невід'ємна частина суспільства, існувала в усі часи, а зараз існує й у віртуальному світі через популяризацію інтернет-ресурсів, безпечність громадян і ліберальне кримінальне законодавство в сфері кібершахрайства.

В умовах стрімкого розвитку громадянського суспільства інформаційної доби й досі виділяють одну з найдинамічніших груп суспільно небезпечних посягань – кіберзлочини. В літературі є термінологічна визначеність «кібернетичний злочин» як передбачене кримінальним законом суспільно небезпечне винне діяння, що полягає в протиправному використанні інформаційних та комунікативних технологій, відповідальність за яке встановлена законодавством про кримінальну відповідальність. [2, с. 434].

У чинній редакції Кримінального кодексу України (далі – ККУ) передбачено самостійний розділ про злочини в кіберпросторі – розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Положення цього розділу неодноразово змінювалися і доповнювалися, що свідчить про актуальність врегулювання цієї проблеми на законодавчому рівні нашої державі. Згідно з ст. 361-1 та ст. 361-2 ККУ передбачено найсуворіше покарання у вигляді позбавлення волі на строк до п'яти років з конфіскацією програмних чи технічних засобів, які є власністю винної особи [1, с. 157-158].

Значна м'якість кримінально-правових санкцій цієї групи злочинів не перешкоджає здійсненню суб'єктом суспільно небезпечного діяння. Через недосконаліть чинного законодавства спостерігається сумна тенденція щодо росту кібернетичних злочинів на базі механізму інвестиційно-кредитної діяльності банківських та фінансових установ. Так, надалі збільшується кількість противоправних операцій з платіжними картками як різновид кібернетичного злочину. За даними досліджень Української міжбанківської асоціації членів платіжних систем ЕМА відомо, якщо

тенденція збережеться, то вже до кінця поточного року кожен тридцятий українець може стати жертвою кібершахраїв [3]. Саме тому, з метою попередження і протидії кібернетичної злочинності потрібно внести зміни у розділ XVI ККУ, в частині посилення покарання та передбачення для даної групи застосування додаткових покарань.

Крім того, серйозну загрозу інформаційній безпеці сьогодні створюють кібератаки, які можуть бути причиною порушення політики безпеки інформації або нанесенню збитків автоматизованій системі. У широких IT-колах існує термін «DoS-атаки» (англ. Denial-of-service attack), наміром яких є напад на комп'ютерну систему з метою зробити комп'ютерні ресурси або інформацію недоступними користувачам [2, с. 427].

Не можу не зазначити, що загрози інформаційній безпеці можуть створюватися шляхом використання IT для шпигунства, а також шляхом зловмисного використання соціальних мереж іноземними спецслужбами [4, с. 34-36]. Задля попередження загроз основам національної безпеки, для безпечного використання кіберпростору та боротьби з комп'ютерною злочинністю, уряд нашої держави продовжує активно розробляти законодавчу базу, шукати інноваційні шляхи забезпечення належної безпеки доступу до мережі Інтернет, а також збереження інформації з обмеженим доступом. Реформування підрозділів МВС та створення кіберполіції Національної поліції України є позитивним кроком для боротьби з особливою групою злочинів. Проте брак необхідного досвіду та навичок, а також недосконале структурування, відсутність розмежування компетенції підрозділів не приносить значної користі у IT-сфері.

Дуже важливо сьогодні зберегти увагу до вирішення питання проблеми кібернетичної злочинності і продовжувати реалізовувати програми протидії з урахування сучасного розвитку інформаційних технологій. Тільки систематичне вивчення та консолідація практичного надбання допоможе зберегти цілісність національної інформаційної безпеки нашої держави.

Список використаних джерел:

1. Кримінальний кодекс України від 5 квітня 2001 р. (із змінами та доповненнями) // Відомості Верховної Ради України. – 2001. – № 25-26. – Ст. 131. [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2341-14.

2. IT-право: теорія та практика: навч. посіб. / авт. кол. ; за ред. Є.О.Харитонова, О.І. Харитонової. – Одеса : Фенікс, 2017. – 472 с.

3. Новинки от телефонных мошенников [Електронний ресурс]. – Режим доступу: https://ema.com.ua/new-tricks-of-telephone-scams/

3. Шпигунство за нової доби // Український тиждень. – 2015. – № 31. – С. 34-36.

Науковий керівник: к.ю.н., доцент Колодін Д.О.