в Україні [Електронний ресурс]. – Режим доступу : http://virtuni.education.zp.ua/info_cpu/sites/default/files/aref_Strynevich.pdf.

5. Струневич О.П. Адміністративне законодавство про надання рекламних послуг: особливості сучасного стану / О.П. Струневич // Науковий вісник Херсонського державного університету. – 2015. – Вип. 1. – Т. 3. – С. 112-116.

9. Наливайко Л. Р. Конституційно-правова відповідальність: питання теорії та практики : дис. канд. юрид. наук : 12.00.02 / Л. Р. Наливайко ; Київський національний ун- т ім. Тараса Шевченка. – К., 2000. – 180 с.

Шматкова Анастасія Вадимівна
студентка юридичного факультету
Науковий керівник** – к.ю.н. **Кузьміна І.С.
(Дніпропетровський державний
університет внутрішніх справ)

ПРОБЛЕМИ НАЦІОНАЛЬНОГО ЗАКОНОДАВСТВА У СФЕРІ БОРОТЬБИ ІЗ КІБЕРЗЛОЧИННІСТЮ

Сучасний етап науково-технічного прогресу охопив фактично весь світ, зумовивши стрімкий перехід до глобального процесу інформатизації. Розвиток суспільства безпосередньо залежить та визначається стрімким розвитком інформаційних та телекомунікаційних технологій.

Так, інформація являє собою один з головних елементів даного процесу. Як зазначав американський вчений Норберт Вінер, «інформація – це позначення змісту, отриманого з зовнішнього світу в процесі нашого пристосування до нього і пристосування до нього наших почуттів». Інакше кажучи, інформація відіграє важливу роль як у житті індивіда, так і в існуванні суспільства в цілому, ставши невід'ємною частиною людського буття. Сьогодні майже в усі сфери людської діяльності успішно впроваджено комп'ютерні технології. Разом з тим українське суспільство не відстає від загальносвітових тенденцій у сферах інформатизації та комп'ютеризації.

З моменту запровадження процесу комп'ютеризації поряд з перевагами з'явились й певні негативні наслідки, найголовнішим з яких є утворення якісно нового виду злочинності – кіберзлочинності. В умовах сучасного науково-технічного прогресу та розвитку інформаційних систем комп'ютерні дані можуть бути передані з однієї точки світу в іншу за декілька секунд. При здійсненні цієї процедури інформація розбивається на частини та передається найзручнішими і доступними каналами, які можуть знаходитись у віртуальному просторі різних країн. Тому об'єкт, суб'єкт злочину та потерпілий не завжди мають єдину територіальну приналежність, що зумовлює налагодження співпраці правоохоронних органів країн світу при розслідуванні злочинів даної категорії.

З метою зупинення дій, спрямованих проти конфіденційності, цілісності

і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, забезпечення належного балансу між правоохоронними інтересами і повагою до основних прав людини держави-члени Ради Європи 23.11.2001 у Будапешті підписали міжнародний договір – Конвенцію про кіберзлочинність (далі – Конвенція), яку 07.09.2005 ратифіковано в Україні.

Відповідно до положень зазначеного міжнародного договору після надання згоди на обов'язковість певним органом законодавчої влади, з моменту затвердження, Конвенція набирає юридичну силу та становить частину національного законодавства країни. До того ж, підписанти погодились у необхідності ведення спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, шляхом створення відповідного законодавства і налагодження міжнародного співробітництва[2].

Після своєї появи поняття«кіберзлочин» одразу ж стало предметом міжнародного і національного правового регулювання. Наслідком його виникнення стало утворення певних проблем, пов'язаних із імплементацією міжнародних правових норм, їх удосконаленням та закріпленням у чинному законодавстві нашої держави, що, в свою чергу, обумовило необхідність теоретико-правового розуміння суті даного поняття.

Терміни, визначені у Конвенції та додаткових протоколах до неї, ще й досі законодавчо не визначені у національних нормативно-правових актах, а чинне вітчизняне законодавство у сфері протидії інформаційним злочинам майже не охоплює усі ключові елементи для ефективної боротьби із кіберзлочинністю всіх рівнів складності.

Оскільки на даний час існують зазначені вище прогалини в чинному законодавстві України, то на прикладі декількох визначень, запропонованих вченими даної галузі, спробуємо усунути неясність у розумінні ключового поняття «комп'ютерний злочин» та уточнити його зміст.

Так, у навчальному посібнику М.В. Салтевський зазначив, що комп'ютерний злочин — це протиправне використання засобів електронно-обчислювальної техніки: великих, середніх і малих машин, у тому числі персональних комп'ютерів, програмних засобів, технологій і комунікативних систем зв'язку в корисливих злочинних цілях. Засобом (знаряддям) вчинення такого злочину слугують комп'ютер, засоби зв'язку і програмні засоби для забезпечення їх працездатності [6].

Проте з даним визначенням можна погодитись лише частково, оскільки злочини в інформаційній сфері можуть бути вчинені не тільки в корисливих злочинних цілях.

На думку вчених В.С. Цимбалюка, П.Д. Біленчука, Б.В. Романюка та інших авторів навчального посібника, комп'ютерний злочин можна визначити як передбачені законом суспільно небезпечні дії, що посягають на встановлений у суспільстві порядок інформаційних відносин та скоюються за допомогою засобів електронно-обчислювальної техніки[7].

Для належного забезпечення безпеки кіберпростору держави та заповнення прогалин чинного законодавства Національним інститутом стратегічних досліджень, до функцій якого входить науковий аналіз і оцінка проблем, перспектив, дослідження проблемних питаньекономічного, демографічного, соціального, гуманітарного, етнополітичного, воєнно-політичного, зовнішньополітичного, інформаційного, екологічного розвитку нашої держави [9], спрямовано низку офіційних запитів до ключових відомств та наукових установ, що мають відношення до інформаційної безпеки держави з метою надання визначень основних термінів у даній сфері[8].

Після детального аналізу відповідей під ключовими поняттями «кібербезпека», «кіберзахист», «кіберзлочин» запропоновано розуміти таке:

1) кібербезпека – стан захищеності кіберпростору в цілому або окремих об'єктів його інфраструктури від ризику стороннього кібернетичного впливу (кібератак), за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз особистим, корпоративним та/або національним інтересам;

2) кіберзахист – сукупність методів і заходів організаційного, нормативно-правового та технічного характеру, спрямованих на забезпечення кібербезпеки;

3) кіберзлочин – кримінальна дія, відповідальність за яку передбачено кримінальним законодавством, яка здійснена (здійснюється) у кіберпросторі (або за допомогою його технічних можливостей) і несе у собі суспільну небезпеку[4].

Отже, виходячи з вищевикладеного, можна стверджувати, що комп'ютерний злочин являє собою суспільно небезпечне злочинне діяння, що здійснювалось у кібернетичному просторі за допомогою комп'ютерних технологій та електронно-обчислювальних засобів, відповідальність за яке передбачено кримінальним законодавством.

Однак, виходячи з Розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» Кримінального кодексу України, можна дійти висновку, що «комп'ютерний злочин» у кримінально-правовому розумінні – це:

- несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст.361 КК України);
- створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст.361-1 КК України);
- несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст.361-2 КК України);
- несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, ком-

п'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст.362 КК України);

- порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється (ст.363 КК України);
- перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст.363-1 КК України)[3].

У своїй статті «Щодо поняття злочинів у сфері комп’ютерних технологій» О.А. Федотов висловив думку, що кримінально-правове тлумачення поняття «комп’ютерний злочин» відрізняється від криміналістичного, яке є значно ширшим, оскільки охоплює й інші склади злочинів, які містяться в КК України, але знаходяться в інших його розділах[5].

Через недосконаліть національного законодавства у сфері протидії кіберзлочинності та певні прогалини постала інша не менш важлива проблема – неналежна координація діяльності правоохоронних структур відповідно до покладених функцій та правового впорядкування меж відповідальності відомств. Відсутність чіткої законодавчої визначеності термінів, фактичне розмежування понять, функцій з метою ефективного практичного їх застосування, впровадження засобів комплексного реагування, недостатність роботи із попередження і запобігання злочинів у цій сфері, а також процедур взаємодії відповідальних відомств роблять уразливими інформаційну безпеку нашої держави.

В Україні функції боротьби з кіберзлочинністю покладено на Департамент кіберполіції Національної поліції України, а якщо питання стосується державної безпеки, то справою займаються працівники Служби безпеки України.

Також слід зазначити, що задля ефективної роботи у сфері протидії кіберзлочинності необхідно мати спеціалістів з комп’ютерної техніки та програмування, так званих ІТ-спеціалістів, та експертів в області комп’ютерно-технічної експертизи. Адже сучасні інформаційні технології удосконалюються щоденно. З огляду на це, окрім наявності відповідних юридичних знань, потрібно володіти спеціальними знаннями і навичками для того, щоб, принаймні, не «відставати» від еволюційного розвитку і вдосконалення техніки разом з інформаційними технологіями та досконально розбиратися у механізмах вчинення кіберзлочинів.

Підсумовуючи, можна дійти висновку, що кіберзлочинність є порівняно новим видом суспільно небезпечних діянь, який удосконалюється і «йде у ногу» з провідними технологіями, що у свою чергу значно ускладнює швидке виявлення таких злочинів та гальмує розробку методів, заходів, які спрямовані на протидію та запобігання зазначеним правопорушенням.

З розгляду певних нормативно-правових актів нашої держави вбачається, що, незважаючи на їх наявність, існує велика загроза кібербезпеки для України. Це зумовлено термінологічною невизначеністю ключових елементів, що, як наслідок, унеможливлює втілення особливих форм захисту, реагування та відповідальності від кіберзлочинності, тобто формування та упорядкування нормативно-правового поля у сфері протидії кіберзлочинності.

Можливим варіантом вирішення даної проблеми є розробка та впровадження базового документа, в якому буде законодавчо закріплено визначення ключових понять, та впроваджено стратегічну програму, яка буде враховувати позитивний міжнародний досвід у сфері протидії кіберзлочинності, та містити у собі комплекс особливих форм захисту та реагування на злочини в кібернетичному просторі, наприклад впровадження систем моніторингу і контролю можливих кіберзагроз.

Окрім цього, нині існують труднощі з кадровим наповненням відповідних структурних підрозділів. Відсутність достатньої кількості фахівців у сфері інформаційних технологій робить Україну залежною від програмних і технічних продуктів іноземного виробництва, що у свою чергу уповільнює впровадження нових сучасних інформаційних технологій в даній галузі.

Тому задля вирішення цього питання необхідно законодавчо впровадити певні кваліфікаційні критерії для працівників структурних підрозділів, які ведуть боротьбу з кіберзлочинністю, а саме наявність певної освіти (у сфері інформаційно-комунікаційних технологій, програмування тощо), знань та навичок, професійного досвіду, які дадуть змогу ефективно протидіяти високотехнологічним злочинам. З боку держави необхідно провести реформування у сфері освіти і науки з даного питання, а саме впровадити спеціалізовану комплексну підготовку (принцип поєднання юридичних та технічних знань) для кадрів, які будуть задіяні у боротьбі із кіберзлочинністю. Для діючих працівників структурних підрозділів можна запровадити стажування у тих державах, з якими налагоджено взаємодію та міжнародне співробітництво у даній сфері, для одержання міжнародного досвіду, навичок та практики, які стануть одними з ключових факторів підвищення результативності роботи правоохоронних органів у даній сфері. Також введення систематичних курсів підвищення кваліфікації та проведення щорічних тестувань особового складу структурних підрозділів дадуть змогу контролювати сталий професійний рівень та знань, потрібних для ефективної та дієвої роботи правоохоронних органів у боротьбі із злочинами, вчиненими в кібернетичному просторі.

Імплементація та впровадження зазначених положень до національного законодавства сприятиме підвищенню рівня ефективності боротьби правоохоронних органів України із кіберзлочинами.

Література

1. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 № 2824-IV // Відомості Верховної Ради України. – 2006. – № 5-6. – Ст. 71.

2. Конвенція про кіберзлочинність: Конвенцію ратифіковано із застереженнями і

заявами Законом № 2824-IV (2824-15)від 07.09.2005 [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/994_575.

3. Кримінальний кодекс України: Закон від 05.04.2001 № 2341-III // Відомості Верховної Ради України. – 2001. – № 25-26. – Ст. 131 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2341-14.

4. Дубов Д., Ожеван М. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування / Д. Дубов, М. Ожеван [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/articles/454.

5. Щодо поняття злочинів у сфері комп'ютерних технологій / О.А. Федотов // Економіка. Фінанси. Право. – 2010. – № 10. – С.37-39.

6. Основи методики розслідування злочинів, скоєних з використанням ЕОМ : навч. посібник / М.В. Салтевський. – Харків: Нац. юрид акад. України, 2000. – 35 с.

7. Біленчук П.Д., Романюк Б.В., Цимбалюк В.С. та ін. Комп'ютерна злочинність: навч. посібник. – К.: Атака, 2001. – 240 с.

8. Питання Національного інституту стратегічних досліджень: Указ Президента України від 16.12.2002 № 1158/2002 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/1158/2002.

9. Про Інститут / Офіційне інтернет-представництво «Національний інститут стратегічних досліджень». – 2012 [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/presentation.html.

Южека Роман Сергійович
студент юридичного факультету
Науковий керівник** – д.ю.н., професор **Наливайко Л.Р.
(Дніпропетровський державний університет внутрішніх справ)

ЩОДО ЗАХИСТУ ПРАВ І СВОБОД ЛЮДИНИ ТА ГРОМАДЯНИНА В УКРАЇНІ НА СУЧАСНОМУ ЕТАПІ ДЕРЖАВОТВОРЕННЯ

Захист прав і свобод людини і громадянина є найважливішим та найголовнішим обов'язком кожної держави світу. Україна не є винятком, оскільки саме стаття 3 Основного Закону України (Конституції України) закріплює фундаментальну базову конституційну засаду, дія якої відповідно спрямовує усю сукупність громадсько-політичних відносин. Права і свободи людини і громадянина та їх гарантії визначають зміст і спрямованість діяльності держави. Конституція України зазначає, що саме держава відповідає перед суспільством, зокрема перед кожною людиною, за свою діяльність, оскільки саме від неї залежить забезпечення реалізації захисту прав і свобод людини і громадянина.

Тема захисту прав і свобод людини і громадянина стала предметом дослідження багатьох вчених: А.С. Головіна, В.М. Кампо, С.В. Ківалова, А.Р. Крусян, В.Я. Тація, С.В. Шевчука та інших. Проте захист прав і свобод