Заході, в силу нейтральної громадської думки, християнських традицій і моральних підвалин лікарів [5, с. 343–345]. Вважаємо, що на даному етапі з упевненістю можна відзначити, що Україна сьогодні не готова до будь-якого кроку в цьому напрямку.

Список використаних джерел:

1. Декларація про евтаназію, прийнята 39-му пленумі Всесвітньою Медичною Асамблеєю (Мадрид, жовтень 1987) / [Електронний ресурс]. – Режим доступу: http://www.medicusamicus.com/index.php? action=laws8

2. Мяловицька Н. А. Евтаназія: право на життя / Мяловицька Н. А., Голопапа Д. І. // Вип. 23, ч. 1, т. 1.// Науковий вісник Ужгородського національного університету. Серія: Право / Ужгородський нац. ун-т. – Ужгород, 2013. – Вип. 23, ч. 1, т. 1. – С. 122–124.

3. Риндя Д. Д. Правові та моральні аспекти евтаназії: реалізація» права на гідну смерть» / Риндя Д. Д. // Сучасні проблеми правової системи України : зб. матеріалів VIII Міжнар. наук.-практ. конф., 26 листоп. 2015 р. – Київ, 2015. – Вип. 7. – С. 260–263.

4. Трофімов І. С. Евтаназія: досвід зарубіжних країн та проблеми легалізації в Україні / І. С. Трофімов // Актуальні проблеми юридичної науки. – Хмельницький, 2011. – Ч. 3. – С. 401–403.

5. Ущапівська Д. П. Евтаназія: проблема легалізації в Україні / Ущапівська Д. П. // Сьомі юридичні читання «Культура і право на початку XXI століття». – К., 2011. – С. 343–345.

Коваль І.О.
студентка,
Науковий керівник: **Діордіца І. В.**
кандидат юридичних наук, доцент,
Навчально-науковий Юридичний інститут,
Національний авіаційний університет

ПОНЯТТЯ ТА ЗМІСТ КІБЕРШПИГУНСТВА

Зростання залежності від інформаційно-комунікаційних технологій робить сучасне українське суспільство більш уразливим перед можливими негативними наслідками протиправного використання кіберпростору. В цих умовах головним завданням держави є вжиття заходів, що дозволять принципово зменшити (а подекуди – унеможливити повністю) негативні наслідки від кібератак.

Існує багато видів кібернетичних загроз, але останнім часом популярності набирає саме кібершпигунство, адже інформація з обмеженим доступом, що циркулює в національних інформаційних ресурсах є стійким об’єктом зацікавленості з боку інших держав, організацій та осіб. Крім того, все більшого поширення набуває політично вмотивована діяльність в кіберпросторі груп активістів (хактивістів), які здійснюють атаки на урядові та приватні сайти, що призводить до порушень роботи інформаційних ресурсів, а також репутаційних та матеріальних збитків. Наприклад, в червні 2016 стало відомо про виявлення несанкційованого втручання до

інформаційної системи Національного комітету Демократичної партії США. В результаті проведеного розслідування було встановлено, що зламати інформаційну систему вдалось двом угрупуванням російських хакерів. Одна група проникла до інформаційної системи ще влітку 2015 року, а інша – в квітні 2016 року. Вкупі, обидва угрупування спромоглись викрасти скриньки електронної пошти а також зібраний компромат на конкурента демократів на виборах – Дональда Трампа [1].

З огляду на це необхідним є визначення поняття та змісту кубершпигунства.

Кібершпигунство є одним із видів кіберзлочинів, а останні в свою чергу мають свою специфіку. Так В. М. Болгова визначає кіберзлочини як 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, с. 85–86]

Кібершпигунство має в собі складову шпигунства, а останнє за Кримінальним Кодексом України (Далі – КК України) є кримінально-караним діянням.

Відповідно до ст. 114 КК України шпигунством є передача або збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю [3].

Відповідно до ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», який набере чинності 9 травня 2018 року кібершпигунством є шпигунство, що здійснюється у кіберпросторі або з його використанням [4].

Виходячи з даних положень можна сказати, що кібершпигунство – це передача або збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю, якщо ці дії вчинені іноземцем або особою без громадянства, що здійснюється у кіберпросторі або з його використанням.

Щоб проаналізувати зміст кібершпигунства, на нашу думку, необхідно здійснити аналіз такого злочину, як шпигунство, а також розглянути загальні ознаки кіберзлочинності.

Проводячи аналіз ст. 114 КК України можна виділити наступне:

1) шпигунство може виражатися у двох формах: 1) передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю; 2) збиранні таких же відомостей з метою передачі іноземній державі, її організаціям або їх представникам.

2) збирання відомостей, що становлять державну таємницю, – це будь-які випадки здобуття таких відомостей (наприклад, викрадення, особисте спостереження, фотографування, підслуховування телефонних розмов та ін.). Нерідко для отримання таких відомостей використовується найскладніша

сучасна техніка (спеціально обладнані літаки, кораблі або автомашини, спеціально встановлені на суші чи на морі прилади для отримання розвідувальної інформації та ін.). Для відповідальності за ст. 114 важливо встановити, що відомості, які становлять державну таємницю, були передані чи збиралися для передачі саме іноземним державам, іноземним організаціям або їх представникам.

3) безпосереднім об'єктом цього злочину є зовнішня безпека України; 4) з об'єктивної сторони шпигунство виражається в передачі або збиранні з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю;

5) предметом шпигунства є відомості, що становлять державну таємницю, вичерпний перелік яких міститься в Законі України «Про державну таємницю» від 21 січня 1994 р. 1. Згідно з цим законом державною таємницею визнається певний вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою;

6) закінченим шпигунство вважається з моменту початку збирання вказаних відомостей або з моменту їх передачі;

7) суб'єктивна сторона цього злочину – прямий умисел, за якого особа усвідомлює, що відомості збираються або передаються іноземній державі, організації або їх представникам і що ці відомості є державною таємницею, яка не підлягає передачі. Мотиви злочину на кваліфікацію не впливають.

8) суб'єкт злочину – іноземець або особа без громадянства, які досягли 16-річного віку. Громадянин України за шпигунство несе відповідальність за ст. 111 – за державну зраду [5].

Що ж до ознак кіберзлочинності, то можна назвати такі:

1) ці злочини вчиняються у віртуальному просторі або в межах комп’ютерних мереж. Віртуальний простір – це модульований за допомогою комп’ютера інформаційний простір, в якому містяться дані про осіб, факти, явища, процеси, представлені в математичному, символьному чи іншому вигляді. Ці відомості знаходяться в процесі руху по локальних і глобальних комп’ютерних мережах, зберігаються в пам’яті будь-якого фізичного або віртуального пристрою, спеціально призначених для їх зберігання, переробки та передачі;

2) кіберзлочини вчиняються за допомогою комп’ютерних систем або шляхом використання комп’ютерних мереж та інших засобів доступу до віртуального простору, а також проти комп’ютерних систем, комп’ютерних мереж і комп’ютерних даних. Таким чином, електронно-обчислювана техніка може виступати як засобом вчинення злочину, так і предметом злочину [6].

Виходячи з зазначеного вище можна стверджувати, що кібершпигунство містить у собі усі ознаки шпигунства, але принциповою відмінністю є те, що з об’єктивної сторони даний злочин полягає у вчиненні за допомогою комп’ютерних систем або шляхом використання компютерних мереж передачі або збирання з метою передачі іноземній державі, іноземній організації або їх

представникам відомостей, що становлять державну таємницю. Також дане діяння має вчинюватися у віртуальному просторі.

На сьогодні комп'ютерні злочини – це одна з найдинамічніших груп суспільно небезпечних посягань. Швидко збільшуються показники поширення цих злочинів, зокрема і кібершпигунства, а також постійно зростає їх суспільна небезпечність. Слід зауважити, що український законодавець приділяє значну увагу цій проблемі: новий Кримінальний кодекс України вперше передбачив самостійний розділ про ці злочини – розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж»; двічі положення цього розділу змінювалися і доповнювалися – це свідчить про актуальність цієї проблеми в суспільстві. Також Верховною Радою України прийнятий новий Закон України «Про основні засади забезпечення кібербезпеки України», що є великим кроком до удосконалення правового регулювання у даній сфері.

Список використаних джерел:

1. Перелік кібератак [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%BB%D1%96%D0%BA_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA#. D0.9A.D1.96. D0. B1. D0. B5. D1.80. D1.88. D0. BF.D0. B8. D0. B3. D1.83. D0. BD.D1.81. D1.82. D0. B2. D0. BE.

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

3. Кримінальний кодекс від 05. 04.2011 року [Електронний ресурс] – Режим доступу до ресурсу: http://zakon3. rada.gov.ua/laws/show/2341–14

4. Про основні засади забезпечення кібербезпеки України від 05. 10. 2017 року [Електронний ресурс] – Режим доступу до ресурсу: http://zakon2.rada.gov.ua/laws/show/2163–19.

5. Науково-практичний коментар ст. 114. Шпигунство [Електронний ресурс] – Режим доступу до ресурсу: http://radnuk.info/komentar/kruminal/osobluva/287-rozd1/4401--114-.html.

6. Поняття та кримінологічна характеристика кіберзлочинності [Електронний ресурс] – Режим доступу до ресурсу: http://lib-net.com/content/9684_Ponyattya_ta_kriminologichna_harakteristika_kiberzlochinnosti.html.