

КРИМІНАЛЬНЕ ПРАВО, КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО, КРИМІНОЛОГІЯ

Вергелес О.А.

студент,

Науковий керівник: Хавронюк М.І.

доктор юридичних наук, професор,

Київський національний університет імені Тараса Шевченка

ПОНЯТТЯ «КІБЕРЗЛОЧИНУ» В ДОКТРИНІ УКРАЇНСЬКОГО КРИМІНАЛЬНОГО ПРАВА

XXI століття характеризується високою комп'ютеризацією усіх сфер суспільного життя. Юриспруденція отримала масу нових завдань, які полягають у тому, щоб оформити відповідні правовідносини на законодавчому рівні.

Це ж стосується і кримінального права, тому що нині багато злочинів вчиняється за допомогою автоматизованих систем передачі інформації (зокрема ЕОМ – як найефективнішого способу заміни розумової діяльності людини). Постає ряд проблем, які потребують нагального вирішення: класифікувати такі злочинні діяння, визначити склади злочинів, просторову юрисдикцію держав, відповідальність, основні ознаки та власне саме поняття кіберзлочину, яке є новелою українського права [1].

Нарівні з поняттям «кіберзлочин» в іноземній доктрині використовують терміни «інтернет-злочин» та «комп'ютерні злочини».

Зокрема, польський науковець Магдалена Самодульська дослідила комп'ютерні злочини та вирізняла їх з поміж інтернет-злочинів та кіберзлочинів у своїй роботі «CRIMES COMMITTED VIA THE INTERNET – SELECTED ASPECTS» [2].

Вона зазначає, що поняття «комп'ютерний злочин» є найбільш широким, і визначається через об'єкт, предмет, знаряддя і спосіб вчинення злочину, натомість інтернет-злочини – це протиправні діяння, єдиною можливістю вчинити які надає Інтернет. Кіберзлочини вона позначає як під категорію комп'ютерних злочинів.

На мою думку, поняття «кіберзлочину» є більш широким ніж «комп'ютерний злочин», через те, що використання слова «комп'ютер» виключає можливе застосування інших технічних пристроїв, які можуть замінити людську розумову діяльність. Тому доцільніше використовувати саме перше – «кіберзлочин», як таке, що повністю визначає характерну ознаку цих злочинів – будь-яку автоматизовану систему. А Інтернет-злочини визначити як підкатегорію кіберзлочинів, обов'язковою ознакою об'єктивної сторони яких є Інтернет (як місце та/або спосіб їх вчинення).

Щоб визначити поняття та обґрунтувати вживання саме поняття «кіберзлочин», потрібно звернутись до кібернетики.

Зокрема, батько кібернетики Норберт Вінер, вважав, що «Кібернетика – це наука про управління, регулювання і передачу інформації в організмі тварини і машини» [3].

Його наступник Георг Клаус вважав визначення занадто широким, тому у 50-х роках дав власне визначення кібернетики як «науки про загальні закони перетворення інформації в складних системах» [4].

Радянський кібернетик Віктор Глушков перевершив своїх попередників чітко визначивши предмет дослідження кібернетики, чим і дав розвиток таким наукам як інформатика, програмування, теорія інформації в Україні. Зокрема він зазначав: «Кібернетика – наука про управління, зв'язок і переробку інформації (або ж наука про управління, або більш точно, наука про загальні закони перетворення інформації в управлінських системах. Основним об'єктом дослідження в кібернетиці є так звані кібернетичні системи». Кібернетичні системи, за його визначенням – це сукупність елементів, які здатні переробляти і передавати інформацію між собою. Основною метою таких систем є автоматизація розумової праці людини. «Прикладами кібернетичних систем можуть бути різного роду автоматичні регулятори в техніці (автопілот) електронно-обчислювальні машини тощо». Завдяки такому великому поясненню, можна припустити, що до таких систем можна зараховувати й роботів, автопілотів в автомобілях, розумні будинки і т.ін. Згодом цей список буде лише поповнюватися [5].

Зі сказаного випливає, що семантично «кіберзлочин» характеризує достатньо велику групу однорідних діянь та пояснює їхню природу та сутність – використання автоматичних пристроїв, які замінюють людську розумову діяльність.

Якщо звернутися до американського кримінального права, то там немає єдиного визначення «кіберзлочину», яке відрізняло б такі злочинні діяння від інших, що були вчинені в реальному світі. Федеральні правоохоронні органи США часто визначають «кіберзлочин», базуючись на юрисдикції певного штату та на основі конкретної справи, яку вони розслідують. Оскільки немає єдиного визначення поняття, то немає і єдиного органу, який би займався розслідуванням виключно таких злочинних діянь.

Один зі спеціалізованих органів – секретна служба Департаменту внутрішньої безпеки США. Зокрема, вони розслідують злочини, які потенційно могли бути вчинені за допомогою комп'ютера.

Британський професор-кримінолог, дослідник кіберзлочинів Девід Волл у своїй книзі зазначив: «Кіберзлочини – це широке означення злочинів, які мають місце в кіберпросторі (штучно створене віртуальне середовище, в межах якого працюють мережеві комп'ютери) [6].

Інші британські вчені Юджин Маклогін та Джон Мансі у своєму словнику кримінального права визначають «кіберзлочин» як неправомірне діяння, яке вчиняється за допомогою або виключно комп'ютером, комп'ютерною мережею, Інтернетом, інформацією, розміщеною в Інтернеті та інформаційними технологіями [7].

Якщо говорити про міжнародні організації, діяльність яких спрямована на запобігання злочинності та збереженню міжнародної безпеки, то лише Інтерпол дає певне означення кіберзлочинам. «Хоча не існує єдиного визначення кіберзлочину, правозостосовча практика вирізняє два типи таких злочинних діянь: високотехнологічний злочин – протиправне злочинне діяння проти комп'ютерного програмного та апаратного забезпечення, здійснене професіоналами, та традиційні кіберзлочини, які вчиняються за допомогою Інтернету: шахрайство, наприклад [8].

Члени ЄС у своїй практиці використовують визначення Європейської комісії, яка зазначає: «Кіберзлочини – це кримінальні діяння, які вчиняються online з використанням мереж електронних комунікацій та інформаційних систем» [9].

Одним з базових міжнародно-правових документів, який визначає види кіберзлочинів та покарання за них, є Конвенція про кіберзлочинність (2001), до якої приєдналась Україна в 2005 році. Хоча документ не дає визначення кіберзлочину, проте тут класифікуються такі злочинні діяння, процесуальні норми, принципи міжнародного співробітництва та рекомендації щодо запобігання. З огляду на те, що Конвенція є джерелом кримінального права та частково регулює поняття «кіберзлочину», це є додатковим аргументом для запровадження в українському законодавстві та доктрині терміну «кіберзлочин» [10].

Одним з нормативних актів в Україні, в якому вживається поняття кіберзлочинності, кіберпростору, кібербезпеки, є Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Документ визначає загрози кібербезпеці, суб'єктів забезпечення кібербезпеки, основні напрямки роботи щодо забезпечення кібербезпеки (серед яких «створення вітчизняної нормативно-правової та термінологічної бази у цій сфері, гармонізація нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО») [11].

Отже, можна зробити висновок, що термін «кіберзлочин», по-перше, є найбільш вдалим для використання в науці кримінального права та законодавстві через його універсальність: застосування в міжнародному кримінальному праві та у деяких вітчизняних нормативно-правових актах роблять його більш зрозумілим. По-друге, семантично «кіберзлочин» найбільш глибоко окреслює ті однорідні суспільні діяння, які посягають на об'єкти кримінально-правової охорони за допомогою різних інформаційних автоматизованих систем, замінюючи при цьому людину.

Тому, кіберзлочин – це суспільно небезпечне, протиправне діяння, яке вчинюється за допомогою штучних систем передачі інформації та місцем вчинення яких є простір, відмінний від матеріального світу (віртуальний світ).

Список використаних джерел:

1. Указ Президента України № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»

[Електронний ресурс] – Режим доступу: <http://www.president.gov.ua/documents/962016-19836>.

2. Samodulska M. CRIMES COMMITTED VIA THE INTERNET – SELECTED ASPECTS [Електронний ресурс] / Magdalena Samodulska – Режим доступу до ресурсу: <http://www.pan-ol.lublin.pl/wydawnictwa/TPraw7/Samodulska.pdf>.

3. Винер Н. Кибернетика, или управление и связь в животном и машине / Норберт Винер. – Москва: Наука, 1983. – 344 с. – (2).

4. Клаус Г. Кибернетика и философия / Георг Клаус. – Москва: Изд-во иностр. лит., 1963. – 531 с.

5. Глушков В. М. Кибернетика. Вопросы теории и практики / Виктор М. Глушков. – Москва: Наука, 1986. – 488 с.

6. Wall D. Cybercrime: The Transformation of Crime in the Information Age [Електронний ресурс] / David Wall – Режим доступу: https://books.google.com.ua/books?id=SiG-zE6yteMC&pg=PA8&hl=uk&source=gbs_toc_r&cad=4#v=onepage&q&f=false.

7. Jewkes Y. The SAGE Dictionary of Criminology [Електронний ресурс] / Yvonne Jewkes – Режим доступу: https://books.google.com.ua/books?id=SiG-zE6yteMC&pg=PA8&hl=uk&source=gbs_toc_r&cad=4#v=onepage&q&f=false.

8. Cybercrime [Електронний ресурс] – Режим доступу: <https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>.

9. Cybercrime [Електронний ресурс] – Режим доступу: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en.

10. Конвенція про кіберзлочинність [Електронний ресурс] – Режим доступу: http://zakon3.rada.gov.ua/laws/show/994_575.

11. Указ Президента України № 96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс] – Режим доступу: <http://www.president.gov.ua/documents/962016-19836>.

Войчишин А.О.

студент,

Науковий керівник: Демешко І.А.

викладач,

Олександрійський політехнічний коледж

НЕЗАКОННИЙ ОБІГ НАРКОТИКІВ

Незаконний обіг наркотиків – надзвичайно складне, різнобічне і водночас суспільно небезпечне явище у сучасному світі. З одного боку, наркотики є корисними і необхідними медичними препаратами, а з іншого – вони заподіюють величезну шкоду, яка практично не піддається обрахунку. Насамперед, це й деградація особистості наркомана, і потяг до вчинення різноманітних злочинів, і зниження матеріально-технічного та інтелектуального потенціалу суспільства, і погіршення його генофонду, і викривлення внаслідок «відмивання наркокоштів» законного розподілу матеріальних благ, і проникнення злочинців у державні та владні структури, і їхній вплив на формування політики держав у злочинних інтересах, і багато чого іншого. Незаконний обіг наркотичних засобів, психотропних речовин і прекурсорів – це діяння з: культивування рослин, включених до Переліку