

Біленчук Петро Дмитрович,

професор кафедри кримінального права та
процесу Національного авіаційного університету,
кандидат юридичних наук, доцент

Малій Микола Іванович,

директор юридичної компанії
ТОВ «АЮР-КОНСАЛТИНГ»

АКТУАЛЬНІ ПИТАННЯ КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ І КІБЕРБЕЗПЕКИ В НОВОМУ ТИСЯЧОЛІТТІ

В наш час людство переживає бурхливий розвиток електронної комп'ютеризації всіх сфер життя [1]. Це надає нові можливості розвитку національних економік [2]. Поширення інформаційних технологій має і свій негативний аспект: це відкриває шлях до антисоціальної та злочинної поведінки [3].

Сьогодні характерними рисами комп'ютерної злочинності є такі:
як правило, це міждержавний (транскордонний, транснаціональний, трансконтинентальний, планетарний) характер злочину (виходить за рамки кордону однієї держави);

труднощі у визначенні «місцезнаходження» злочину;
слабкі зв'язки між ланками в системі електронних доказів;
неможливість спостерігати і фіксувати електронні докази візуально;

широке використання злочинцями засобів шифрування електронної інформації [4].

Починаючи з 1991 року при Генеральному Секретаріаті Інтерполу діє Робоча Група з проблем комп'ютерної злочинності, яка вивчає цей вид злочинів в різних країнах світу, розробляє рекомендації, допомагає у стандартизації національних законодавств, напрацьовує методичний досвід запобігання і розслідування комп'ютерних злочинів.

На даний час в європейських країнах вже створені такі пункти, які надсилають інформацію до Генерального Секретаріату Інтерполу про результативність їх діяльності з запобігання і протидії кіберзлочинності. Ці пункти створені, як правило, в апараті Національних Бюро Інтерполу, або у спеціалізованих підрозділах, які займаються комп'ютерною злочинністю або економічними злочинами. На базі НЦБ Інтерполу в Україні такий пункт був також створений ще 17 вересня 1996 року.

Сучасна теорія і практика свідчить, що забезпечення належного технологічного рівня кібернетичної безпеки і удосконалення чинного законодавства є необхідною умовою подальшого розвитку Індустрії 4.0 та сучасного електронного суспільства [5]. Відомо, що в умовах глобалізації, автоматизації та кібернетизації інформаційних процесів, їх інтеграції в різні сфери державного і суспільного життя керівництво

провідних країн світу постійно приділяє особливу посилену увагу створенню та удосконаленню діяльності ефективних систем, засобів, методів та технологій захисту критичної інформаційної інфраструктури від зовнішніх і внутрішніх загроз кібернетичного характеру. Слід зазначити, що у багатьох провідних країнах світу вже сформовані і діють загальнодержавні системи кібернетичної безпеки критичної інфраструктури – як найбільш оптимальні організаційні структури, що здатні в короткий проміжок часу швидко акумулювати сили та засоби різних державних та правоохоронних органів і установ приватного сектору для протидії кіберзагрозам, кібератакам, кіберзлочинам, кібершпигунству, кібертероризму. В США, Великій Британії, Канаді довгий час діють потужні кіберполіцейські структури (NIPS, FBI, FATF і т.п.) [6]. Сьогодні в США, Польщі та інших країнах світу створюються навіть кібервійська.

Під кібернетичною безпекою розуміють стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток електронного інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом України «Про основні засади забезпечення кібербезпеки України», та іншими законами України. Загальна декларація прав людини, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України фактично закладають міцний міждержавний правовий, організаційний, процедурний фундамент забезпечення кібербезпеки інформаційного простору в Україні, Європі і світі.

Слідча і судова практика свідчить, що на даному етапі цивілізаційного розвитку світу виникають все нові і нові загрози, виклики і небезпеки в сфері критичної інформаційної інфраструктури держав, а також електронної інфраструктури відомств, установ і організацій [7; 8]. Це обумовлено тим, що постійно з'являються нові види міждержавних (транскордонних, транснаціональних, трансконтинентальних, планетарних) кіберзлочинів, які раніше взагалі не зустрічалися в слідчо-судовій практиці. Зокрема, це кіберзлочини, які уже сьогодні скоюються в світовому космічному просторі, а також кіберзлочини, які скоюються з використанням новітніх засобів, методів і технологій електронного інтелекту [9].

У сучасних умовах стрімкий розвиток інформаційних технологій в світі та необхідність обміну інформацією через використання глобальної інформаційної мережі інтернет створюють сприятливий клімат для злочинних посягань: привласнення коштів з банківських рахунків інших осіб, у тому числі і на території інших держав. Зокрема кібератаки, які здійснені на Пентагон та інші держустанови США, відключення систем електропостачання в Західних регіонах [10] України, блокування діяльності аеропорту у Варшаві тощо свідчить про реальні загрози світового масштабу. Беззаперечно, що кіберзлочини сьогодні вже набули транскордонного, транснаціонального, трансконтинентального, планетарного характеру, а тому міжнародна спільнота, враховуючи можливі глобальні негативні наслідки цього соціального явища, намагається постійно контролювати і мінімізувати їх посягання на міждержавні політичні, дипломатичні, економічні, екологічні відносини [11].

Список використаних джерел:

1. Біленчук П.Д. Е-суспільство: цифрове майбутнє України : монографія / П.Д. Біленчук, О.Л. Кобилянський, М.І. Малій та ін. ; за заг ред. П.Д. Біленчука. – 2-ге вид. переробл. – Київ: УкрДГРІ, 2019. – 292 с.
2. Біленчук П.Д. Електронна цивілізація: інноваційне майбутнє України : монографія / П.Д. Біленчук, М.М. Близнюк, О.Л. Кобилянський, М.І. Малій, Ю.О. Пілюков, О.В. Соболев ; за заг. ред. П.Д. Біленчука. – К. : УкрДГРІ, 2018. – 284 с.
3. Біленчук П.Д., Гуцалюк М.В., Кравчук О.В., Козир М.В. Комп'ютерний тероризм: суперхакери, кібертерористи, кіберкриміналісти : монографія. – Київ : Наука і життя, 2008. – 292 с.
4. Біленчук П.Д., Гуцалюк М.В., Романюк Б.В. та ін. Комп'ютерна злочинність : навч. посіб. – Київ : Атіка, 2002. – 240с.
5. Біленчук П.Д. Конвергенція сонячного суспільства знань: креативна освіта і цивілізаційний розвиток : монографія / П.Д. Біленчук, Я.О. Береський, О.Л. Кобилянський, М.І. Малій, Р.В. Перелігіна ; за заг.ред. П.Д. Біленчука. – К. :УкрДГРІ, 2019. – 416с.
6. Біленчук П., Малій М. Космічне партнерство України і США: Міжнародна правнича дипломатія в дії // Юридичний Вісник України. – 2019. – № 45. – С. 12–13.
7. Біленчук П.Д., Малій М.І. Електронне кримінальне провадження. Пріоритетні напрями цивілізаційного розвитку та можливості імплементації в Україні // Юридичний Вісник України. – 2019. – № 42–43. – С. 20–21.
8. Біленчук П.Д., Малій М.І. Електронне кримінальне провадження. Пріоритетні напрями цивілізаційного розвитку та можливості імплементації в Україні (Ч. 2) // Юридичний Вісник України. – 2019. – № 44. – С. 12.

9. Біленчук П., Малій М. Космічна й електронна кіберзлочинність: загрози і виклики нового тисячоліття // Юридичний Вісник України. – 2019. – № 41. – С. 14.

10. Біленчук П., Малій М. Кіберсвіт у новому тисячолітті. Хто вони: кіберзлочинці, кібершахраї, кібертерористи? // Юридичний Вісник України. – 2019. – № 39. – С. 14–15.

11. Біленчук П.Д., Малій М.І. Сучасні комп'ютерні злочинці та кібертерористи: новітні технології на службі організованого злочинного світу // Бизнес и безопасность. – 2019. – № 4. – С. 2–4.

Біляков Андрій Миколайович,

професор кафедри судової медицини та медичного права Національного медичного університету імені О. О. Богомольця, доктор медичних наук, професор

Ергард Наталія Миколаївна,

доцент кафедри судової медицини та медичного права Національного медичного університету імені О. О. Богомольця, кандидат медичних наук, доцент

Волобуєв Олександр Євгенович,

асистент кафедри судової медицини та медичного права Національного медичного університету імені О. О. Богомольця

ОСОБЛИВОСТІ СУДОВО-МЕДИЧНОЇ ЕКСПЕРТИЗИ ПРИ ВИЯВЛЕННІ МЕТАДОНУ

В останні роки в Україні набуває все більшого поширення програма метадонної терапії за рахунок коштів «Глобального фонду». 24 травня 2019 року Міністерством охорони здоров'я України (надалі – МОЗ України) було затверджено Наказ № 1177 «Про затвердження графіків розподілення лікарського засобу «Метадон-3Н» (метадону гідрохлорид – синтетичний, довготривалої дії агоніст опіїдних рецепторів) для проведення замісної підтримуючої терапії». Метою програми метадонної терапії є заміщення парентеральної форми введення наркотичних речовин на пероральне введення. Метадон вводиться в організм виключно пероральною формою, використовуючи або таблетовану форму метадону, або у вигляді сиропу. Обов'язковою умовою програми метадонної терапії є те, що дозування підбирають виключно індивідуально для кожного пацієнта з наркотичною залежністю, а також він особисто отримує метадон чітко за графіком розподілення та в присутності медичного персоналу приймає цей лікарський засіб.

В останній рік в Києві збільшились летальні випадки з виявленням слідів метадону в крові померлих осіб.