умовно вільні зразки; створювати умови для експертного дослідження, якщо воно проводиться за межами експертної установи, в якій працює експерт.

Забезпечення проведення експертиз не зводиться лише до зазначених дій слідчого та прокурора. Воно включає, крім суто процесуального, такі аспекти як організаційний, управлінський, фінансовий, інформаційний, технічний, кадровий та інші, забезпечувати які слідчий та прокурор не уповноважені, оскільки, навіть, не являють собою державні органи досудового розслідування чи прокуратури, в яких працюють.

Згідно із ст.ст.9, 11, 13 Закону «Про прокуратуру» представляти органи прокуратури у зносинах з державними установами, а до таких за ч.3 ст.7 Закону «Про судову експертизу» належать ті, що проводять судово-медичні і судово-психіатричні експертизи (тобто майже всі з обов'язкових) уповноважені їх керівники. Згідно зі ст. 39 КПК організація досудового розслідування покладається на керівників органів досудового розслідування, які також уповноважені представляти їхні інтереси у відносинах з іншими державними установами. Саме від керівників цих органів, а не слідчих і прокурорів залежить фінансове забезпечення витрат, пов'язаних із проведенням експертиз, реальний допуск експерта до об'єктів дослідження, які знаходяться за межами установи, в якій він працює, та створення інших умов для його праці. Щодо інших аспектів забезпечення проведення вказаних експертиз, то Закон «Про судову експертизу» їх покладає на керівництво державних спеціалізованих установ судової експертизи та експертних служб, що функціонують в системі юстиції, охорони здоров'я, оборони, СБУ, МВС та прикордонної служби.

Отже, ч.2 ст.242 КПК повинна починатися фразою: «Слідчий або прокурор зобов'язаний звернутися до експертної установи або експерта для проведення експертизи щодо:…»

Список використаних джерел

1. Фуллей Лон Л. Мораль права: пер. з англ. Н. Комарової. Наук. вид. – К.: Сфера, 1999. – 232 с.

Біленчук Петро Дмитрович,
професор кафедри кримінального права і процесу Національного авіаційного університету

Малій Микола Іванович,
директор юридичної компанії ТОВ «АЮР-КОНСАЛТИНГ»,
генеральний директор ТОВ «АРМАТЕХ-СЕРВІС»

ЕКСПЕРТНО-КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ЕЛЕКТРОННО-КОСМІЧНОЇ ЗЛОЧИННОСТІ

Протягом 1990-2019 років нами вивчаються питання пов’язані з бурхливим розвитком унікального феномена, відомого в усьому світі під назвою «кібертероризм», «кіберзлочинність», «комп’ютерна злочинність» [6]. На сьогоднішній день це поняття включає **всі протизаконні дії, при яких електронне опрацювання інформації було знаряддям їх скоєння або їх об’єктом** [7]. Таким чином у це коло проблем потрапили не тільки злочини, безпосередньо пов’язані з комп’ютерами, електронно-комунікаційними системами і мережами, але й такі, як шахрайство з кредитними магнітними картками, злочини у галузі телекомунікацій (шахрайство з оплатою міжнародних телефонних переговорів), незаконне використання банківської мережі електронних платежів, програмне «піратство», шахрайство з використанням ігрових автоматів та багато інших злочинів. До цієї групи також відносяться питання, пов’язані з використанням електронних доказів комп’ютерного походження, які використовуються при запобіганні і розслідуванні традиційних злочинів [1].

Нещодавно стало відомо, що NASA розслідує перший у світі злочин, який скоєний у космосі (космічному кіберпросторі). Підгрунтям розслідування цього злочину, скоєного в космічному просторі стало те, що екс-дружина американської жінки-астронавта заявила про злочин, вчинений на космічній орбіті Землі.

Зокрема, колишня дружина американського астронавта заявила, що її партнерка навіть після розлучення з нею продовжувала незаконно стежити за станом її особистих фінансових рахунків. При чому вона це здійснювала в тому числі під час виконання своєї професійної місії на Міжнародній космічній станції (МКС).

Про факт правового спору двох суб’єктів конфліктної ситуації, який, ймовірно, став першим злочином, скоєним в космосі, нещодавно повідомило The New York Times (https://www.nytimes.com/2019/08/23/us/nasa-astronaut-anne-mcclain.html).

В цьому повідомленні зазначається, що колишня дружина М. – офіцер повітряної розвідки США у відставці помітила, що хтось незаконно входить в її банківський аккаунт. Встановивши цей факт, вона звернулася в банк з проханням визначити комп’ютери, з яких здійснюється цей вхід. Як стало відомо, що одним з них виявився спеціальний комп’ютер, зареєстрований у мережі Національного управління з аеронавтики (NASA). У зв’язку з цим У. подала скаргу на незаконний вхід в її банківський акаунт у Федеральну торговельну комісію США.

Повернувшись на Землю, М. в показаннях під присягою, даних головному інспектору NASA, визнала, що дійсно здійснювала вхід, використовуючи пароль, яким подружжя користувалося раніше під час спільного життя. За словами адвоката астронавта, вона робила це, щоб

переконатися, що у У. і її чотирирічного біологічного сина, якого вони раніше виховували разом, досить коштів для існування. За словами М., колишня дружина жодного разу не казала їй, що заходити в її аккаунт їй тепер уже заборонено.

Слід зазначити, що згідно з чинними на Міжнародній космічній станції правилами, які спільно узгодили, встановили і підписали між собою Євросоюз, Канада, Росія, США і Японія, на астронавтів і космонавтів, які працюють на міжнародній космічній станції, при вирішенні виникаючих спірних юридичних питань то тут на них поширюється їх національне чинне законодавство [8]. Крім того, існує реальна правова можливість видачі злочинця на Землю в іншу країну, якщо там захочуть притягнути до відповідальності іноземця за злочин який скоєний у космосі.

Слід зазначити, що скарга, пов'язана з доступом до банку з космічної станції, є лише одним з ряду складних правових питань, що виникли в епоху звичайних космічних подорожей, які, як очікується, будуть зростати з початком широкомаштабних досліджень космічного простору, космічних подорожей фахівців (астронавтів, космонавтів) в тому числі і розвитку космічного туризму.

Випадки про різні криміногенні події, які відбувалися в космічному просторі відомі і раніше.

Так відомо, що ще у 2011 році НАСА організувало спецоперацію, спрямовану на вивчення дій вдови космічного інженера, яка хотіла продати місячний камінь. У 2013 році російський супутник був пошкоджений після зіткнення з уламками з супутника, зруйнованого Китаєм в ході випробування ракети в 2007 році. У 2017 році австрійський бізнесмен подав до суду на компанію з космічного туризму, намагаючись повернути свій депозит за заплановану поїздку, яка з різних причин була заблокована і не просувалася, тобто по факту не була реалізована.

Зокрема директор Центру глобального космічного права Клівлендського державного університету Марк Сундал справедливо зазначає так: «Те, що він знаходиться в космосі, не означає, що він не підкоряється закону».

За словами пана Сундала, однією з потенційних проблем, які можуть виникнути у зв'язку з будь-яким космічним кримінальним злочином або судовим процесом з приводу позаземних банківських комунікацій, є відкриття: вірогідно співробітники НАСА будуть побоюватися, наприклад, відкрити високочутливі комп'ютерні мережі і бази даних для перевірки пересічними юристами. Але такі юридичні питання в майбутньому, за його словами, будуть неминучі, оскільки в скорому часі люди будуть проводити більше часу в космосі. Про це свідчать активні космічні розробки під керівництвом Ілона Маска [2].

Розвиток наукових досягнень в новому тисячолітті засвідчує, що особливо небезпечним сьогодні є можливість використання кримінальними угрупуваннями електронного інтелекту в злочинних цілях. Як стало відомо засоби, методи і технології електронного інтелекту уже сьогодні несуть

загрозу соціально-комунікаційним системам і мережам. Зокрема, англійські і американські вчені справедливо стверджують, що електронний інтелект в скорому майбутньому може стати небезпечною зброєю в руках кібершахраїв, кібертерористів та кіберзлочинців. Про ці загрози, виклики і небезпеки зазначено в опублікованому днями стосторінковому дослідженні The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Тому очевидно, що постає справедливе запитання так в чому ж саме полягає реальна загроза світові з боку електронного інтелекту і як цьому реально зарадити?

Звіт, в якому висвітлюються реальні загрози електронного інтелекту для людства, був підготовлений групою з 26 провідних дослідників електронного інтелекту – відомих вчених Кембриджського, Оксфордського і Стенфордського університетів, а також експертів Electronic Frontier Foundation та OpenAI та представників інших авторитетних дослідницьких відомств, установ і організацій.

Реальна небезпека для електронної цивілізації полягає в тому, що сучасні можливості використання електронного інтелекту в освіті, науці і практиці стають більш могутніми, широкомаштабними і потужними [3;4;5]. У зазначеному вище дослідженні визначаються три основні напрями, для яких існує найбільше викликів, ризиків, загроз і небезпек – це цифрова (електронна) безпека, фізичні об’єкти та політична сфера.

Так в чому все ж таки полягає реальна небезпека для електронної цивілізації? Фахівці стверджують, що електронний інтелект, потрапивши в руки зловмисників, може фактично знизити , а інколи можливо і знищити реально створені захисні безпекові перешкоди, перепони для проведення руйнівних хакерських атак.

Відомо, що сучасні ноозасоби і ноотехнології електронного інтелекту уже сьогодні можуть виявити критичні помилки і недоліки програмного забезпечення та швидко вибирати потенційних жертв для скоєння різного роду фінансових та економічних злочинів. Більше того, ноозасоби електронного інтелекту можуть сприяти використанню соціальної інженерії як методу кібератаки. Це обумовлено тим, що інформація отримана з інтернету про персональні дані тої чи іншої людини може бути використана для автоматизованого створення шкідливих сайтів/посилань чи електронних листів, на які, швидше за все, відповідатиме потенційна жертва, адже вони надходитимуть вірогідно від справжніх людей та імітуватимуть їхній стиль спілкування», – стверджують фахівці, які підготували даний звіт.

Більше того подальший розвиток і удосконалення ноозасобів електронного інтелекту, на думку авторів даного дослідження, може призвести до того, що переконливі чат-боти зможуть долучати людей до тривалих діалогів, таким чином збільшуючи рівень довіри до себе, або навіть набувати вигляду реальних людей у відеочаті.

Іншою реальною небезпекою в кіберпросторі, яка з’являється на горизонті, це можливість кібератаки на фізичні об’єкти. Автори звіту

справедливо попереджають, що ноозасоби електронного інтелекту можуть безперешкодно проникати як у системи безпілотних автомобілів, так і безпілотних літаків, поїздів, кораблів, реально управляти ними та призводити по спеціальному коду для розкрадання майна, ресурсів, коштів, але і до аварій та катастроф. Ще одним прикладом може бути використання «армій дронів», які за допомогою технології розпізнавання обличчя можуть вбивати людей, наголошується у дослідженні. Таким чином існує реальна загроза створення роботів-вбивць.

У даному звіті також описується можливий сценарій, в якому робот-прибиральник офісів на ім'я SweepBot, який оснащений бомбою, проникає у міністерство фінансів та «губиться» серед інших машин такого ж виробника. Причому робот-зловмисник спочатку поводить себе достатньо ввічливо і природньо – збирає сміття, підмітає коридори, доглядає за вікнами, аж поки програма для розпізнавання обличчя не зафіксує певну особу зацікавлену зловмисниками і не запустить відповідний пусковий механізм вибухового пристрою. Очевидно, що прихований вибуховий пристрій може вбивати не тільки розпізнану певну особу, але і спричиняти поранення працівників, які можуть випадково стояти неподалік. Таким чином, швидкий розвиток індустрії електронного інтелекту засвідчує, що сьогодні це уже не просто науково-фантастична літературна історія-передбачення, а уже дійсно створена реальність, тобто конкретна технологічна небезпека і загроза цивілізаційного розвитку. Очевидно, що це все зобов'язує відповідні установи кібербезпеки уже сьогодні приступити до розробки стратегії, тактики і мистецтва поведінки в таких ситуаціях.

На завершення слід зазначити, що очевидно сформулювати реальний подальший чіткий розвиток сценаріїв використання можливостей космічного кіберпростору і електронного інтелекту в злочинних цілях сьогодні складно. Водночас, важливо уже сьогодні відповідним державним органам, освітнім та науковим установам приступити до розробки та реалізації на практиці наступних стратегічних кроків і прийняття управлінських тактичних рішень, а саме:

- створити чітку і надійну безпекову міждержавну правову базу можливостей використання космічного простору і електронного інтелекту в освітній, науковій і праксеологічній діяльності з метою запобігання і протидії можливим кіберзагрозам, викликам і небезпекам;

- розробникам новітніх електронних ноозасобів, методів і технологій штучного інтелекту технологічно запобігти можливим загрозам неправомірного використання електронного інтелекту в різних сферах життєдіяльності;

- розробити впорядковану правову, організаційну і технологічну систему запобігання і протидії шкідливому використанню космічного простору і електронного інтелекту як на національному, так і на міждержавному (світовому) рівнях.

Список використаних джерел

1. Біленчук П., Малій М. Кіберсвіт у новому тисячолітті. Хто вони: кіберзлочинці, кібершахраї, кібертерористи?//Юридичний Вісник України, 2019.-№39.-с.14-15.
2. Біленчук П., Малій М. Космічна й електронна кіберзлочинність: загрози і виклики нового тисячоліття//Юридичний Вісник України, 2019.-№41.-с.14.
3. 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.
4. 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. Соболєв, за заг. Ред. П.Д. Біленчука -К.: УкрДГРІ, 2018. -284 с.
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. Перелигіна; за заг.ред. П.Д. Біленчука.-К.:УкрДГРІ, 2019.- 416с.
6. Біленчук П.Д., Гуцалюк М.В., Романюк Б.В. та ін. Комп'ютерна злочинність. Навч. посіб. Київ: Атіка, 2002.-240с.
7. Біленчук П.Д., Гуцалюк М.В., Кравчук О.В., Козир М.В. Комп'ютерний тероризм: суперхакери, кібертерористи, кіберкриміналісти: Монографія. Київ: Наука і життя, 2008.-292с.
8. Біленчук П., Малій М. Космічне партнерство України і США: Міжнародна правнича дипломатія в дії//Юридичний Вісник України, 2019.-№45.-с.12-13.

Білозьоров Євген Вікторович,
заступник директора навчально-наукового інституту № 2 Національної академії внутрішніх справ, кандидат юридичних наук, доцент

МЕТОДОЛОГІЧНІ АСПЕКТИ ВИКОРИСТАННЯ ДІЯЛЬНІСНОГО ПІДХОДУ В КРИМІНАЛІСТИЦІ

На сьогодні розвиток юридичної науки обумовлений інтеграційними та глобалізаційними процесами, що відбуваються в Європі та світі, її переходом від методологічного монізму до світоглядно-методологічного плюралізму. Це, у свою чергу, викликає необхідність концептуального перегляду традиційних уявлень про державно-правові закономірності та поглибленого