УДК 343

І.М. Сопілко д.ю.н., професор, С.Я. Лихова д.ю.н., професор,
П.Д. Біленчук к.н.ю., доцент
(Національний авіаційний університет, Україна)

Космічний кіберзлочин як загроза національній безпеці України

В сучасному світі значного розвитку набувають кібертехнології в інформаційній сфері. Особливу загрозу несе їхнє суспільно небезпечне використання за допомогою космічних технологій. В статті розкриваються особливості впливу кібератак на національну безпеку України.

У сучасних умовах стрімкий розвиток інформаційних технологій в світі та необхідність обміну інформацією через використання глобальної інформаційної мережі інтернет створюють сприятливий клімат для наземних і космічних злочинних електронних посягань: привласнення коштів з банківських рахунків інших осіб, у тому числі і на території інших держав світу. Зокрема кібератаки, які здійснені на Пентагон та інші держустанови США, відключення систем електропостачання в Західних регіонах України, блокування діяльності аеропорту у Варшаві тощо свідчать про реальні електронні загрози світового маштабу. Беззаперечно, що кібервійни, кібератаки, кіберзлочини сьогодні вже набули транскордонного, транснаціонального, трансконтинентального, планетарного і сьогодні вже космічного характеру, а тому міжнародна спільнота, враховуючи можливі глобальні негативні наслідки цього надзвичайно небезпечного соціального явища, намагається постійно контролювати і мінімізувати їхні посягання на міждержавні політичні, дипломатичні, економічні, екологічні відносини [1, с.7].

З метою подолання таких надзвичайно небезпечних загроз у Європі був прийнятий базовий документ для запобігання і протидії міжнародній кіберзлочинності для європейських країн. Зокрема, це Конвенція Ради Європи про кіберзлочинність від 23.11.2001 р. та Додатковий протокол до неї від 28.01.2003 р. Сьогодні ця Конвенція є дієвим правовим фундаментом для розробки і удосконалення відповідного законодавства європейських держав. На наш погляд, ця Конвенція вже потребує удосконалення.

Що стосується космічної кіберзлочинності, то нещодавно стало відомо, що NASA розслідує перший у світі злочин, який вчинений у космосі (космічному кіберпросторі). Підгрунтям розслідування цього злочину, стало те, що потерпіла Н. заявила про злочин, вчинений на космічній орбіті Землі американською астронавткою.

Про цей факт правового спору двох суб'єктів конфліктної ситуації, який, ймовірно, став першим злочином, вчинений у космосі, нещодавно повідомило The New York Times [2].

Сьогодні вже відомі випадки про різні криміногенні події, які відбувалися в космічному просторі. 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 супутника, зруйнованого Китаєм в ході випробування ракети ще в 2007 році. У 2017 році австрійський бізнесмен подав до суду на компанію з космічного туризму, намагаючись повернути свій депозит за заплановану подорож, 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 зазначив, що якщо особа знаходиться в космосі, це не означає, що вона не підкоряється закону [3].

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 [3]. Про це свідчать активні космічні розробки під керівництвом Ілона Маска.

Реальною небезпекою в космічному кіберпросторі, яка вже сьогодні з'являється в нашому житті, є можливість кібератаки з космосу на фізичні об'єкти. Автори звіту «The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation» справедливо попереджають, що ноозасоби електронного інтелекту можуть безперешкодно проникати у системи безпілотних автомобілів, безпілотних літаків, поїздів, кораблів, реально управляти ними, призводити по спеціальному коду до розкрадання майна, ресурсів, коштів. Також ці засоби можуть призводити як до наземних, так і до космічних 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 як на Землі, так і в космосі роботів-вбивць [4].

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, яка цікавить зловмисників 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 світові установи з наземної та космічної кібербезпеки уже сьогодні приступити до розробки стратегії, тактики і мистецтва запобігання та протидії таким злочинам [4; 5, с.195-200].

Реалізуючи стратегічні завдання кібербезпеки нещодавно в Об'єднаних

Арабських Еміратах влада Дубая оголосила про створення космічного суду для врегулювання майбутніх правопорушень на орбіті Землі (Укрінформ, 19 березня 2021 року) [6].

На основі аналізу судової практики нами встановлений юридичний факт вчинення першого в Україні космічного кіберзлочину, який нещодавно вже розглянутий в українському суді (справа № 910/20546/20) [7].

Небезпечність вчинення космічних злочинів пов'язана з тим, що такі дії зловмисників можуть бути здійснені проти основ національної безпеки України (Розділ І Особливої частини КК України), проти миру, безпеки людства та міжнародного правопорядку (Розділ XX Особливої частини КК України). Тому очевидно, що космічний кіберзлочин, який розглядався в українському суді загрожує не тільки основам національної безпеки України, але і життю та здоров'ю особи (Розділ ІІ Особливої частини КК України). Об'єктом посягання кіберзлочинів можуть бути правовідносини у сфері господарської діяльності (Розділ VII Особливої частини КК України), громадська безпека (Розділ IX Особливої частини КК України), правовідносини у сфері охорони державної таємниці, недоторканості державних кордонів (Розділ XIV Особливої частини КК України), а особливо ці діяння небезпечні у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (Розділ XVI Особливої частини КК України). Очевидно, що в наш час такі космічні кіберзлочини особливо є небезпечними у сфері службової діяльності та професійної діяльності, пов'язаної з наданням публічних послуг (Розділ XVII Особливої частини КК України) і звичайно в період військових дій в Україні це правопорушення проти миру, безпеки людства та міжнародного правопорядку (Розділ XX Особливої частини КК України) [8, с.70-267].

Цей космічний кіберзлочин був вчинений вперше на території і в космічному просторі України та на територіях та в космічному просторі семи держав світу із використанням ряду міжнародних систем супутникового зв'язку та наземних станцій електрозв'язку в жовтні 2018 року.

Ці космічні кібератаки здійснювалися з інтервалом менше секунди та загальною тривалістю більше 24 годин (в період з 14 жовтня 2018 р. по 18 жовтня 2018 р.) на території Буркіна-Фасо, Сьєрра-Леоне, Мальдів, Сполучених Штатів Америки, Російської Федерації, Куби та України.

Як було встановлено в судовому засіданні, жодна служба кібербезпеки семи держав і телекомунікаційних установ (операторів космічних телекомунікацій, операторів магістральних телекомунікаційних мереж супутникового зв'язку, операторів наземних телекомунікаційних служб, в тому числі і державних органів семи країн світу: Буркіна-Фасо, Сьєрра-Леоне, Мальдів, Сполучених Штатів Америки, Російської Федерації, Куби та України) не здійснили відповідних безпекових заходів щодо протидії космічним кібератакам, кіберзагрозам здійснених в космічному кіберпросторі.

На завершення слід зазначити, що, очевидно, сформулювати реальний подальший чіткий розвиток сценаріїв використання можливостей космічного кіберпростору і електронного інтелекту в злочинних цілях наразі складно. Водночас, важливо уже сьогодні відповідним державним органам у всіх країнах світу, освітнім та науковим установам приступити до розробки та

реалізації на практиці таких стратегічних кроків і прийняття управлінських тактичних рішень, а саме:

- створити міждержавні умови з кібербезпеки космічного простору для гарантування конституційних прав та свобод людини і громадянина [5, с.47-55];

- створити чітку і надійну міждержавну кібербезпекову 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 кібербезпекових електронних ноозасобів, методів і технологій штучного інтелекту технологічно запобігти можливим загрозам неправомірного використання електронного інтелекту в різних сферах космічної 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 [9, с.78];

- створити об'єднання провідних електронних держав світу для формування безпекових стандартів надання електронних довірчих послуг [10, с.29-71].

Список літератури

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. NASA Astronaut Anne McClain Accused by Spouse of Crime in Space. URL: https://www.nytimes.com/2019/08/23/us/nasa-astronaut-anne-mcclain.html
3. Совершено первое преступление в космосе? URL: https://cripo.com.ua/scandals/soversheno-pervoe-prestuplenie-v-kosmose
4. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. URL: https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217
5. Електронне суспільство, електронне право, кібербезпека: стратегія розвитку інноваційної ери. Монографія / П.Д. Біленчук, О.Л. Кобилянський, М.І. Малій, Р.В. Перелигіна, Т.Ю. Тарасевич [та ін.]; за заг. ред. П.Д. Біленчука і Т.Ю. Тарасевич. К.: УкрДГРІ, 2020. 388 с.
6. ОАЕ створює перший у світі космічний суд. URL: https://www.ukrinform.ua/rubric-world/3183255-oae-stvorue-persij-u-sviti-kosmicnij-sud.html
7. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua
8. Кримінальний кодекс України: Закон України від від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
9. Біленчук П.Д., Борисова Л.В., Кобилянський О.Л., Собина В.О. Стратегія інформаційної безпеки України: правові засади захисту інформації: монографія. К.: УкрДГРІ, 2018. 288 с.
10. ІТ-сфера в Україні. Законодавство. Судова практика. Коментар. Київ. Юрінком Інтер, 2018. 360 с.