ПОВІТРЯНЕ, КОСМІЧНЕ, ЕКОЛОГІЧНЕ ПРАВО

DOI: 10.18372/2307-9061.59.15585
УДК 004.9:351.746.1(477)(045)

С. Я. Лихова,
доктор юридичних наук, професор
ORCID ID: https://orcid.org/0000-0003-4755-7474

П. Д. Біленчук,
кандидат юридичних наук, доцент
ORCID ID: https://orcid.org/0000-0002-9599-0347

КОСМІЧНІ І НАЗЕМНІ КІБЕРЗАГРОЗИ ТРЕТЬОГО ТИСЯЧОЛІТТЯ: ЗАСОБИ ПІЗНАННЯ, ДОКАЗУВАННЯ, РОЗСЛІДУВАННЯ

Національний авіаційний університет
проспект Любомира Гузара,1, 03680, Київ, Україна
E-mails: sofia.lykhova@gmail.com, aur.consalt@gmail.com

Мета: *аналіз феномену космічних і наземних кіберзагроз на основі використання новітніх засобів пізнання, доказування, розслідування.* ***Методологічну основу дослідження*** *склали загальнонаукові методи пізнання, за допомогою яких автори розв'язують питання пізнання, доказування, розслідування космічних електронних злочинів вчинених в кіберпросторі.* ***Результати:*** *автори наголошують на необхідності проведення спеціальних досліджень космічної кіберзлочинності, оскільки такі криміногенні явища загрожують національній безпеці України.* ***Обговорення:*** *автори констатують, що сучасний стан законодавчого врегулювання запобігання і протидії космічній кіберзлочинності є недостатнім, а тому потребує прийняття відповідних конвенцій і законів як на світовому рівні, так і на загальнодержавному рівні.*

Ключові слова: *космічна кіберзлочинність; електронний кіберпростір; кібербезпека.*

Постановка проблеми та її актуальність. У сучасних умовах стрімкий розвиток інформаційних технологій в світі та необхідність обміну інформацією через використання глобальної інформаційної мережі інтернет реально створюють сприятливий клімат як для наземних, так і космічних електронних злочинних посягань: незаконного доступу до державних та приватних комп'ютерних баз даних; баз даних фінансово-кредитних установ (внутрішніх банківських комп'ютерних систем); телефонних комунікацій; комп'ютерних систем підприємств; наукових установ і навчальних закладів; привласнення коштів з банківських рахунків інших осіб, у тому числі і на території інших держав світу. Нещодавні кібератаки, які здійснені на Пентагон, трубопровідні транспортні мережі та інші державні установи критичної інфраструктури США, відключення систем електропостачання в Західних регіонах України, блокування діяльності аеропорту у Варшаві тощо уже конкретно свідчать про реально існуючі наземні і космічні електронні загрози, ризики і небезпеки світового маштабу. Світова практика показує, що кібервійни, кібератаки, кібербулінг, кібертероризм, кіберзлочини в даний час вже набули не тільки транскордонного, транснаціонального, трансконтинентального, планетарного, але і космічного характеру [1]. Це зобов'язує міжнародну спільноту, враховуючи можливі глобальні негативні наслідки світового впорядкування цього надзвичайно небезпечного соціального явища, постійно аналізувати, моніторити такі зловмисні наміри та контролювати і мінімізувати їхні пося-

гання на державні та міждержавні правові, політичні, дипломатичні, освітні, наукові, економічні, екологічні, соціально-комунікаційні відносини.

Аналіз останніх досліджень і публікацій. Слід зазначити, що з метою подолання таких надзвичайно небезпечних загроз у Європі ще у 2001 році був прийнятий базовий правовий документ для запобігання і протидії міжнародному кібертероризму і кіберзлочинності на території європейських країн. Зокрема, була прийнята Конвенція Ради Європи про кіберзлочинність від 23.11.2001 р. та Додатковий протокол до неї від 28.01.2003 р. Очевидно, що сьогодні ця Європейська конвенція є потужним фундаментом і дієвим правничим документом для використання, подальшої розробки і удосконалення відповідного чільного законодавства в європейських країнах. На наш погляд дана Конвенція сьогодні вже теж потребує удосконалення новими ідеями, які обумовлені сучасними тенденціями цивілізаційного розвитку електронної комунікації в світі.

Відомо, що ряд провідних країн світу для забезпечення миру, безпеки людства та міжнародної безпеки цивілізації створили власні космічні відомства, установи і організації. Так, наприклад, у Сполучених Штатах Америки в 2019 році створено космічні сили. В Японії нещодавно створені космічні війська. В Україні довгий час вже діє Центр космічного спостереження.

Мета статті: наукова стаття присвячена аналізу космічних електронних загроз в сучасному кіберпросторі як об'єкта кримінологічного, кримінально-правового і криміналістичного системного мережевоцентричного дослідження.

Виклад основного матеріалу. Аналіз міжнародної судової практики свідчить про реальні факти виникнення космічної кіберзлочинності в світі. Зокрема, нещодавно стало відомо, що NASA розслідує перший у світі комп'ютерний злочин, який вчинений у космосі (космічному кіберпросторі). Підгрунтям розслідування цього комп'ютерного злочину, вчиненого в космічному кіберпросторі стало те, що потерпіла Н. заявила про космічний злочин, вчинений з космічної орбіти Землі американською астронавткою К., яка перебувала в той час на космічній станції.

Про цей реальний факт правового спору двох суб'єктів конфліктної ситуації, який, ймовірно, став одним з перших комп'ютерних злочинів, вчинених в космосі, нещодавно повідомило The New York Times [2].

Сьогодні органам правопорядку і громадськості вже стали відомі реальні випадки про вчинення різних криміногенних зловмисних дій, які відбувалися в космічному просторі. Так, наприклад, відомо, що, десять років тому, ще у 2011 році НАСА (Національне управління з аеронавтики і дослідження космічного простору (англ. National Aeronautics and Space Administration (NASA) організувало спецоперацію, спрямовану на вивчення неправомірних дій вдови космічного американського інженера, яка хотіла, порушуючи норми міжнародного космічного права, продати місячний камінь. А у 2013 році російський супутник зазнав аварії, оскільки був пошкоджений після його зіткнення з уламками з супутника, зруйнованого Китаєм в ході випробування космічної ракети ще в 2007 році. У 2017 році австрійський бізнесмен подав до суду на компанію з космічного туризму, намагаючись повернути свій депозит за заплановану ним поїздку, на космічному кораблі, яка з різних об'єктивних і суб'єктивних причин була заблокована і не просувалася, тобто по факту не була реалізована.

Аналізуючи різні ситуації, які відбуваються сьогодні в космічному просторі, директор Центру глобального космічного права Клівлендського державного університету США Марк Сундал на основі проведених досліджень зловмисних злочинних дій вчинених в космосі справедливо зазначає, що особа, яка знаходиться в космосі, не означає, що він не підкоряється закону» [3].

За словами Марка Сундала, однією з потенційних фактичних проблем, які можуть виникнути у зв'язку з будь-яким космічним карним злочином або космічним судовим процесом з приводу використання як наземних, так і позаземних банківських комунікацій, є відкриття закритих даних і вірогідно, що співробітники НАСА будуть побоюватися, наприклад, відкрити високочутливі режимні втаємничені комп'ютерні мере-

жі, автоматизовані системи і засекречені бази даних для перевірки звичайними, не допущеними до секретності юристами (слідчими, прокурорами, суддями, адвокатами та іншими правозахисниками). Але такі юридичні питання в майбутньому, за його словами, будуть звичайно неминучі, і потребуватимуть обов'язкових прозорих механізмів реалізації правовідносин, оскільки в скорому часі люди будуть проводити більше часу не тільки на Землі, але і в космосі [3]. Про це свідчать активні наукові дослідження і вже створені унікальні космічні розробки під керівництвом Ілона Маска [4] та інших провідних країн світу (Велика Британія, Індія, Китай, США, Об'єднані Арабські Емірати, Франція, Японія) [5].

Іншою реальною небезпекою вчинення зловмисних електронних дій в космічному електронному кіберпросторі, яка вже сьогодні реально з'являється на горизонті, це можливість електронної інформаційної кібератаки з космосу на наземні фізичні об'єкти. Автори звіту «The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation» справедливо попереджають, що сучасні ноозасоби і грід-технології електронного інтелекту дозволяють вже сьогодні безперешкодно проникати як у системи наземних установ і організацій, зокрема, безпілотних автомобілів, так і безпілотних літаків, поїздів, кораблів. Таким чином це дозволяє реально управляти ними по спеціальному коду з метою вчинення зловмисних дій, що сприяє реальній можливості здійснювати не тільки розкрадання майна, ресурсів, коштів, але також можливості вчинення і наземних, так і до космічних загроз у вигляді епідемій, аварій та катастроф. Ще одним небезпечним прикладом вчинення космічних чи електронних зловмисних дій може бути використання «армій дронів», які за допомогою новітніх грід-технологій розпізнавання обличчя, голосу, запаху, особливих рис поведінки можуть вбивати людей, наголошується у цьому дослідженні. Таким чином уже сьогодні існує реальна загроза створення і використання як на Землі, так і в космічному просторі (ближньому і дальньому) електронних роботів-вбивць. Про загрози для цивільної авіації незаконного застосування електронних засобів пишуть і сучасні вітчизняні автори [6, с. 28-33].

У цьому узагальненому науковому звіті також описується можливий сценарій, в якому електронний робот-прибиральник офісів на ім'я SweepBot, який оснащений спеціальною бомбою, проникає у міністерство фінансів та «губиться» серед інших автоматизованих керованих машин такого ж виробника. Причому даний електронний робот-зловмисник спочатку поводить себе в новому середовищі достатньо акуратно, ввічливо і природньо – збирає сміття, підмітає коридори, доглядає за вікнами, аж поки комп'ютерна програма для розпізнавання обличчя не зафіксує індивідуальні риси певної особи зацікавленої зловмисниками і не запустить код відповідного пускового електронного механізму вибухового пристрою. Очевидно, що інколи прихований вибуховий електронний пристрій може вбивати не тільки розпізнану зловмисником-роботом певну особу, але і спричиняти поранення працівників, які можуть випадково знаходитися поруч або неподалік. Таким чином, швидкий розвиток індустрії електронного інтелекту засвідчує те, що сьогодні це уже не просто науково-фантастична літературна історія-передбачення, а уже дійсно створена об'єктивна реальність, тобто існує конкретна технологічна небезпека і загроза подальшого цивілізаційного розвитку. Очевидно, що ці обставини зобов'язують відповідні світові і регіональні аналітичні установи з наземної та космічної електронної кібербезпеки уже сьогодні приступити до розробки і впровадження кібербезпекової стратегії, тактики і мистецтва запобігання та протидії таким електронним злочинам.

Відомо, що нещодавно з метою реалізації стратегічних завдань протидії космічній кіберзлочинності та формування надійної космічної кібербезпеки в Об'єднаних Арабських Еміратах влада Дубая оголосила про створення космічного суду для врегулювання майбутніх цивільних правовідносин та запобіганню правопорушень в космічному просторі на орбіті Землі. Питання правового регулювання інформаційної безпеки активно досліджує І.В. Поліщук [7, с. 27-32].

Дійсно, на сайті Міжнародного фінансового центру Дубая (DIFC) зазначається, що у 2021 році суди Міжнародного фінансового центру Дубая і Фонд майбутнього Дубая (DFF) приступили до

реалізації нової правничої ініціативи «Суди майбутнього», створюючи та впроваджуючи перший у світі космічний суд.

Таким чином, як повідомило агентство Укрінформ 19 березня 2021 року, ОАЕ дійсно уже приступило до фактичного створення першого у світі космічного суду.

В цьому повідомленні вказується, що новий арбітражний космічний суд буде спеціалізуватися на космічній діяльності в основному приватних компаній, на розбіжностях з приводу купівлі супутників або неправомірного зіткнення космічних пристроїв (космічних апаратів, супутників, міжнародних космічних станцій) на навколоземній орбіті. Таке рішення продиктоване прогресом в космічній галузі, який був досягнутий Об'єднаними Арабськими Еміратами в останні роки. Це обумовлено також і тим, що інші країни, такі як США, Китай розробили новітні проривні технології в космічній галузі. Зокрема відомо, що приватний підприємець Ілон Маск уже сьогодні контролює понад 25% супутників, які працюють в космічному просторі.

Слід також зазначити, що космічна галузь у світовому правничому контексті досліджується і регулюється міжнародним космічним правом. На даний час вся діяльність в космічному просторі регулюється міжнародними конвенціями та резолюціями, в тому числі Договором ООН щодо мирного використання космосу, який набрав чинності ще у 1967 році.

Зокрема відомо, що крім того деякі держави також підписали між собою двосторонні або багатосторонні угоди для забезпечення правового регулювання своєї космічної діяльності. Це обумовлено також і тим, що донедавна космічна сфера ближнього і дальнього космосу була фактично майже виключно прерогативою провідних країн світу і потужних державних організацій тільки деяких країн, а зараз же для засвоєння космічного простору залучаються уже і приватні компанії. Зокрема, в Україні теж ведуться творчі пошуки в даному напряму.

Факти вчинення зловмисних дій в космічному просторі відомі вже і в Україні. Так на основі консолідованого системного аналізу судової практики нашої країни нами встановлений юридичний факт вчинення першого в Україні космічного електронного кіберзлочину, який нещодавно (3 березня 2021 р.) вже розглянутий в українському суді [8].

Вважаємо, що небезпечність вчинення такого роду електронних космічних злочинів пов'язана з тим, що такі дії зловмисників несуть загрозу цивілізації, оскільки можуть бути здійснені як проти миру, безпеки людства, так і реально впливати на міжнародний правопорядок (Розділ XX КК України). Очевидно, що космічний електронний кіберзлочин, який нещодавно розглядався в українському суді, на наш погляд, загрожує не тільки основам національної безпеки України (Розділ I КК України), але і направлений проти життя та здоров'я особи (Розділ II КК України), проти волі, честі, гідності та ділової репутації особи (Розділ III КК України), проти приватної, комунальної і державної власності (Розділ VI КК України). Фактично такі дії зловмисників небезпечні також і у сфері господарської діяльності (Розділ VII КК України), оскільки направлені проти громадської безпеки (Розділ IX КК України) та особливо небезпечні у сфері охорони державної таємниці, недоторканості державних кордонів (Розділ XIV КК України), і сьогодні надзвичайно небезпечними у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (Розділ XVI КК України). На нашу думку, в еру електронної асиметричної комунікації такі космічні електронні кіберзлочини особливо є небезпечними також і у сфері службової діяльності та професійної діяльності, пов'язаної з наданням публічних послуг (в тому числі і електронних послуг) (Розділ XVII КК України) і, звичайно, є небезпечними в період здійснення військових дій агресором проти України, оскільки це правопорушення направлене проти миру, безпеки людства та міжнародного правопорядку (Розділ XX КК України).

Системний мережевоцентричний аналіз надання зловмисникам електронних послуг показав, що вони здійснювалися з допомогою систем супутникового зв'язку EMSAT, ORATION TECHNOLOGIES і супутникової технології на базі міжнародної супутникової мережі

GLOBALSTAR, а також наземних станцій електрозв'язку.

Відомо, що система супутникового зв'язку EMSAT (європейська система мобільного супутникового зв'язку) забезпечує голосовий і факсимільний зв'язок, передачу даних і повідомлень (SMS), визначення координат місця розташування об'єкту (GPS) з точністю до 30 метрів на території всієї зони обслуговування. EMSAT введена в експлуатацію ще в 1999 році і складається з одного геостаціонарного супутника Italsat F2 (крапка стояння 16,48 с.д.), що забезпечує обслуговування всіх європейських країн, північної частини Африки й Азії. До складу наземного сегмента входить базова станція, розташована в м. Ларіо (Італія, оператор мережі Telespazio), що управляє доступом абонентів до космічного сегменту і забезпечує сполучення EMSAT з наземними мережами загального користування.

Що стосується супутникової технології, яка реалізована на базі супутникової мережі Globalstar, що використовувалася для надання якісних послуг, то вона прагне зберегти зв'язок передового досвіду як провідний глобальний постачальник надійних комерційних супутникових рішень, що використовуються на наших дорогах, водних шляхах та віддалених місцевостях у всьому світі. Звертаємо увагу, що супутникові рішення Globalstar забезпечуються власною мережею супутників, які постійно працюють та мають високу надійність.

Важливим є і те, що сучасна технологія Globalstar щодня пов'язує людей завдяки надійному супутниковому зв'язку через надзвичайно чітку та безпечну супутникову мережу. Супутники Globalstar забезпечують надійність та працездатність у всьому світі, що з'єднує користувачів у районах, де традиційні мережі ненадійні або недоступні. Його супутникові продукти оснащують мережу послугами передачі голосу та даних, комерційними можливостями відстеження та обміну повідомленнями IoT та SPOT Business, які обслуговують безліч компаній, робітників та любителів активного відпочинку у віддалених програмах для бізнесу та розваг.

Відомо, що подібно до «зігнутих труб» або дзеркал на небі супутники Globalstar вловлюють сигнали з більш ніж 80% поверхні Землі. Супутники Globalstar передають сигнали клієнтів за допомогою технології CDMA до антен на відповідному наземному шлюзі, потім сигнали передаються через локальні мережі. Цей високоефективний дизайн пропонує найкоротший час затримки підключення і дозволяє Globalstar модернізувати наземну і супутникову системи за допомогою новітніх технологій на місцях.

Слід зазначити, що нове супутникове сузір'я Globalstar Orbit (LEO) та наземна інфрастуктура нового покоління забезпечують виняткову якість та надійність покриття і якісне обслуговування клієнтів.

Причому 24 наземні станції Globalstar слугують мостом між супутниками LEO та традиційно комунікаційною інфраструктурою на шести континентах. Цей зв'язок забезпечує зв'язок із понад 120 країнами світу. Наземна інфраструктура нового покоління базується на конфігурації мультимедійної підсистеми протоколу інтернету (IMS), що дозволяє інженерам супутникової мережі постійно адаптуватися до мінливих потреб користувачів.

Фактично послуга, що надається Globalstar працює далеко за межі наземних мереж, щоб забезпечити якісний трафік багатьом компаніям і працівникам, які працюють за межами періодичного або недоступного стільникового покриття.

Додатково наголошуємо, що всесвітня навігаційна система GPS (Global Positioning System), яка базується на використанні 24 штучних супутників Землі, що виведена на орбіту американським космічним відомством NASA за програмою NAVSTAR дозволяє наглядати (як всевидяче пильне око) за особливо дорогими об'єктами, які зацікавлюють криміналітет (наприклад, прогресивними пересувними військовими об'єктами, надзвичайно дорогими автомобілями марок «Мерседес», «Ягуар» чи «Порш»). Фактично об'єкт, обладнаний апаратурою GPS, перебуває під постійним наглядом системи всевидячого космічного ока і його місцезнаходження може бути кожної миті визначене у будь-якій точці земної кулі з точністю від 20 до 100 метрів. Водночас, координати військових об'єктів і спеціальних комплексів

(ядерних, ракетних пересувних машин), обладнаних більш дорогими приладами спостереження, можуть визначатися з точністю до кількох сантиметрів. Причому, це означає, що будь-який пересувний комплекс, автомобіль у будь-якій ситуації може бути зупинений одним лише телефонним дзвінком.

Ці супутники перебувають на 6 орбітах висотою близько 17 000 км над поверхнею Землі. Супутники постійно рухаються зі швидкістю близько 3 км/с, роблячи два повних оберти навколо нашої планети менш, ніж за 24 години. Кожен супутник важить більш як 900 кг і має розмір між крайніми точками (з розкритими сонячними батареями) близько 5 м. Перший з них був запущений у лютому 1978 року. На супутниках установлені радіопередавачі потужністю 50 Вт, що випромінюють сигнали на 3-х частотах. Для цивільних GPS-приймачів виділена частота 1575,42 МГц. Працездатність супутника зберігається протягом 10 років.

Однією з найважливіших переваг GPS перед наземними системами, що існували раніше, є незалежність від погоди. Незалежно від того, для яких цілей використовується навігація, GPS-приймач готовий показати місцерозташування конкретного об'єкта саме тоді, коли про це поступає запит.

Спрощено система GPS може бути описана в такий спосіб: кожен супутник передає сигнал, який, образно говорячи, повідомляє, що він – супутник X, зараз він займає положення Y, це повідомлення було відправлене в час Z. Звичайно, це сильне спрощення, але воно допоможе зрозуміти ідею неспеціалістам. GPS-приймачу досить мати сигнали від трьох супутників, щоб визначити широту і довготу (двомірна фіксація). Якщо ж супутників буде чотири чи більше, приймач зможе визначити положення об'єкта в тримірному просторі, тобто обчислити його широту, довготу і висоту. Постійно відслідковуючи місце розташування об'єкта протягом певного часу, GPS-приймач зможе досить точно визначити швидкість і напрямок руху наземного об'єкта (наприклад, автомобіля).

Важливо акцентувати увагу ще і на тому, що вказаний вище перший космічний кіберзлочин був вчинений не тільки на наземній території і космічному просторі України, але і на наземних територіях та космічних просторах загалом семи держав світу (причому на різних континентах) з допомогою використання потужних інструментів міжнародних систем супутникового зв'язку (європейської системи мобільного супутникового зв'язку EMSAT, глобальної ORATION TECHNOLOGIES, а також супутникової технології на базі міжнародної супутникової мережі GLOBALSTAR) та наземних станцій електрозв'язку ряду країн світу в жовтні 2018 року. Цікаво, що даний трафік кібератак здійснювався посекундно понад 24 години підряд.

Цікавим є і те, що ці наземні і космічні електронні кібератаки здійснювалися з інтервалом інколи до секунди, а в більшості випадків тривалістю від однієї, двох, трьох, чотирьох та більше секунд та загальною тривалістю електронного кібернападу більше 24 годин (в період з 14 жовтня 2018 р. по 18 жовтня 2018 р.) на території як Буркіна-Фасо, Сьєрра-Леоне, Мальдів, Сполучених Штатів Америки, Російської Федерації, Куби, так і України. Також, слід зазначити, що за одну секунду сьогодні технологічно можливо передавати 1440 кілобайт інформації, а за двадцять чотири години цей показник складає значно більшу кількість передаваних відомостей, даних тощо.

Як було встановлено в судовому засіданні, жодна служба кібербезпеки не зацікавилася дією електронних зловмисників, оскільки не виявила, не задокументувала і не здійснила відповідних технологічних безпекових заходів щодо протидії цим космічним кібератакам, кіберзагрозам, кіберзлочинам здійснених в наземному і космічному кіберпросторі в період з 14 жовтня 2018 р. по 18 жовтня 2018 р.

Висновки. Підводячи підсумки викладеного слід зазначити, що очевидно сьогодні сформулювати конкретний дієвий прогноз подальшого чіткого розвитку реальних сценаріїв використання технологічних можливостей електронного наземного і космічного кіберпростору, а також електронного інтелекту в зловмисних цілях як теоретично, так і практично достатньо складно та проблематично. Водночас, вважаємо, що важливо уже сьогодні відповідним безпековим міжнародним органам світу (ООН, ОБСЄ, ЮНЕСКО,

ФАТФ, МПА, Інтерполу, Європолу) та окремих державних установ (Великої Британії- Мі-5, Мі-6; США – АНБ, ЦРУ, ФБР; України – РНБО та інших країн), освітнім та науковим установам (університетам, інститутам, академіям, коледжам, безпековим науково-дослідним інститутам) приступити до розробки та реалізації в освіті, науці і на практиці наступних стратегічних кроків і прийняття відповідних безпекових управлінських тактичних рішень, а саме:

– розробити міждержавні стандарти з метою забезпечення кібербезпеки наземного та космічного кіберпростору для гарантування невідчужуваних та непорушних конституційних прав та свобод людини і громадянина;

– розробити Генеральною Асамблеєю ООН та прийняти чітку і надійну міждержавну кібербезпекову правову базу (Конвенцію ООН) реальних можливостей використання наземного і космічного кіберпростору (ближнього і дальнього) та електронного інтелекту в освітній, науковій і праксеологічній діяльності з метою запобігання і протидії можливим електронним кіберзагрозам, кібератакам, кіберзлочинам кібервикликам і кібернебезпекам;

– акцентувати увагу розробників новітніх кібербезпекових електронних ноозасобів, креативних методів і грід-технологій електронного інтелекту на те, що необхідно технологічно запобігти та протидіяти можливим кіберзагрозам неправомірного використання космічного простору і електронного інтелекту в різних сферах наземної та космічної життєдіяльності;

– відповідним міжнародним безпековим організаціям, відомствам і установам світу розробити впорядковану правову, організаційну і технологічну систему запобігання і протидії шкідливому використанню космічного простору і електронного інтелекту як на національному, регіональному, так і на міждержавному (світовому) рівнях (транскордонному, транснаціональному, трансконтинентальному, планетарному, космічному (близький космос, далекий космос));

– створити міжнародне об'єднання потужних провідних електронних держав світу для формування, розробки і впровадження єдиних безпекових стандартів надання електронних довірчих послуг на всій земній кулі [9, с. 29-71];

– забезпечити впровадження в космічну діяльність новітніх розробок у галузі кібербезпеки, здійснених науковцями Національного авіаційного університету спільно з Інститутом електронної фізики НАН України, Національним космічним агентством України та правничою компанією «АЮР-КОНСАЛТИНГ» [10].

Література

1. Біленчук П.Д., Малій М.І. Космічна й електронна кіберзлочинність: загрози і виклики нового тисячоліття. *Lexinform*: веб-сайт. 2019. URL: https://lexinform.com.ua/dumka-eksperta/ kosmichna-j-elektronna-kiberzlochynnist-zagrozy-i-vyklyky-novogo-tysyacholittya/

2. NASA Astronaut Anne McClain Accused by Spouse of Crime in Space. The New York Times: веб-сайт. URL: https://www.nytimes.com/ 2019/08/23/us/astronaut-space-investigation.html

3. Совершено первое преступление в космосе? URL: https://cripo.com.ua/scandals/sovershenо-pervoe-prestuplenie-v-kosmose/

4. Ешлі Венс. Ілон Маск. Tesla. Spase X і шлях у фантастичне майбутнє. Пер. з англ. Мирослави Лузіної. Вид. 5. Київ: Вид. ФОП Фористина О.В., 2017. 416 с.

5. Шваб Клаус. Четверта промислова революція. Харків. 2019. 416 с.

6. Sopilko I.M., Bezzubov D.O. Accidents on board an aircraft: goals and objectives of the investigation. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. Київ: НАУ, 2019. № 4(53). С. 28-33.

7. Поліщук І.В. Особливості правового регулювання інформаційної безпеки в цивільній авіації України. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. Київ: НАУ, 2020. № 2 (55). С. 27-32.

8. Сопілко І.М., Лихова С.Я., Біленчук П.Д. Космічний кіберзлочин як загроза національній безпеці України. Матеріали XV Міжнародної науково-технічної конференції «АВІА-2021». Київ: НАУ, 2021. URL: http://conference.nau.edu.ua/ index.php/AVIA/AVIA2021/paper/view/8017/6667

9. ІТ-сфера в Україні. Законодавство. Судова практика. Коментар. Київ. Юрінком Інтер, 2018. 360 с.

10. Меморандум про співробітництво між Національним авіаційними університетом та правничою компанією ТОВ «АЮР-КОНСАЛТИНГ» (23 жовт. 2019 р.); Біленчук П.Д., Малій М.І. Пріоритетні напрями досліджень психологічного портрету електронного зловмисника. Актуальні проблеми психологічного забезпечення службової діяльності працівників правоохоронних органів: зб. тез Міжнар. наук.-практ. конф. (м. Київ, 30 жовтня 2020 р.). Київ: ДНДІ МВС України, 2020. 267 с.

References

1. Bilenchuk P.D., Malii M.I. Kosmichna y elektronna kiberzlochynnist: zahrozy i vyklyky novoho tysiacholittia. *Lexinform*: veb-sait. 2019. URL: https://lexinform.com.ua/dumka-eksperta/kosmichna-j-elektronna-kiberzlochynnist-zagrozy-i-vyklyky-novogo-tysyacholittya/

2. NASA Astronaut Anne McClain Accused by Spouse of Crime in Space. The New York Times: veb-sait. URL: https://www.nytimes.com/2019/08/23/us/astronaut-space-investigation.html

3. Soversheno pervoe prestuplenye v kosmose? URL: https://cripo.com.ua/scandals/sovershenо-pervoe-prestuplenie-v-kosmose/

4. Eshli Vens. Ilon Mask. Tesla. Spase X i shliakh u fantastychne maibutnie. Per. z anhl. Myroslavy Luzinoi. Vyd. 5. Kyiv: Vydavets FOP Forystyna O.V., 2017. 416 s.

5. Shvab Klaus. Chetverta promyslova revoliutsiia. Kharkiv. 2019. 416 s.

6. Sopilko I.M., Bezzubov D.O. Accidents on board an aircraft: goals and objectives of the investigation. *Naukovi pratsi Natsionalnoho aviatsiinoho universytetu. Seriia: Yurydychnyi visnyk «Povitriane i kosmichne pravo»*. Kyiv: NAU, 2019. № 4 (53). S. 28-33.

7. Polishchuk I.V. Osoblyvosti pravovoho rehuliuvannia informatsiinoi bezpeky v tsyvilnii aviatsii Ukrainy. *Naukovi pratsi Natsionalnoho aviatsiinoho universytetu. Seriia: Yurydychnyi visnyk «Povitriane i kosmichne pravo»*. Kyiv: NAU, 2020. № 2 (55). S. 27-32.

8. Sopilko I.M., Lykhova S.Ia., Bilenchuk P.D. Kosmichnyi kiberzlochyn yak zahroza natsionalnii bezpetsi Ukrainy. Materialy KhV mizhnarodnoi naukovo-tekhnichnoi konferentsii «AVIA-2021». Kyiv: NAU, 2021. URL: http://conference.nau.edu.ua/ index.php/AVIA/AVIA2021/paper/view/8017/6667

9. IT-sfera v Ukraini. Zakonodavstvo. Sudova praktyka. Komentar. Kyiv. Yurinkom Inter, 2018. 360 s.

10. Memorandum pro spivrobitnytstvo mizh Natsionalnym aviatsiinymy universytetom ta pravnychoiu kompaniieiu TOV «AIuR-KONSALTYNH» (23 zhovtnia 2019 r.); Bilenchuk P.D., Malii M.I. Priorytetni napriamy doslidzhen psykholohichnoho portretu elektronnoho zlovmysnyka. Aktualni problemy psykholohichnoho zabezpechennia sluzhbovoi diialnosti pratsivnykiv pravookhoronnykh orhaniv: zb. tez Mizhnar. nauk.-prakt. konf. (m. Kyiv, 30 zhovtnia 2020 r.). Kyiv: DNDI MVS Ukrainy, 2020. 267 s.

S. Lykhova, P. Bilenchuk

SPACE AND TERRESTRIAL CYBER THREATS OF THE THIRD MILLENNIUM: MEANS OF COGNITION, EVIDENCE, INVESTIGATION

National Aviation University
Liubomyra Huzara Avenue, 1, 03680, Kyiv, Ukraine
E-mails: sofia.lykhova@gmail.com, aur.consalt@gmail.com

Purpose: *analysis of the phenomenon of space and ground cyber threats based on the use of the latest means of cognition, proof, investigation.* ***The methodological basis*** *of the research was general scientific methods of cognition, with the help of which the authors solve the issues of cognition, proof, investigation of space electronic crimes committed in cyberspace.* ***Results:*** *the authors emphasize the need for special research on space cybercrime, as such criminogenic phenomena threaten the national security of Ukraine.* ***Discussion:*** *the authors state that the current state of legislation on the prevention and counteraction of space cybercrime is insufficient, and therefore requires the adoption of relevant conventions and laws both at the global level and at the national level. The authors suggest the following:*

– to develop interstate standards to ensure the cybersecurity of terrestrial and space cyberspace to guarantee inalienable and inviolable constitutional rights and freedoms of man and citizen;

– to develop by the UN General Assembly and to adopt a clear and reliable interstate cybersecurity legal framework (UN Convention) of real opportunities for the use of terrestrial and space cyberspace (near and far) and electronic intelligence in educational, scientific and practical activities to prevent and counter cyber threats, cybercrime, cybercalls and cyber hazards;

– to focus the attention of developers of the latest cybersecurity electronic tools, creative methods and grid technologies of electronic intelligence on the need to technologically prevent and counteract possible cyber threats of misuse of outer space and electronic intelligence in various spheres of terrestrial and space life;

– relevant international security organizations, agencies and institutions of the world to develop an orderly legal, organizational and technological system to prevent and combat harmful use of outer space, and electronic intelligence at the national, regional and interstate (global) levels (transboundary, transnational, transcontinental, planetary, space) (near space, far space));

– to create an international association of powerful leading electronic states of the world for the formation, development and implementation of common security standards for the provision of electronic trust services around the globe;

– to ensure the introduction into space of the latest developments in the field of cybersecurity carried out by scientists of the National Aviation University in conjunction with the Institute of Electronic Physics of the National Academy of Sciences of Ukraine, the National Space Agency of Ukraine and the law firm AUR-CONSULTING.

Keywords: *space cybercrime; electronic cyberspace; cybersecurity.*