DOI: 10.18372/2307-9061.60.15950
УДК 343.326:004.056.53(045)

В. В. Філінович,
кандидат юридичних наук
ORCID ID: https://orcid.org/0000-0001-8824-615X

КІБЕРБЕЗПЕКА ТА ЗАГРОЗИ АВІАЦІЙНІЙ СФЕРІ: ПРАВОВИЙ АСПЕКТ

Національний авіаційний університет
проспект Любомира Гузара, 1, 03680, Київ, Україна
E-mail: vvfilinovich@gmail.com

Мета: *дослідити особливості та сучасний стан кібернетичної безпеки в авіаційній сфері та правові можливості її захисту.* ***Методи дослідження:*** *застосовувалися загальновизнані методи наукового пізнання, а саме: аналітичний, порівняльно-правовий, системно-структурний та інші.* ***Результати:*** *досліджено поняття, суть, характеристики і особливості кібербезпеки в авіаційній сфері, вказано на проблеми захисту об'єктів критичної інфраструктури, авіаперевізників та пасажирів та надано пропозиції щодо подолання таких проблем.* ***Обговорення:*** *дискусія у дослідженні присвячена пошуку шляхів вирішення проблеми забезпечення надійного рівня кібербезпеки в авіаційних комп'ютерних системах і мережах та необхідності гармонізації вітчизняного законодавства з даного питання із міжнародними стандартами.*

Ключові слова: *кібербезпека; цивільна авіація; інформаційна безпека; кіберпростір; кіберзлочини; кібератака.*

Постановка проблеми та її актуальність. Сьогодні більшість із нас вже не уявляє свого життя без інформаційних технологій. Вони використовуються повсюдно – в усіх сферах суспільного взаємодії, у т.ч. в авіації. Таке використання зазначених благ не позбавлене ряду проблем, особливо щодо безпеки. Кіберзагрози зазвичай мають транснаціональний характер і справляють відповідний вплив як на національному, регіональному, так і на міжнародному рівнях.

Цивільна авіація сьогодні не може існувати поза кібербезпекою. В іншому випадку застосування сучасних технологій і розробок е транспортному полі не матиме сенсу. Погодьтеся, термін «кібертероризм» знайомий більшості людей на планеті.

Сучасна цивільна авіація використовує широку комп'ютерну взаємопов'язану систему: це і аеронавігаційні системи, і системи управління повітряними суднами, і зв'язок з аеропортами тощо. Таким чином, у всьому простежується вплив і залежність від цифровізації, що, в свою чергу, таїть в собі таку проблему як складність у прогнозуванні можливих ризиків, так як має місце взаємодія між людьми і системами.

Всесвітньо відома і визнавана Міжнародна організація цивільної авіації (також – ІКАО, від англ. *ICAO – International Civil Aviation Organization*) розробляє і впроваджує міжнародні норми цивільної авіації, допомагає країнам реалізувати особливу Стратегію кібербезпеки. В даному напрямку співпрацюють й інші суб'єкти. Таким чином, захист критично важливої інфраструктури, інформаційно-комунікаційних систем і даних цивільної авіації від кібернетичних загроз сьогодні вийшли на перший план як для окремо взятих держав, так і для світової спільноти в цілому.

Аналіз досліджень і публікацій. Окремі науково-теоретичні розробки з даного питання були здійснені такими науковцями як Р. Аткінсон, П.Д. Біленчук, Т. Кіслінг, С.Я. Лихова, І.В. Поліщук, І.М. Сопілко, Е. Укванду, Н.В. Філик, Х. Хінді, Ю. Циглер та іншими.

Мета статті. В даному науковому дослідженні автор ставить за мету дослідити та проаналізувати сучасний стан кібернетичної безпеки в авіаційній сфері, визначити особливості правового регулювання вказаного напрямку та надати власні рекомендації щодо його покращення та вдосконалення.

Виклад основного матеріалу. Як уже згадувалося, із приходом і активним використанням інформаційно-комунікаційних технологій в авіаційній сфері підвищилась ефективність функціонування цивільної авіації та, одночасно, виник цілий пул вразливостей і потенційних загроз у даній сфері. Сьогодні існує безліч документів із безпеки авіації, проте ризики з кожним днем стають все істотнішими. Судіть самі: маючи в своєму розпорядженні комп'ютер і open source-програму, а також володіючи якщо не базовими, то досить середніми навичками хакинга, студент-бакалавр без особливих зусиль зможе декодувати сигнали з аеронавігаційних пристроїв. Що ж говорити в такому випадку про «досвідчених» хакерів, яким для злому супутникової навігації і систем зв'язку достатньо кількох хвилин. І це далеко не єдина проблема даної сфери. Саме тому як уряди окремих країн, так і іменити організації докладають чимало зусиль для забезпечення кібернетичної безпеки у сфері критичної інфраструктури.

Для початку розберемо поняття кібербезпеки. Відзначимо, що єдиного підходу до його визначення не існує. Так, наприклад, А.Т. Танггал розглядає цей термін як стан або процес захисту, а також відновлення пристроїв, мереж, комп'ютерних систем і програмного забезпечення (далі – ПЗ) при кібератаці будь-якого типу [1].

Н. Кагалвалла і П. Чурі розглядають досліджуваний нами концепт як спосіб захисту комп'ютерних систем від загроз на кшталт вірусів [3].

Українське законодавство в особі Закону України від 05.10.2017 № 2163-VIII (стаття 1) визначає кібербезпеку як захищеність життєво важливих інтересів людей і громадян, самої держави і її суспільства при взаємодії в кіберпросторі. При цьому повинно бути забезпечено як розвиток цифрового комунікаційного середовища, так і інформаційного суспільства, а разом з ними – виявлення і протидію можливим і цілком реальним загрозам нацбезпеки нашої держави у кіберпросторі [2].

Таким чином можна зробити висновок, що кібербезпека передбачає здійснення дій, спрямованих на управління ризиками в кібернетичному просторі. І здійснюють їх як окремі компанії, так і цілі уряди для захисту конфіденційності, правдивості та доступності інформації та різних активів у кіберпросторі.

Варто розуміти й те, що ж таке взагалі авіація і безпосередньо цивільна авіація. Як вказує І.С. Похиленко, авіація є діяльність юридичних осіб будь-якої організаційно-правової форми, метою якої є створення і використання повітряного простору людьми за допомогою використання літаків та інших літальних апаратів [5, с. 17]. Також для цілей даного дослідження візьмемо за основу підхід до поняття «цивільна авіація», запропонований Е. Укванду, Х. Хінді та іншими, який має на увазі опис категорії невійськових за своїм характером польотів (як приватних, так і комерційних). Зазначене включає в себе всі аспекти авіаційної екосистеми і авіоніки, в т.ч. управління повітряним рухом, авіакомпанії і аеропорти [4].

Варто розуміти, що кібербезпека є одним із видів або навіть стовпів інформаційної безпеки. І.В. Поліщук так визначає її з точки зору цивільної авіації: це стан захищеності аеронавігації та безпеки польотів, так само як і забезпечення повноти надання даних при обслуговуванні повітряного руху та авіапасажирів. І при такому стані будь-які неправомірні дії по використанню інформації не завдають відчутної шкоди діяльності суб'єктів авіаційного поля у процесі використання відповідних об'єктів [6, с. 29].

Таким чином, інформаційні системи і технології стали невід'ємною частиною авіаційної екосистеми. Відзначимо, що у 2018 році було проведено дослідження, в ході якого зроблено аналіз наявної практики щодо кібербезпеки в цивільній і військовій авіаційній промисловості США. В ході зазначеного було встановлено, що хоча уряд Федерального управління аеропортів (FAA) і приватні суб'єкти усіма силами намагаються стри-

мувати величезний масив кібератак, але цього недостатньо. Також потрібні додаткові дії щодо введення запобіжних заходів проти подібних загроз у процесі розробки, використання і обслуговування авіаційних навігаційних систем [4].

Наголосити на важливості підтримання належного рівня кібернетичної безпеки можна за допомогою наступних наглядних прикладів нещодавніх атак в авіаційній сфері.

Stuxnet. У 2009-2010 роках мережевий вірус Win32/Stuxnet вразив персональні пристрої і автоматизовані системи управління виробництвом за допомогою внесення змін до потоку даних промислових підприємств і аеропортів. Вважається, що основною метою кіберзлочинців були іранські заводи із виробництва збагаченого урану, атакувавши які можна було нанести удар по усьому ядерному проекту. Підсумок: заражені 200 тис. пристроїв, Іран мусив позбутися тисячі центрифуг для збагачення уранового палива.

Comac C919. Як сказано в звіті експертної групи Crowdstrike, за 2010-2015 роки китайське міністерство держбезпеки, за допомогою послідовної координації дій кіберзломщиків і взаємодії з інсайдерами з авіаційних і аерокосмічних корпорацій, здобуло інформацію про секретні проекти у сфері інтелектуальної власності. Останні були потрібні для розробки Китаєм особливо потужного літака, не вдаючись до поставок поза межами країни.

WannaCry. У травні 2017 року кібератаці піддалися комп'ютери, що використовували операційну систему Microsoft Windows. Особливий вірус (програма-вимагач) WannaCry впливав на так звану вразливість «zero-day», зашифровуючи дані на заражених комп'ютерах, після чого жертвам пропонували заплатити за розшифровку. Вперше виявлений в Іспанії, вірус серйозно «вдарив» і по українських системах, негативно вплинувши на роботу банків і аеропортів. Загальна сума завданих збитків склала $ 1 млрд, при цьому постраждали більше 500 тис. комп'ютерів у 150 державах.

Petya, NotPetya і ExPetr. У червні того ж року кібератакам піддалися корпоративні мережі компаній і державних служб по всій земній кулі. Маючи кілька назв, вірус Petya, що базувався на кодах хакерського угруповання Equation, також шифрував дані (базу даних) про всі файли на диску пристрою, після чого пропонував оплатити розшифровку за допомогою біткоінів. Саме Україна найбільше постраждала від цієї проблеми, була порушена робота понад 300 організацій, в т.ч. аеропорту Бориспіль, Приватбанку, Запоріжжяобленерго, Київстару та інші. Загальна сума завданих збитків склала понад $ 10 млрд.

British Airways. Даний авіаперевізник був оштрафований на значну суму в 183 мільйони фунтів стерлінгів через допущений витік даних, у результаті якого понад півмільйона персональної інформації авіапасажирів було викрадено. Дане правопорушення було скоєне з використанням шахрайського веб-ресурсу.

Cathay Pacific. Ця гонконгська авіакомпанія у тому ж 2018 році також пережила кібератаку. В ході неї особисті дані 9,4 мільйонів користувачів були вкрадені.

EasyJet. У кінці січня 2020 року компанія зіткнулася із кібератакою, в ході чого адреси електронної пошти близько 9 мільйонів її клієнтів були розкриті, а разом з ними і дані банківських карт понад 2 тисяч осіб.

Sunburst. Про цю кібератаку, що торкнулася тисячі організацій по всьому світу і відому як «найнебезпечніша кібератака в історії Америки» вперше заявили 13 грудня 2020 року. Від дій кіберзлочинців постраждали такі суб'єкти як НАТО, Казначейство і Держдеп США, Європейський парламент, Microsoft, а також представники авіаційного сектору [7; 8, с. 31.2].

Таким чином, проблема полягає в тому, що практично будь-який авіапасажир літака, маючи на руках мобільний пристрій із інтернет-доступом (або навіть без нього), може підключитися до систем судна, при цьому його практично до останнього не викриють. Так само як подібний доступ до систем повітряного авіалайнера може дістати суб'єкт, що не знаходиться на борту, а лише підключився до смартфону будь-якого пасажира і впровадився у такий спосіб у системи судна. Зазначене дає практично необмежені можливості для різних терористичних організацій вести незаконні, а часом і вельми не-

безпечні дії, які можуть призвести до людських жертв. Звернемо увагу на те, що порушення правильного функціонування хоча б одного навігаційного вузла, наприклад, що відповідає за параметри на пульті управління пілота, здатне негативно впливати на можливість успішної посадки літака, а це, знову таки, людські жертви.

Варто відзначити, що військова авіація, у порівнянні з цивільною, сьогодні більш захищена, проте дійсно 100-відсоткових дієвих методів щодо забезпечення кібербезпеки не існує і тут. Справа у тому, що сучасні дрони і військовий авіатранспорт – це набір електронних компонентів, які скеровуються не стільки людиною, скільки спеціальною програмою. Відповідно, умілий хакер може зламати її і внести зміни в програмне забезпечення. Таким чином, кібератаки здатні повністю змінити хід ведення бойових дій.

Відповідно, проблема забезпечення кібербезпеки в авіації зараз актуальна як ніколи. Це змусило як приватні компанії, так і уряди країн, і міжнародні організації вживати заходів для забезпечення необхідного рівня авіаційної кібербезпеки. Так, у 2019 році в рамках 40 сесії Асамблеї ІКАО була прийнята Резолюція А40-10 про кібербезпеку у цивільній авіації. Суть її зводилася до проголошення важливості взаємного вирішення проблем, що виникають у полі авіаційної кібербезпеки. Асамблея, в тексті Резолюції А40-10, закликала ІКАО та країни-учасниці усіма засобами сприяти прийняттю і втіленню в життя Пекінської конвенції про боротьбу з незаконними актами по відношенню до міжнародної цивільної авіації та Протоколу до Конвенції про боротьбу із незаконним захопленням повітряних суден, вважаючи вказане дієвим способом протистояти кібератакам. Також зазначеним суб'єктам слід здійснювати наступні заходи з протидії кіберзагрозам у даній сфері: прийняти і виконувати стратегію кібербезпеки; організувати державно-галузеві партнерства і механізми як на національному, так і на міжнародному рівнях, в рамках чого обмінюватися інформацією щодо кіберзагроз, превентивних заходів та інцидентів, що вже мали місце; розробити принципи і залучити ресурси для забезпечення структурної безпеки систем і їх стійкості, способів передачі даних, так само як і впровадити методи моніторингу систем і виявлення інцидентів із наступним поданням повідомлень про вказане; передбачити і виявити загрози і ризики, які виникають в результаті авіаційних кіберінцидентів; систематично проводити судово-криміналістичний аналіз інцидентів в галузі кібернетичної безпеки; всіляко заохочувати вироблення загального розуміння країнами-учасницями суті і небезпеки кіберзагроз, ризиків, параметрів визначення важливості об'єктів, які потребують забезпечення захисту, так само як і координацію дій між державними органами і галуззю при розробці політики та планів щодо забезпечення кібернетичної авіаційної безпеки; визначити список завдань і обов'язків національних органів та інших зацікавлених сторін з даного питання тощо [9].

Відзначимо, що в ході зазначеного заходу отримав схвалення Глобальний план авіаційної безпеки (від англ. ICAO GLOBAL AVIATION SECURITY PLAN, також – GASEP). Його учасниками стали 160 держав світу. Основною метою GASEP є задоволення потреб країн-учасниць у підвищенні рівня безпеки авіаперельотів за допомогою взаємодії із зацікавленими сторонами не на локальному, а саме на глобальному рівні. План передбачає, що міжнародне співтовариство буде вести скоординовані дії, щоб досягти п'яти пріоритетних результатів: 1) підвищити обізнаність про кібернетичні ризики та загрози і забезпечити адекватне і своєчасно реагування на них; 2) удосконалити технологічні ресурси і впровадити інновації; 3) зробити нагляд і контроль якості більш дієвими; 4) впровадити культуру безпеки і підвищити рівень людського потенціалу; 5) розширити межі співпраці і надати більш об'ємну підтримку [10].

Отже, з огляду на все вищевикладене, перед державами постало серйозне випробування щодо забезпечення захисту цивільної авіації, оскільки будь-яке втручання ззовні може легко призвести до непоправних наслідків.

Висновки. Сьогодні практично жодна сфера людської діяльності не обходиться без використання інформаційних технологій. Це твердження

однаково можна застосувати і до авіаційного сектору. Але повсюдна інформатизація стала приводом для зловмисників «перевіряти» системи на міцність, зазвичай з метою наживи. Таким чином кібератаки стали звичайною справою. Для аерокосмічної галузі ця проблема особливо актуальна, адже хакерські зловмисні дії дають злочинцям можливість проникати в комп'ютерні системи і мережі не тільки комерційних компаній, але й організацій критичної інфраструктури, а потім – підривати їх діяльність або контролювати її.

Більшість країн світу, стурбовані цим питанням, активно впроваджують нові методи по виявленню можливих кіберзагроз. Проте знати про існуючу загрозу – це лише частина справи, ніяк не обійтися без вироблення відповідних методів захисту. З точки зору технічного забезпечення популярним є використання спеціальних дублюючих систем, незалежно працюючих одна від одної, хоча, безумовно, цілковита безпека не гарантується. Не менш важливим є відмежування систем літаків від імовірного втручання ззовні, наприклад шляхом ізолювання обладнання від бортових систем, а також проходження звірки даними, які передають екіпажу судна із землі. Також на регулярній основі кожен авіаперевізник повинен проводити офіційну оцінку ризиків.

Що стосується правового захисту, то необхідна розробка та удосконалення наявних нормативно-правових актів щодо забезпечення своєчасного запобігання, виявлення і реагування на кібератаки. Щоб розробити ефективну структуру кібербезпеки в авіаційній сфері, необхідно виконати такі дії-кроки: 1) гармонізувати національне законодавство із міжнародними стандартами; 2) оцінити і забезпечити належне розуміння безпосередніх небезпек і ймовірних атак; 3) постійно проводити дослідження і втілювати в життя особливі розробки; 4) забезпечити своєчасне та адекватне реагування на кіберінциденти; 5) визначити дієві принципи авіаційного проектування і експлуатації повітряних суден; 6) встановити і застосовувати загальні кіберстандарти і правила щодо авіаційних систем для зниження ризиків; 7) активно використовувати методи, рекомендовані ІКАО щодо забезпечення безпеки польотів; 8) обмінюватися інформацією про виклики та загрози з питань кібербезпеки в ході симпозіумів та конференцій.

Що ще можна зробити:

- розвивати культуру кібернетичної безпеки серед працівників сфери, тобто забезпечити просування позитивної культури кібербезпеки і підвищення обізнаності в галузі, для чого проводити тренінги і семінари із залученням фахівців як з авіаційної та інформаційної сфери, так і з освітньо-дослідного сектора;

- вести комунікацію і співпрацю з усіма зацікавленими сторонами (учасники авіаційної галузі та зовнішні організації) для цілей розробки передових методів і управління потенційними вразливостями;

- підвищити довіру і забезпечити транспарентність – необхідно встановити і впровадити єдиний глобальний підхід до кібербезпеки.

На закінчення відзначимо, що тільки сукупність зазначених дій, як технічних, так і правових, економічних і соціально-орієнтованих, здатна забезпечити захист авіаційних комп'ютерних систем і мереж від сучасних загроз і викликів кібербезпеки.

Література

1. Tunggal A.T. Why is Cybersecurity Important? Abi Tyas Tunggal. UpGuard. 2021. URL: https://www.upguard.com/blog/cybersecurity-important.

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовт. 2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

3. Kagalwalla N. and Churi P.P. Cybersecurity in aviation: an intrinsic review. 2019. 5th International conference on computing, communication, control and automation (ICCUBEA). Pp. 1-6. DOI: 10.1109/ICCUBEA47591.2019. 9128483.

4. Cyber-security challenges in aviation industry: a review of current and future trends / E. Ukwandu, M.B. Amine, H. Hindy etc. Cornell University, 2021. № 1. P. 1–25.

5. Похиленко І.С. Поняття авіаційної діяльності. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «По-*

вітряне і космічне право». Київ: НАУ, 2019. № 3(52). С. 15-19. DOI: https://doi.org/10.18372/2307-9061.52.13928

6. 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. DOI: https://doi.org/10.18372/2307-9061.55.14771

7. Зуйкова А. Десять самых громких кибератак XXI века. *РБК*. 2021. URL: https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e.

8. Filinovych V. Cybersecurity gaps as a problem of modern aviation: legal aspect. Международная научно-техническая конференция «АВИА», North America, apr. 2021. URL: http://conference.nau.edu.ua/index.php/AVIA/AVIA2021/ paper/ view/ 7995/6631. Date accessed: 10 Aug. 2021.

9. Резолюции Ассамблеи ИКАО. 40-я сессия. Монреаль: Международная организация гражданской авиации, 2019. 174 с. URL: https://www.icao.int/Meetings/a40/Documents/Resolutions/a40_res_prov_ru.pdf

10. ICAO Global aviation security plan (GASeP). ICAO. 2017. URL: https://www.icao.int/Security/Pages/Global-Aviation-Security-Plan.aspx.

References

1. Tunggal A.T. Why is Cybersecurity Important? Abi Tyas Tunggal. UpGuard. 2021. URL: https://www.upguard.com/blog/ cybersecurity-important.

2. Pro osnovni zasady zabezpechennja kiberbezpeky Ukrai'ny: Zakon Ukrai'ny vid 05 zhovt. 2017 r. № 2163-VIII. *Vidomosti Verhovnoi' Rady Ukrai'ny*. 2017. № 45. St. 403.

3. Kagalwalla N. and Churi P.P. Cybersecurity in aviation: an intrinsic review. 2019. 5th International conference on computing, communication, control and automation (ICCUBEA). Pp. 1-6. DOI: 10.1109/ICCUBEA47591.2019. 9128483.

4. Cyber-security challenges in aviation industry: a review of current and future trends / E. Ukwandu, M.B. Amine, H. Hindy etc. Cornell University, 2021. № 1. P. 1–25.

5. Pohylenko I.S. Ponjattja aviacijnoi' dijal'nosti. *Naukovi praci Nacional'nogo aviacijnogo universytetu. Serija: Jurydychnyj visnyk «Povitrjane i kosmichne pravo»*. Kyi'v: NAU, 2019. № 3(52). S. 15-19. DOI: https://doi.org/10.18372/2307-9061.52.13928

6. Polishhuk I.V. Osoblyvosti pravovogo reguljuvannja informacijnoi' bezpeky v cyvil'nij aviacii' Ukrai'ny. *Naukovi praci Nacional'nogo aviacijnogo universytetu. Serija: Jurydychnyj visnyk «Povitrjane i kosmichne pravo»*. Kyi'v: NAU, 2020. № 2(55). S. 27-32. DOI: https://doi.org/10.18372/2307-9061.55.14771

7. Zujkova A. Desjat' samyh gromkih kiberatak XXI veka. *RBK*. 2021. URL: https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e.

8. Filinovych V. Cybersecurity gaps as a problem of modern aviation: legal aspect. Международная научно-техническая конференция «АВИА», North America, apr. 2021. URL: http://conference.nau.edu.ua/index.php/AVIA/AVIA2021/ paper/ view/ 7995/6631. Date accessed: 10 Aug. 2021.

9. Rezoljucii Assamblei IKAO. 40-ja sessija. Monreal': Mezhdunarodnaja organizacija grazhdanskoj aviacii, 2019. 174 s. URL: https://www.icao.int/ Meetings/ a40/Documents/ Resolutions/a40_res_prov_ru.pdf

10. ICAO Global aviation security plan (GASeP). ICAO. 2017. URL: https://www.icao.int/ Security/Pages/Global-Aviation-Security-Plan.aspx.

Valeria Filinovych

CYBERSECURITY AND THREATS TO THE AVIATION SECTOR: LEGAL ASPECT

National Aviation University
Liubomyra Huzara Avenue, 1, 03058, Kyiv, Ukraine
E-mail: vvfilinovich@gmail.com

Today information technologies are used everywhere – in all spheres of social interaction, including and in aviation. This use of the benefits mentioned is not without several problems, especially concerning security. Cyber threats are usually transnational and have a corresponding impact at both the national, territorial, and international levels. Civil aviation today cannot exist outside of cybersecurity. Otherwise, the use of modern technologies and developments in the transport field will not make sense, especially in connection with the growing problem of cyber terrorism.

Purpose: *to study the features and current state of cybersecurity in the aviation sector and the legal possibilities for its protection.* ***Research methods*** *that were used during the research are generally recognized methods of scientific knowledge, namely: analytical, comparative-legal, systemic and structural, and others.* ***The results:*** *the concept, essence, characteristics, and features of cybersecurity in the aviation sector were studied, the problems of protecting critical infrastructure facilities, air carriers, and passengers were pointed out, and suggestions for overcoming such problems were presented.* ***Discussion****: the discussion in the study is devoted to finding ways for solving the problem of ensuring a reliable level of cybersecurity in aviation computer systems and networks and the need to harmonize domestic legislation on this issue with international standards.*

Analysis of recent studies and publications made it possible to point to individual scientific and theoretical works of such scientists as R. Atkinson, P. Bilenchuk, T. Kisling, S. Lykhova, I. Polishchuk, I. Sopilko, E. Ukvandu, N. Filyk, H. Hindi, Y. Tsigler and others.

Most countries in the world are concerned about maintaining an adequate level of cybersecurity in the aviation sector. Therefore, they are actively introducing new methods to identify possible cyber threats. However, knowing about the existing threat is only part of the matter; we cannot do without developing appropriate methods of protection. There is a set of technical means of protection used in this area, but they do not give a 100% guarantee. Concerning legal protection, it is necessary to develop new and improve the existing regulatory legal acts to ensure timely warning, detection, and response to cyber-attacks. To develop an effective cybersecurity framework in the aviation sector, it is necessary, inter alia, to harmonize national legislation with international standards; ensure timely and adequate response to cyber incidents; establish and apply common cyber standards and aviation systems regulations to mitigate risks; actively use the methods recommended by ICAO to ensure flight safety and not only. In the opinion of the author of the study, trying to solve the problem under consideration using only one sectoral method will not lead to success, which is why it is important to use a mixture of technical and legal, and socioeconomic means.

Keywords: *cybersecurity; civil aviation; information security; cyberspace; cybercrime; cyberattack.*