DOI: 10.18372/2307-9061.68.17969
УДК 343.326:004.056.53(045)

Є. В. Криволап,
здобувач вищої освіти третього (освітньо-наукового) рівня
ORCID ID: https://orcid.org/0000-0003-2599-2520

Ю. Л. Юринець,
доктор юридичних наук, професор
ORCID ID: https://orcid.org/0000-0003-0281-3251

Л. М. Бєлкін,
кандидат технічних наук, старший науковий співробітник, адвокат
ORCID ID: https://orcid.org/0000-0001-8672-8147

ПИТАННЯ НЕЙТРАЛІЗАЦІЇ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ЦИВІЛЬНОЇ АВІАЦІЇ: ПРАВОВИЙ АСПЕКТ

Національний авіаційний університет
проспект Любомира Гузара, 1, 03058, Київ, Україна
E-mail: belkinleonid@ukr.net

Метою *статті є дослідження сучасних підходів до правового регулювання у сфері виявлення, нейтралізації та управління вразливостями інформаційно-комунікаційних систем, у тому числі – цивільної авіації.* ***Методи дослідження:*** *документальний аналіз, узагальнення правової інформації, інформації із сфери кіберзахисту інформаційно-комунікаційних систем, а також практики кіберзахисту інформації від різноманітних кібератак.* ***Результати:*** *встановлено, що у найбільш концентрованому вигляді під вразливістю системи слід розуміти нездатність системи протистояти реалізації певної загрози або сукупності загроз, що особливо небезпечно на авіаційному транспорті. У зв'язку із цим питання протидії кіберзагрозам стає предметом спеціальної уваги в авіаційній сфері, у тому Міжнародної організації цивільної авіації (ІКАО), а також інших міжнародних організацій у сфері авіаційного транспорту (Міжнародна асоціація повітряного транспорту (ІАТА), Міжнародна координаційна рада асоціацій космічної промисловості (ІККАІА) тощо). В Україні законом затверджена Державна Програма авіаційної безпеки цивільної авіації. Разом із тим, підсилення кібербезпеки на авіаційному транспорті здійснюється в контексті запровадження загальних методів та принципів кібербезпеки. Важливим кроком запровадження в Україні системи нейтралізації вразливостей слід вважати законодавче врегулювання процедур Bug bounty – тестування електронних сервісів із залученням зовнішніх фахівців, яке дає можливість виявити вразливі місця і недоліки в програмних продуктах. Регулювання здійснюється Порядком пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, затвердженим постановою Кабінету Міністрів України від 16.05.2023 р. № 497.* ***Обговорення:*** *удосконалення правового регулювання у сфері виявлення, нейтралізації та управління вразливостями інформаційно-комунікаційних систем, у тому числі цивільної авіації, сприятиме підвищенню безпеки цивільної авіації.*

Ключові слова: *кібербезпека; кібератака; критична інфраструктура; вразливість; комп'ютерні мережі.*

Постановка проблеми та її актуальність. Сьогодні практично жодна сфера людської діяльності, у тому числі й цивільна авіація, не обходиться без використання інформаційних технологій. Але повсюдна інформатизація стала приводом для зловмисників атакувати комп'ютерні інформаційні системи. Таким чином кібератаки стали звичайною справою [1, с. 41-42]. Отже, цивільна авіація сьогодні не може існувати поза кібербезпекою [1, с. 38]. Автори статті [2] наводять відомості про те, що протягом 2006-2018 рр. авіаційна галузь у світі зазнала мінімум 12 значущих кібернетичних атак [2, с. 26-27]. Зазначається, що Україна вперше зазнала кібернетичної атаки на комп'ютерні системи та центральний сервер аеропортів Борисполю та Харкова у червні 2017 р. За оцінкою фахівців Європейського агентства з безпеки польотів (EASA), протягом 2019 року авіаційні системи світу щомісяця піддавалися кібератакам до 1000 разів [2, с. 27].

В літературі описаний випадок, коли стороння особа зламала систему розваг у польоті (IFE) у літаку та перезаписала код на комп'ютері керування тягою літака під час перебування на борту. Зловмисник зміг віддати команду набору висоти і змусити літак ненадовго змінити курс, йдеться в статті [3]. В подальшому ця особа пояснювала ФБР, що у такий спосіб тестувала електронні системи управління літаком на вразливість.

Загрози інформаційній безпеці проявляються не самостійно, а через можливу взаємодію з найбільш слабкими ланками системи захисту, тобто через фактори уразливості. Загроза призводить до порушення діяльності систем на конкретному об'єкті-носії [4, с. 99].

Вказані загрози в авіаційній сфері спонукали зайнятися цією проблемою Міжнародну організацію цивільної авіації (ІКАО). Організацією, зокрема, розроблений План дій із забезпечення кібербезпеки (січень 2022 року) [5]. У пункті 1.3.1 Плану вказано, що загрози для кібербезпеки набувають все більш поширеного характеру, тому це питання займає одне з центральних місць при обговоренні та аналізі ризиків та вразливості в рамках системи цивільної авіації. Визначено, що вразливість – це слабка ланка в інформаційній системі, процедурах забезпечення безпеки системи, внутрішніх засобах контролю чи процесі реалізації, що може бути використано чи викликано суб'єктом загрози. Це може бути система, яка прямо або опосередковано підтримує функціонування авіаційної системи. Серед засадничих елементів стратегії кібербезпеки визначене, зокрема, дійове законодавство і нормативні положення.

Отже, дослідження правових аспектів питань нейтралізації вразливостей інформаційно-комунікаційних систем цивільної авіації є актуальним.

Аналіз досліджень і публікацій з проблеми. Специфічні питання проблем вразливості інформаційно-комунікаційних систем цивільної авіації досліджені недостатньо. Разом із тим, велике значення для вирішення цих проблем мають дослідження забезпечення кібербезпеки в широкому сенсі. Актуальність кібернетичної безпеки в авіаційній галузі загострилася через всебічне використання мережі «Інтернет» та бездротового зв'язку [2, с. 25]. Бездротові мережі, на відміну від дротових, надзвичайно вразливі до можливих атак і несанкціонованого доступу [6, с. 99]. Проведені дослідження показали, що в даний час існують об'єктивні причини появи вразливостей в системному програмному забезпеченні. Одним з актуальних питань, пов'язаних із захистом програмного забезпечення, залишається оцінка його вразливості та нейтралізації останньої [7, с. 141]. У монографії [8], зокрема, сформульовані напрямки забезпечення безпеки польотів: метод оцінки рівня «забрудненості» баз даних авіаційних операторів; заходи з виявлення найбільш вразливих елементів безпеки авіаційної діяльності; захист уразливих елементів шляхом розробки рекомендацій щодо забезпечення безпеки польотів; комплекс моделей і методів оцінки достовірності вхідної інформації [8, с. 152]. У західній системі кібербезпеки вважається, що той факт, що IT-менеджери або вище керівництво знають, що IT-системи та програми мають вразливості, і не роблять нічого, щоб запобігти IT-ризику, розглядається як проступок в більшості законодавств [9]. Таким чином, питання нейтралізації вразливостей інформаційно-комунікаційних си-

стем, зокрема, в цивільної авіації, повинно ґрунтуватися на міцному фундаменті національного законодавства, що інтегровано у міжнародну систему. Окремі питання управління вразливістю розглянуто у статті співавтора [10].

Виклад основного матеріалу дослідження. Протягом 2020-2021 рр. в Україні прийнята низка безпекових стратегій України, зокрема: Стратегія національної безпеки України від 14.09.2020 р., затверджена Указом Президента України від 14.09.2020 р. № 392/2020; Стратегія інформаційної безпеки від 15.10.2021 р. (Указ від 28.12.2021 р. № 685/2021); Стратегія кібербезпеки України від 14.05.2021 р. (Указ від 26.08.2021 р. № 447/2021). Ключовою у системі наведених безпекових Стратегій є Стратегія національної безпеки України від 14.09.2020 р. Як зазначено у коментарі Міністерства оборони України [11], ця Стратегія є орієнтиром для розробки галузевих стратегій розвитку. Отже, вказані безпекові Стратегії діють не ізольовано, а у взаємозв'язку одна із одною [12].

У пункті 47 Стратегії національної безпеки України зазначено, що Україна запровадить національну систему стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на широкий спектр загроз, що, зокрема, передбачатиме: оцінку ризиків, своєчасну ідентифікацію загроз і визначення *вразливостей*.

В розділі 1 Стратегії кібербезпеки України зазначено, що поширення кіберзагроз на усі сфери життєдіяльності та вдосконалення інструментарію їх реалізації зумовлює необхідність зміни стратегії і тактики протидії ним. Набуває значимості максимально швидке виявлення *вразливостей* і кібератак, реагування та поширення інформації про них для мінімізації можливої шкоди.

В розділі 6 «Стратегічні завдання» щодо розбудови національної системи кібербезпеки виділені, зокрема, наступні вадливі напрями:

- запровадження на постійній основі оцінки стану захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів на *вразливість*, встановлення обов'язковості та періодичності проведення такої оцінки з урахуванням категорій критичності об'єктів, стимулювання участі у цих заходах фахівців з кібербезпеки приватного сектору;

- запровадження скоординованого виявлення та розкриття вразливостей інформаційно-комунікаційних систем.

Варто зазначити, що поняття «вразливість» використовується і в Законі України «Про основні засади забезпечення кібербезпеки України» (від 05.10.2017 № 2163-VIII). Згідно пункту 15 ч. 3 ст. 8 цього Закону, функціонування національної системи кібербезпеки забезпечується, зокрема, шляхом: 15) впровадження організаційно-технічної моделі національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію *вразливості* комунікаційних систем. Згідно ч. 5 ст. 8 цього Закону, впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, системи виявлення *вразливостей* і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань. Цим же Законом частина 1 статті 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» доповнена пунктом 91, яким до обов'язків Служби віднесені «координація, організація та проведення аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на *вразливість*».

Таким чином, в законодавстві України питанням нейтралізації вразливостей приділяється

велика увага як важливому чиннику кібербезпеки, однак універсального юридичного визначення цьому поняттю не надано. Разом із тим, на офіційному рівні визначення «вразливість системи» («system vulnerability») надане у Нормативному документі НД ТЗІ 1.1-003-99 Служби безпеки України «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» [13]. Згідно пункту 4.2.11 цього документу, вразливість системи (system vulnerability) – нездатність системи протистояти реалізації певної загрози або сукупності загроз.

Разом із тим, у Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, затвердженому постановою Кабінету Міністрів України від 16.05.2023 р. № 497 (далі – Порядок № 497), терміни «вразливість системи» вживається в такому значенні – це властивість системи, через використання якої створюється загроза для її безпеки, порушується сталий, надійний та штатний режим функціонування системи, здійснюється несанкціоноване втручання в її роботу, створюється загроза для безпеки (захищеності) електронних інформаційних ресурсів, конфіденційності, цілісності, доступності таких ресурсів. Зазначається, що цей термін використовується саме для цілей цього Порядку.

Повертаючись до питання вразливостей інформаційно-комунікаційних систем цивільної авіації, слід зазначити, що спеціальної уваги цьому питанню у Повітряному кодексі України приділяється недостатньо. Інформаційна безпека розглядається в контексті загальної безпеки авіації. Так, згідно пункту 20 ч. 1 ст. 1 Кодексу, безпека авіації – стан галузі цивільної авіації, за якого ризик завдання збитків людям чи майну знижується до прийнятного рівня у результаті безперервного процесу визначення рівня небезпеки і керування ним та утримується на такому рівні, або знижується далі, у сферах безпеки польотів, авіаційної безпеки, охорони навколишнього природного середовища, економічної безпеки та інформаційної безпеки. Згідно ч. 1 ст. 10 Кодексу, безпека авіації складається з безпеки польотів, авіаційної безпеки, екологічної безпеки, економічної та інформаційної безпеки. При цьому спеціально про кібербезпеку в Кодексі не згадується. Можливо, це пов'язано із тим, що Повітряний кодекс України прийнятий 19.05.2011 р. (№ 3393-VI), що раніше Закону України «Про основні засади забезпечення кібербезпеки України» (від 05.10.2017 р. № 2163-VIII). Разом із тим, згідно Державній Програмі авіаційної безпеки цивільної авіації, затвердженій Законом України від 21 березня 2017 року № 1965-VIII:

35) кібератака – несанкціоновані дії, що здійснюються за допомогою інформаційно-комунікаційних технологій та спрямовані на порушення конфіденційності, цілісності та доступності інформації, яка обробляється в інформаційній (автоматизованій), телекомунікаційній, інформаційно-телекомунікаційній системі, або порушення сталого функціонування такої системи, суб'єктів авіаційної діяльності;

36) кіберзагрози цивільній авіації – наявні та потенційно можливі явища і чинники, що становлять загрозу кібербезпеці та можуть призвести до актів незаконного втручання в діяльність цивільної авіації;

82) технічний захист критично важливих інформаційних авіаційних систем – діяльність, спрямована на протидію кіберзагрозам цивільній авіації для унеможливлення блокування або втручання в системи, забезпечення цілісності, доступності і контрольованості інформації, що використовується у системах.

Згідно пункту 173 Державної Програми, з метою захисту цивільної авіації від кіберзагроз уповноважений орган з питань цивільної авіації: визначає пріоритети у сфері протидії кіберзагрозам цивільної авіації; здійснює державний нагляд за станом захисту критично важливих інформаційних авіаційних систем суб'єктами авіаційної діяльності від кіберзагроз цивільній авіації; під час оцінки рівня загрози цивільній авіації від кіберзагроз враховує стан захисту критично важливих інформаційних авіаційних систем та зв'язних технологій суб'єктами авіаційної діяльності; погоджує перелік критично важливих інформаційних авіаційних систем; проводить їх ідентифікацію, збір, узагальнення

та облік даних; впроваджує систему відбору, перевірки та підготовки фахівців з питань протидії кіберзагрозам цивільній авіації.

Згідно пункту 174 Державної Програми, суб'єкти авіаційної діяльності для протидії кіберзагрозам цивільній авіації: визначають перелік критично важливих інформаційних авіаційних систем, що використовуються суб'єктом авіаційної діяльності, втручання в роботу яких прирівнюється до акту незаконного втручання, та подають його на затвердження уповноваженого органу з питань цивільної авіації; розробляють і створюють моделі загроз для кожної критично важливої інформаційної авіаційної системи, погоджують такі моделі з уповноваженим органом з питань цивільної авіації; забезпечують технічний захист кожної з критично важливих інформаційних авіаційних систем; запроваджують контроль за ефективністю здійснення заходів щодо захисту та у разі необхідності застосовують додаткові заходи безпеки.

В Інструкції з оцінки рівня загрози безпеці цивільної авіації України, затвердженій Наказом Міністерства інфраструктури України від 17.06.2020 р. № 356, зареєстрованим в Міністерстві юстиції України 01.10.2020 р. за № 960/35243, для оцінки рівня загрози та ризиків передбачене врахування таких видів загроз, як кібератаки та кіберзагрози.

Як зазначено у статті [14], Генеральний секретар ІКАО Фан Лю під час свого виступу на засіданні РБ ООН 27.09.2017 р. підтвердив, що серед усіх загроз безпеці цивільної авіації, найновітнішою, безумовно, є стрімке поширення у сфері авіації кібертехнологій, «і чим більш ми покладаємося на комп'ютери та інформаційні технології, тим більше ми піддаємо себе кіберзагрозам» [14, с. 39]. У статті також наголошується, що крім ІКАО питання протидії кіберзагрозам стає предметом спеціальної уваги і інших міжнародних організацій в авіаційній сфері, у, серед яких Міжнародна асоціація повітряного транспорту (ІАТА), Міжнародна координаційна рада асоціацій космічної промисловості (ІККАІА) тощо [14, с. 38].

У Плані дій ІСАО із забезпечення кібербезпеки (січень 2022 року) [5] зазначено, що 39-та сесія Асамблеї ІКАО підтвердила важливість та невідкладність захисту критичних систем інфраструктури цивільної авіації від кібератак. У Плані дії визначено: інформаційна безпека – це збереження конфіденційності, цілісності та доступності інформації. Також сюди можуть бути включені інші властивості, такі як справжність, підзвітність, безвідмовність та достовірність; кібербезпека – комплекс технологій, засобів контролю та заходів, а також процесів та практичних методів, призначених для забезпечення конфіденційності, цілісності, доступності та загального захисту систем, мереж, програм, пристроїв, інформації та даних від атак, пошкоджень, несанкціонованого доступу, використання та/або експлуатації.

Засадничими елементами політики у сфері кібербезпеки визначені: забезпечення включення кібербезпеки як компоненту систем безпеки польотів та авіаційної безпеки цивільної авіації та комплексних механізмів управління ризиком; забезпечення сумісності різних методик оцінки ризику для кібербезпеки цивільної авіації; розроблення політики в галузі кібербезпеки з урахуванням повного життєвого циклу авіаційних систем.

Таким чином, проблематика інформаційної та кібер- безпеки у сфері цивільної авіації вирішується виходячи із загальних закономірностей інформаційної та кібер- безпеки, з урахуванням особливостей авіаційної сфери. Наприклад, в інформаційному матеріалі [15] повідомлено про універсальний продукт із захисту від кібератак, який може закрити задачі будь-якого підприємства, у тому числі – аеропортів.

Для підвищення ефективності виявлення вразливостей в Україні протягом 2022-2023 рр. офіційно запроваджена так звана система bug bounty – це тестування електронних сервісів із залученням зовнішніх фахівців, яке дає можливість виявити вразливі місця і недоліки в програмних продуктах. Процедура широко застосовується у всьому світі[1]. Процедура по суті заохочує так званих «білих» хакерів на договірній основі атакувати певні системи з метою пе-

[1] https://thedigital.gov.ua/news/posilyuemo-kiberzakhist-uryad-ukhvaliv-mekhanizm-provedennya-bug-bounty

ревірки їх стійкості до таких атак і пошуку вразливостей. За знайдені помилки пропонується винагорода. Це дозволяє розробникам усунути помилки, перш ніж широка громадськість дізнається про них, запобігаючи випадкам масових зловживань. Програми Bug bounty були реалізовані в компаніях Mozilla, Facebook, Yahoo!, Google, Reedit, Square і Microsoft[2]. Безпечність застосунку «Дія» також тестувалася за допомогою програми Bug bounty[3].

Офіційне запровадження даної системи в Україні здійснювалося у 2 етапи. На першому етапі були внесені відповідні зміни у Кримінальний кодекс (КК) України. Так, стаття 361 КК України визнавала кримінально караним «несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Разом із тим, Законом України від 24.03.2022 року № 2149-IX «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» стаття 361 КК України була доповнена частиною 6, відповідно до якої дії, передбачені цією статтею, не вважаються несанкціонованим втручанням в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, *якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж.*

На другому етапі запровадження системи Bug bounty Кабінет Міністрів України затвердив згаданий вище Порядок № 497. Цей Порядок визначає механізм здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Дія цього Порядку не поширюється на інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі, в яких обробляється службова інформація та/або інформація, що становить державну таємницю, розвідувальну таємницю, банківську таємницю.

Організація пошуку потенційної вразливості системи здійснюється її власником. У разі потреби власник системи може прийняти рішення про залучення координатора для організації пошуку потенційної вразливості системи. Залучення координатора відбувається шляхом укладення між власником системи та координатором договору про надання послуг з організації пошуку потенційної вразливості системи. У разі коли договір про надання послуг з організації пошуку потенційної вразливості системи передбачає надання координатором платних послуг, такий договір укладається відповідно до вимог законодавства у сфері публічних закупівель.

Пошук потенційної вразливості системи здійснюється на підставі публічної пропозиції. Публічна пропозиція оприлюднюється власником системи на власному офіційному веб-сайті. У разі залучення власником системи координатора публічна пропозиція оприлюднюється координатором на його власному офіційному вебсайті. У такому разі власник системи оприлюднює на своєму офіційному веб-сайті посилання на відповідну сторінку веб-сайту координатора. Публічна пропозиція викладається українською мовою, при цьому додатково власник системи або координатор може викласти пропозицію іноземною мовою, яка є офіційною мовою Ради Європи.

Публічна пропозиція розробляється власником системи або координатором відповідно до примірної публічної пропозиції про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж і методичних рекомендацій з розроблення публічної пропозиції про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, що затверджуються Адміністрацією Держспецзв'язку. Така Примірна публічна про-

[2] https://uk.wikipedia.org/wiki/Bug_Bounty
[3] https://diia.gov.ua/news/diya-projshla-perevirku-bagbaunti-ta-pidtverdila-bezpechnist-zastosunku

позиція затверджена Наказом Адміністрації Держспецзв'язку від 14.07.2023 № 599**.**

Зокрема, як зазначено вище, стороння особа, яка зламала систему розваг у польоті (IFE) у літаку, в подальшому пояснювала, що у такий спосіб тестувала електронні системи управління літаком на вразливість [3]. Однак без договору із відповідними власниками систем такі дії будуть вважатися незаконними – несанкціонованим втручанням.

Висновки. Проведене дослідження сучасних підходів до правового регулювання у сфері виявлення, нейтралізації та управління вразливостями інформаційно-комунікаційних систем, у тому числі – цивільної авіації. У найбільш концентрованому вигляді вразливість системи – це нездатність системи протистояти реалізації певної загрози або сукупності загроз, що особливо небезпечно на авіаційному транспорті, де «чим більш ми покладаємося на комп'ютери та інформаційні технології, тим більше ми піддаємо себе кіберзагрозам». У зв'язку із цим питання протидії кіберзагрозам стає предметом спеціальної уваги Міжнародної організації цивільної авіації (ІКАО), а також інших міжнародних організацій у сфері авіаційного транспорту (Міжнародна асоціація повітряного транспорту (IATA), Міжнародна координаційна рада асоціацій космічної промисловості (ІККАІА) тощо). В Україні законом затверджена Державна Програма авіаційної безпеки цивільної авіації. Разом із тим, підсилення кібербезпеки на авіаційному транспорті здійснюється в контексті загальних методів та принципів кібербезпеки. Важливим кроком запровадження в Україні системи нейтралізації вразливостей слід вважати законодавче врегулювання процедур Bug bounty.

Література

1. Філінович В.В. Кібербезпека та загрози авіаційній сфері: правовий аспект. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право».* Київ: НАУ, 2021. № 3 (60). С. 38-43. DOI: 10.18372/2307-9061.60.15950.

2. Ільєнко А.В., Ільєнко С.С., Кваша Д.С. Сучасний стан забезпечення кібернетичної безпеки цивільної авіації України та світу. *Кібербезпека: освіта, наука, техніка.* 2020. № 1 (9). С. 24-34. DOI: 10.28925/2663-4023.2020.9.2436.

3. Zetter Kim. Feds Say That Banned Researcher Commandeered a Plane. Wired. 2015. May 15. URL: https://www.wired.com/category/ backchannel/

4. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посібник. Дніпро, Дніпроп. держ. унт внутріш. справ, 2020. 144 с.

5. Cybersecurity Action Plan. ICAO. Second edition, January 2022. 25 p. Appendix 12 p. URL: https://www.icao.int/aviationcybersecurity/Documents/ CYBERSECURITY %20ACTION%20PLAN %20-%20Second%20edition.EN.pdf

6. Корольков Р.Ю., Лаптєв С.О. Натурне моделювання атаки «War Driving» на бездротову мережу. *Кібербезпека: освіта, наука, техніка.* 2022. № 1 (18). С. 99-105. DOI: 10.28925/2663-4023.2022.18.99107.

7. Халіфе Кассем, Криховецький Г.Я., Кучук Г.А. Оцінка вразливості системного програмного забезпечення. *Системи управління, навігації та зв'язку.* 2017. Вип. 6(46). С. 141-144.

8. Харченко В.П., Алєксєєв О.М. Система управління ризиками авіаційної діяльності. Київ: НАУ, 2018. 312 с.

9. What is a vulnerability? Knowledgebase. ICTEA. URL: https://www.ictea.com/cs/knowledgebase.php?action=displayarticle&id=2092&language=english

10. Guoqiang Fu, Криволап Є.В. Особливості термінології в англомовній літературі у сфері кібербезпеки. *Наукові праці Національного авіаційного університету: Серія «Юридичний вісник. Повітряне і космічне право*». Київ: НАУ, 2023. № 1 (66). С. 63-71. DOI: https://doi.org/10.18372/2307-9061.66.17419

11. Рік діяльності Уряду: розробка стратегічних документів у сфері безпеки та оборони. Міністерство оборони України. URL: https://www.mil.gov.ua/special/news.html?article=61846

12. Криволап Є.В., Юринець Ю.Л. Взаємозв'язок безпекових стратегій України з інформаційною безпекою та кібербзпекою. *Ак-*

туальні питання у сучасній науці. 2023. № 8(14). С. 477-487.

13. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Нормативний документ НД ТЗІ 1.1-003-99. Затверджено наказом від 28 квіт. 1999 р. № 22 Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. 1999. 22 с. URL: https://tzi.ua/assets/ files/1.1_003_99.pdf

14. Григоров О.М. Міжнародно-правові стандарти кібербезпеки цивільної авіації. *Актуальні проблеми держави і права*: зб. наук. пр. Вип. 91 / редкол.: Г.І. Чанишева (голов. ред.) та ін. Одеса: Гельветика, 2021. С. 38-43.

15. Безпека в авіації: чому це важливо саме зараз. GigaCloud. 01.03.2019. URL: https://gigacloud.ua/blog/zahodi/kiberbezpeka-v-aviacii-chomu-ce-vazhlivo-same-zaraz

References

1. Filinovych V.V. Kiberbezpeka ta zahrozy aviatsiinii sferi: pravovyi aspekt. *Naukovi pratsi Natsionalnoho aviatsiinoho universytetu: Seriia «Iurydychnyi visnyk. Povitriane i kosmichne pravo».* Kyiv: NAU, 2021. № 3(60). S. 38-43. DOI: 10.18372/2307-9061.60.15950.

2. Ilienko A.V., Ilienko S.S., Kvasha D.S. Suchasnyi stan zabezpechennia kibernetychnoi bezpeky tsyvilnoi aviatsii Ukrainy ta svitu. *Kiberbezpeka: osvita, nauka, tekhnika.* 2020. № 1(9). S. 24-34. DOI: 10.28925/2663-4023.2020.9.2436.

3. Zetter Kim. Feds Say That Banned Researcher Commandeered a Plane. Wired. 2015. May 15. URL: https://www.wired.com/category/ backchannel/

4. Hrebeniuk A.M., Rybalchenko L.V. Osnovy upravlinnia informatsiinoiu bezpekoiu: navch. posibnyk. Dnipro, Dniprop. derzh. unt vnutrish. sprav, 2020. 144 s.

5. Cybersecurity Action Plan. ICAO. Second edition, January 2022. 25 p. Appendix 12 p. URL: https://www.icao.int/aviationcybersecurity/Documents/CYBERSECURITY %20ACTION%20PLAN %20-%20Second%20edition.EN.pdf

6. Korolkov R.Iu., Laptiev S.O. Naturne modeliuvannia ataky «War Driving» na bezdrotovu merezhu. *Kiberbezpeka: osvita, nauka, tekhnika.* 2022. № 1(18). S. 99-105. DOI: 10.28925/2663-4023.2022.18.99107.

7. Khalife Kassem, Krykhovetskyi H.Ia., Kuchuk H.A. Otsinka vrazlyvosti systemnoho prohramnoho zabezpechennia. *Systemy upravlinnia, navihatsii ta zviazku.* 2017. Vyp. 6(46). S. 141-144.

8. Kharchenko V.P., Alieksieiev O.M. Systema upravlinnia ryzykamy aviatsiinoi diialnosti. Kyiv: NAU, 2018. 312 s.

9. What is a vulnerability? Knowledgebase. ICTEA. URL: https://www.ictea.com/cs/ knowledgebase.php?action=displayarticle&id= 2092&language=english

10. Guoqiang Fu, Kryvolap Ye.V. Osoblyvosti terminolohii v anhlomovnii literaturi u sferi kiberbezpeky. *Naukovi pratsi Natsionalnoho aviatsiinoho universytetu: Seriia «Iurydychnyi visnyk. Povitriane i kosmichne pravo».* Kyiv: NAU, 2023. № 1(66). S. 63-71.

11. Rik diialnosti Uriadu: rozrobka stratehichnykh dokumentiv u sferi bezpeky ta oborony. Ministerstvo oborony Ukrainy. URL: https://www.mil.gov.ua/special/ news.html? article=61846

12. Kryvolap Ye.V., Yurynets Yu.L. Vzaiemozviazok bezpekovykh stratehii Ukrainy z informatsiinoiu bezpekoiu ta kiberbzpekoiu. *Aktualni pytannia u suchasnii nautsi.* 2023. № 8(14). S. 477-487.

13. Terminolohiia v haluzi zakhystu informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu. Normatyvnyi dokument ND TZI 1.1-003-99. Zatverdzheno nakazom vid 28 kvit. 1999 r. № 22 Departamentu spetsialnykh telekomunikatsiinykh system ta zakhystu informatsii Sluzhby bezpeky Ukrainy. 1999. 22 s. URL: https://tzi.ua/assets/files/1.1_003_99.pdf

14. Hryhorov O.M. Mizhnarodno-pravovi standarty kiberbezpeky tsyvilnoi aviatsii. *Aktualni problemy derzhavy i prava:* zb. nauk. pr. Vyp. 91 / redkol.: H.I. Chanysheva (holov. red.) ta in. Odesa: Helvetyka, 2021. S. 38-43.

15. Bezpeka v aviatsii: chomu tse vazhlyvo same zaraz. GigaCloud. 01.03.2019. URL: https://gigacloud.ua/blog/zahodi/kiberbezpeka-v-aviacii-chomu-ce-vazhlivo-same-zaraz

Evgeniy Krivolap, Julia Iurynets, Leonid Belkin

ISSUE OF NEUTRALIZATION OF VULNERABILITIES INFORMATION AND COMMUNICATION SYSTEMS OF CIVIL AVIATION: LEGAL ASPECT

National Aviation University
Liubomyra Huzara Avenue, 1, 03058, Kyiv, Ukraine
E-mail: belkinleonid@ukr.net

The aim *of the article is to research modern approaches to legal regulation in the field of detection, neutralization and management of vulnerabilities in information and communication systems, including civil aviation.* ***Research methods:*** *documentary analysis, summarization of legal information, information from the field of cyber protection of information and communication systems, as well as practices of cyber protection of information from various cyber attacks.* ***Results:*** *it was established that in the most concentrated form, system vulnerability should be understood as the inability of the system to resist the implementation of a certain threat or set of threats, which is especially dangerous in air transport. In this regard, the issue of combating cyber threats becomes the subject of special attention in the aviation sphere, including the International Civil Aviation Organization (ICAO), as well as other international organizations in the field of air transport (International Air Transport Association (IATA), International Coordinating Council of Aerospace Industries Associations (ICCAIA), etc.). In Ukraine, the State Civil Aviation Safety Program is approved by law. At the same time, the strengthening of cyber security in aviation transport is carried out in the context of the introduction of general methods and principles of cyber security. An important step in the introduction of the vulnerability neutralization system in Ukraine should be considered the legislative regulation of Bug bounty procedures - testing of electronic services with the involvement of external specialists, which makes it possible to identify vulnerabilities and flaws in software products. Regulation is carried out by the Procedure for searching and identifying potential vulnerabilities of information (automated), electronic communication, information and communication systems, electronic communication networks, approved by the Cabinet of Ministers of Ukraine Resolution No. 497 of 05/16/2023.* ***Discussion****: improvement of legal regulation in the field of detection, neutralization and management of vulnerabilities of information and communication systems, including civil aviation, will contribute to increasing the safety of civil aviation.*

Key words: *cyber security; cyber attack; critical infrastructure; vulnerability; computer networks.*

Стаття надійшла до редакції 11.09.2023