***Світлана ГУЦУ***
*кандидатка юридичних наук, доцентка, професорка ХАІ,*
*доцентка кафедри права гуманітарно-правового факультету*
*Національного аерокосмічного університету ім. М. Є. Жуковського*
*«Харківський авіаційний інститут», м. Харків, Україна*
*ORCID: 0000-0003-1373-6079*
*e-mail: s.gutsu@khai.edu*

# ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В АВІАЦІЙНІЙ СФЕРІ: МІЖНАРОДНО-ПРАВОВИЙ АСПЕКТ

**Анотація.** У величезному просторі технологічного прогресу авіація виділяється як маяк **інновацій** та **безпеки**. Однак авіація змінюється. Подальша цифровізація та взаємозв'язок авіаційних систем підштовхує галузь до нового покоління операційних ризиків і ризиків безпеки. Проте, як і в будь-якому прогресі, є зворотний бік медалі. Ті самі технології, які рухають нас вперед, створюють нові ризики, особливо у сфері інформаційної безпеки. Незважаючи на те, що інновації забезпечують додаткову функціональність і підвищення ефективності, такі вдосконалення також відкривають двері для використання нововведених уразливостей, які можуть призвести до більш несприятливих наслідків, ніж сприятливих. Цифрові загрози сьогодні стали такими ж, а то й більш поширеними, враховуючи кількість цифрових систем, які впроваджуються в усіх галузях галузі: навігації, зв'язку, авіоніці, корпоративних системах, технічному обслуговуванні та ремонті тощо. Питання інформаційної (кібер) безпеки авіаційної галузі не втрачають своєї актуальності. Аналіз результатів статистичних досліджень кібератак в авіаційній сфері свідчить про необхідність вдосконалення правових інструментів інформаційного захисту, з урахуванням тенденцій інформатизації та глобалізації авіаційної галузі.
**Ключові слова:** інформаційна безпека, інформаційні технології, забезпечення інформаційної безпеки, правове регулювання, авіаційна безпека.

Авіаційна промисловість стала свідком значної цифрової трансформації та інтеграції інструментів інформаційно-комунікаційних технологій (ІКТ) у механічні пристрої за останні кілька десятиліть. Але, чим інтегрованіша система, тим більша вразливість в інструментах ІКТ і програмному забезпеченні, яке керує системою. Ця сфера доволі широка: від безпеки приладів керування літаками і польотами до клієнтських баз даних авіакомпаній і аеропортів. Так, на початку 2021 року авіакомпанія Malaysia Airlines почала сповіщати клієнтів про те, що внаслідок витоку даних стала доступною особиста інформація учасників програми Enrich для часто літаючих пасажирів. Злом стався у стороннього постачальника ІТ-послуг, дані учасників Enrich були розкриті в період з березня 2010 року по червень 2019 року. Розкрита інформація включає імена учасників, контактну інформацію, дату народження, стать, номер постійного клієнта, статус і винагороди. рівень рівня. Паролі учасників не були розкриті. Невідомо, скільки учасників Enrich постраждали від злому[1].

Крім того, згідно зі звітом Blackberry Global Threat Intelligence Report за 2023 рік:

– частота унікальних атак шкідливого програмного забезпечення зросла на 50% між жовтнем 2022 року та січнем 2023 року;

– кількість кібернападів, про які було повідомлено в Eurocontrol, зросла на 530% між 2019 та 2020 роками. У 2020 році було зафіксовано 775 кібернападів на авіакомпанії та 150 — на аеропорти;

– у першій половині 2023 року кількість кібератак в авіаційній індустрії зросла на 24% у всьому світі;

– частота унікальних атак шкідливого програмного забезпечення зросла на 50% між жовтнем 2022 року та січнем 2023 року [2].

Поширене та миттєве підключення до мережі, яке колись обмежувалося IT-середовищем, тепер є частиною глобальної авіаційної культури. Інформаційні системи авіакомпаній, передові технологічні виробники літаків та інші партнери авіаційної галузі спільно використовують цей зв'язок для передачі інформації, підвищення обізнаності та звітування про стан робочого середовища. Цілісність цієї авіаційної цифрової структури вимагає, щоб усі учасники прийняли та використовували ефективні стратегії інформаційної безпеки, які зосереджені на постійному вдосконаленні для захисту від кіберзагроз. Наявність і дотримання чітко визначеної стратегії інформаційної безпеки захищає інформацію про клієнтів авіакомпанії, захищає цифрові активи авіакомпанії та забезпечує точність інформації, якою обмінюються в рамках авіації [3]. Інформаційна безпека загалом, а в авіації зокрема може розглядатися у широкому і вузькому розумінні. У вузькому – як безпека інформації, у широкому – це стан захищеності як від загроз безпеки інформації, так і від загроз нанесення шкоди інформаційним технологіям. Під інформаційною безпекою авіації слід розуміти захищеність інформації (в першу чергу в авіаційних телекомунікаційних системах) від незаконного доступу й використання. Відповідно до частини 1 статті 10 Повітряного кодексу України [4] безпека авіації складається з безпеки польотів, авіаційної безпеки, екологічної безпеки, економічної та інформаційної безпеки. Таким чином, законодавством визначено безпеку авіації як комплексне правове явище, що покликане забезпечувати комплексний правовий підхід її правового регулювання. Інформаційна безпека є частиною безпеки авіації і пов'язана вона з безпекою інформації, інформаційних систем та технологій, захистом та охороною інформації, забезпеченням інформаційної безпеки та усуненням можливих загроз [5].

Насьогодні система правового і локального регулювання інформаційної та/або кібер безпеки авіаційної сфери є доволі розгалуженою і широкою (Таблиця 1). Як представники цього бізнесу, так окремі держави і міжнародні інституції приймають всіх можливих заходів

щодо розробки і впровадження правил і інструментів безпеки. Але, нажаль, це не гарантує повного захисту від неправомірного втручання в роботу авіаційного обладнання, баз даних чи програмного забезпечення підприємств і організацій авіаційної сфери.

Таблиця 1. – Міжнародні правові інструменти та документи безпеки авіаційної галузі [6]

| Джерело | Регуляторні документи |
|---|---|
| **Міжнародні інструменти повітряного права** | – Конвенція про боротьбу з незаконним захопленням повітряних суден (1970)<br>– Конвенція про боротьбу з незаконними актами, що загрожують безпеці цивільної авіації (1971)<br>– Протокол про боротьбу з незаконними актами насильства в аеропортах, що обслуговують міжнародну цивільну авіацію, доповнення до Конвенції про боротьбу з незаконними актами, що загрожують безпеці цивільної авіації (1971)<br>– Конвенція про боротьбу з незаконними актами, що стосуються міжнародної цивільної авіації (2010)<br>– Пекінський додатковий протокол до Гаазької конвенції 1970 року про боротьбу з незаконним захопленням повітряних суден (2010) |
| **Міжнародна організація цивільної авіації (ІСАО)** | – Додаток 17 – Безпека. Захист міжнародної цивільної авіації від актів незаконного втручання<br>– Стратегія ІСАО з кібербезпеки в авіації<br>– Док 8973 Посібник з авіаційної безпеки (обмежений доступ)<br>– Док 9985 Посібник з безпеки управління повітряним рухом (обмежений доступ)<br>– Док 10108 Глобальна контекстна заява про ризики (обмежений доступ)<br>– Резолюція Асамблеї А40-10: Протидія кібербезпеці в цивільній авіації |
| **Європейська комісія** | – Виконавчий регламент Комісії (ЄС) 2015/1998 від 5 листопада 2015 року, що встановлює детальні заходи для впровадження основних загальних стандартів авіаційної безпеки<br>– Виконавчий регламент Комісії (ЄС) 2019/1583 від 25 вересня 2019 року, що вносить зміни до виконавчого регламенту (ЄС) 2015/1998, встановлюючи детальні заходи для впровадження основних загальних стандартів авіаційної безпеки щодо кібербезпеки |

| Джерело | Регуляторні документи |
|---|---|
| | – Виконавчий регламент Комісії (ЄС) 2017/373 від 1 березня 2017 року, що встановлює загальні вимоги для постачальників послуг управління повітряним рухом/навігаційних послуг та інших функцій мережі управління повітряним рухом і нагляду за ними, скасовуючи Регламент (ЄС) № 482/2008, Виконавчі регламенти (ЄС) № 1034/2011, (ЄС) № 1035/2011 і (ЄС) 2016/1377 та змінюючи Регламент (ЄС) № 677/2011<br>– Інструментарій з кібербезпеки транспорту |
| **Європейська стратегічна координаційна платформа (ESCP)** | Стратегія з кібербезпеки в авіації |
| **США: Федеральна авіаційна Адміністрація (FAA)** | – Code of Federal Regulations (CFR) Title 14 Aeronautics and Space (incl. Part 23, 25, 27, 29, etc.)<br>– Закон про переоформлення від 2018 року, публічний закон №: 115-254<br>– Стандарти польоту. Управління інформацією Система (FSIMS)<br>– Політика PS-AIR-21.16-02,Створення Спец Умови для Кібербезпеки |
| **Велика Британія: Управління цивільної авіації (CAA)** | – Стратегія Кібербезпеки в авіації<br>– CAP 1849: Керівництво з визначення критичних систем з кібербезпеки<br>– CAP 1850: Рамка оцінки кібербезпеки (CAF) для авіації<br>– CAP 1753: Процес нагляду за кібербезпекою в авіації (CAA) |

Останніми роками європейські регулюючі органи почали визнавати та розглядати ризики, пов’язані з цифровими системами. Законодавство щодо кібербезпеки вже почало набувати чинності, як-от Директива ЄС NIS2, яка вимагає від усіх держав-членів запровадити правила кібербезпеки для відповідних організацій до жовтня 2024 року. Зараз ми бачимо, що такі міркування розглядаються в авіаційній галузі через **п**рийняття постанов ЄС у 2022 році, що вимагає від профільних організацій створити та впровадити систему управління інформаційною безпекою (ISMS). Так, Делегований регламент Комісії (ЄС) 2022/1645, прийнятий 14 липня 2022 року, містить спеціальні правила для управління ризиками інформаційної безпеки в авіаційному секторі. Цей регламент є доповненням до ширшого Регламенту (ЄС) 2018/1139, який встановлює загальні правила цивільної авіації та засновує Агентство Європейського Союзу з авіаційної безпеки. Регламент спрямований на виявлення та управління ризиками інформаційної безпеки, які можуть вплинути на безпеку авіації,

зосереджуючись на системах інформаційних і комунікаційних технологій і даних, що використовуються в цивільній авіації.

Перші «Правила легкого доступу (EAR) для інформаційної безпеки (частина IS)»[7] від Агентства авіаційної безпеки Європейського Союзу (EASA) встановлюють «вимоги до управління ризиками інформаційної безпеки, що потенційно можуть впливати на безпеку авіації». Попередні правила кібербезпеки діяли лише для виробників оригінального обладнання – на відміну від EAR (частина IS), яка поширюється на весь авіаційний сектор. Кінцеві терміни відповідності до жовтня 2025 року та лютого 2026 року стосуватимуться різних типів організацій, як визначено в допоміжних законах ЄС.

До них належать: організації з технічного обслуговування, постачальники послуг з управління льотною придатністю, авіаоператори, аеромедичні центри, організації з підготовки диспетчерів повітряного руху та оператори пристроїв для моделювання польоту. Також у списку є аеропорти, постачальники інфраструктури зв'язку, організації навігаційної інфраструктури, повітряні вежі та засоби спостереження.

Правила розроблено для того, щоб забезпечити ефективне управління ризиками інформаційної безпеки в авіаційній галузі, що є важливим фактором безпеки в цілому. Узгодження з авіаційними стандартами США вже погоджено, і планується регулярне оновлення Правил легкого доступу (частина IS), що перетворить їх на набір правил, які з часом змінюватимуться [8].

Документ визначає що: «Система управління інформаційною безпекою (СУІБ) – це систематичний підхід до встановлення, впровадження, експлуатації, моніторингу, перегляду, підтримки та постійного покращення стану інформаційної безпеки організації». Його метою є захист інформаційних активів таким чином, щоб оперативні цілі та цілі безпеки організації могли бути досягнуті ефективним і результативним способом з урахуванням ризиків.

Загалом кажучи, СУІБ встановлює процес управління ризиками інформаційної безпеки на основі результатів аналізу впливу на інформаційну безпеку, які в основному визначають його масштаби. Якщо порушення інформаційної безпеки можуть спричинити або сприяти наслідкам безпеки авіації, вимоги безпеки інформації мають обмежити їхній вплив на рівні безпеки авіації, які вважаються прийнятними. Таким чином, усі ролі, процеси чи інформаційні системи, які можуть спричинити або сприяти наслідкам для безпеки авіації, підпадають під дію Регламенту (ЄС) 2023/203. СУІБ забезпечує засоби для прийняття рішень щодо необхідних засобів контролю інформаційної безпеки для всіх архітектурних рівнів (управління, бізнес, застосування, технології, дані) і доменів (організаційний, людський, фізичний, технічний). Крім того, це дозволяє керувати вибором, впровадженням і роботою

засобів контролю інформаційної безпеки. Нарешті, це дозволяє керувати управлінням, управлінням ризиками та відповідністю (GRC) у межах СУІБ.

**Висновок.** Цей досвід варто врахувати при вдосконаленні вітчизняного законодавства, що стосується інформаційної безпеки авіації. Як, зазначає Поліщук І. В.: «Функціонування системи цивільної авіації в Україні на сучасному етапі безпосередньо пов'язане, насамперед, із забезпеченням належності та своєчасності інформаційних потоків, впровадженням нових інформаційних технологій, глобалізацією та інтеграцією авіаційних інформаційних систем згідно міжнародних стандартів».[5] На нашу думку доцільним буде доповнити Повітряний кодекс України терміном «Інформаційна безпека авіації» та законодавчо визначити комплекс заходів по боротьбі із загрозами інформаційній безпеці шляхом чіткого врегулювання механізмів їх виявлення, попередження та усунення.

**Список використаних джерел:**


1. Захист авіаційної промисловості від цифрових загроз https://airportindustry-news.com/protecting-the-aviation-industry-from-digital-threats/
2. Bashar Ahmed Alohali.Aviation Cybersecurity National Governance. 2023. https://www.icao.int/MID/Documents/2023/Cybersecurity%20Symposium/2.2%20Saudi%20Arabia%20-%20Aviation%20Cybersecurity%20National%20Governance.pdf
3. Securing Airline Information on the Ground and in the Air http://www.lb.boeing.com/commercial/aeromagazine/articles/2012_q3/5/
4. Повітряний кодекс України від 19 трав. 2011 р. № 3393-VI. URL: http://zakon.rada.gov.ua/ laws/show/3393-17.
5. Поліщук, І. В. (2020). FEATURES OF LEGAL ADJUSTING OF INFORMATIVE SAFETY IN CIVIL AVIATION OF UKRAINE. Scientific Works of National Aviation University. Series: Law Journal "Air and Space Law", 2(55), 27–32. https://doi.org/10.18372/2307-9061.55.14771
6. Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation. Edition 4.0 | December 2022. https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilation-of-cyber-regs.pdf
7. Easy Access Rules for Information Security (Regulations (EU) 2023/203 and 2022/1645) file:///C:/Users/pagin/Downloads/Easy_Access_Rules_for_Information_Security_0.pdf
8. Джон Лейден Що таке нові правила інформаційної безпеки ЄС EAR для авіації? https://www.isms.online/data-protection/what-are-the-eus-new-ear-information-security-rules-for-aviation/