3. Фінансово-економічні наслідки війни. URL: https://lb.ua/blog/tetiana_bohdan/550614_finansovoekonomichni_naslidki.html (дата звернення: 21.03.2024).

УДК 343.326:004.056.53(043.2)

КІБЕРБЕЗПЕКА В АВІАЦІЙНІЙ СФЕРІ: ПРАВОВИЙ АСПЕКТ

Сисак Владислав Тарасович

Національний авіаційній університет, Київ

Науковий керівник – Лихова С.Я., д.ю.н., проф.

Ключові слова: кібербезпека, авіація, інформаційна безпека, кіберпростір, кіберзлочини, кібератака.

Більшість з нас сьогодні не може уявити своє життя без інформаційних технологій, які широко застосовуються в усіх сферах взаємодії, включаючи авіацію. Використання цих технологій має свої проблеми, особливо з погляду безпеки, оскільки кіберзагрози часто мають транснаціональний характер і впливають на національний, регіональний і міжнародний рівні. Цивільна авіація сьогодні не може існувати без належного захисту в кіберпросторі. В іншому випадку використання сучасних технологій і розробок у транспорті не матиме сенсу. Багатьом відомий термін «кібертероризм», який стає все більш відомим усім жителям планети [1].

Для наукового обґрунтування результатів досліджень на тему кібербезпеки в авіаційній сфері використаний аналітичний метод, а саме проаналізовано взаємозв’язок сучасних кіберзагроз в авіаційній сфері у правовому аспекті та зроблені висновки з використанням системно-структурного методу.

Так, комунікація через електронні засоби стала основою для банків, авіакомпаній та корпорацій, допомагаючи забезпечити їхню стабільність. Проте, кіберзлочинці не обов'язково діють на вулицях: студенти та підлітки з ноутбуками та доступом до мережі можуть стати злочинцями. У військових конфліктах вони перетворюються на інформаційних воїнів, використовуючи кібератаки та «взломи» для ефективних атак.

Під час військового конфлікту в Україні кібератаки шахраїв, які намагаються незаконно заволодіти коштами через Інтернет, завдають значної шкоди, подібно до руйнування на полі бою. Статистика вказує, що виявлені випадки кіберзлочинів зростали майже в 7,5 рази від 1998 по 2021 рік, не враховуючи класичні комп'ютерні правопорушення та рівень прихованості [2].

Слід зазначити, що військова авіація сьогодні має більше захисту порівняно з цивільною авіацією. Однак немає жодного методу, який гарантував би сто відсотковий захист від кіберзагроз. Основна проблема полягає в тому, що сучасні дрони та військовий авіатранспорт складаються переважно з електронних компонентів, керованих не стільки людиною, скільки спеціальною програмою. Це означає, що вправний хакер може вторгнутися в цю програму та змінити її функціонування. Таким чином, кібератаки можуть повністю змінити хід бойових операцій.

Сьогодні майже кожна галузь людської діяльності неможлива без використання інформаційних технологій, і це стосується й авіаційного сектору. Проте, широка диджиталізація також відкрила двері для кіберзлочинців, які тестують системи на стійкість, зазвичай з метою здобутку матеріальних вигод. Кібератаки стали нормою, особливо в аерокосмічній галузі, де хакери можуть проникати в комп'ютерні системи та мережі не лише комерційних компаній, але й організацій критичної інфраструктури, щоб перешкоджати їхній роботі або контролювати її [3].

Щодо правового захисту, важливо розвивати та удосконалювати наявні законодавчі акти для своєчасного запобігання, виявлення та реагування на кібератаки. Для створення ефективної структури кібербезпеки в авіаційній сфері необхідно вжити такі заходи: Гармонізувати національне законодавство з міжнародними стандартами; Оцінити і захистити належне розуміння можливих небезпек і атак; Проводити постійні дослідження та впроваджувати нові розробки; Забезпечити швидке і адекватне реагування на кіберінциденти; Визначити ефективні принципи проектування та експлуатації авіаційних систем; Установити і застосовувати загальні кіберстандарти для зниження ризиків.

Висновок

Лише за умови вжиття всіх цих заходів, як технічних, так і правових, економічних і соціально-орієнтованих, можливо забезпечити захист авіаційних комп'ютерних систем і мереж від сучасних загроз кібербезпеки. Для сучасного суспільства, зокрема, для спеціалістів в авіаційній сфері важливо постійно підвищувати культуру кібербезпеки серед персоналу, проводячи навчання та семінари з фахівцями з авіаційної та інформаційної галузей Встановлювати комунікацію та співпрацю з усіма зацікавленими сторонами для розробки передових методів управління вразливостями. Збільшувати довіру та забезпечувати прозорість, створюючи єдиний глобальний підхід до кібербезпеки.

Список використаних джерел:

1. Cyber-security challenges in aviation industry: a review of current and future trends / E. Ukwandu, M.B. Amine, H. Hindy etc. Cornell University, 2021. No 1. P. 2–4.

2. Боротьба з кіберзлочинністю в умовах воєнного стану. URL: https://jurliga. ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanuzakon-2149-ix (дата звернення: 17.03.2024).

3. 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. No 2 (55). С. 28-29. DOI: https://doi.org/10.18372/2307-9061.55.14771.

УДК 343.326:004.056.53(043.2)

ПИТАННЯ КІБЕРБЕЗПЕКИ У СФЕРІ ЦИВІЛЬНОЇ АВІАЦІЇ

Шиян Юлія

Національний авіаційний університет, Київ

Науковий керівник: Чулінда Л.І., к.ю.н., доц

Ключові слова: кібербезпека, інформаційна безпека, Асамблея ICAO, транспортна інфраструктура, цивільна авіація, безпека польотів.

Уся система цивільної авіації працює на основі довіри, відповідальності, яка перебуває у фокусі всієї діяльності Міжнародної організації цивільної авіації (ICAO). Пасажири очікують на безпечний політ, оператори вірять, що системи безпеки відповідатимуть їхнім потребам, а держави довіряють Міжнародній організації цивільної авіації, яка створює гармонізовані глобальні стандарти, що забезпечують безпечну та ефективну систему цивільної авіації. Кібербезпека транспортних систем на сьогодні потребує щоденного удосконалення, оскільки виникають потенційні загрози внаслідок поєднання кібернетичних можливостей законних і незаконних учасників у повітряному просторі, під час актів незаконного захоплення суден та авіалайнерів. Це не лише порушує безпеку, а й вимагає розробки нових стратегій захисту кібербезпеки у сфері транспортної інфраструктури.

Варто зважати на те, що кібербезпека є одним із видів або навіть стовпів інформаційної безпеки. І.В. Поліщук так визначає її з погляду 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