DOI https://doi.org/10.46845/2541-8254-2025-5(52)-30-30

УДК 338.14

ИССЛЕДОВАНИЕ КИБЕРУГРОЗ В АСПЕКТЕ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ГРАЖДАНСКОЙ АВИАЦИИ

А.Т. Мельник, студентка,
ФГБОУ ВО «Калининградский государственный технический университет»
melnikanastasia@mail.ru

В. Б. Горбунова, кандидат экономических наук, доцент,
ФГБОУ ВО «Калининградский государственный технический университет»

В статье исследуется влияние киберугроз на экономическую безопасность воздушного транспорта, анализируются основные виды кибератак, на основе официальных данных оцениваются потенциальные уязвимости в авиационной инфраструктуре и предлагаются направления по снижению рисков киберугроз с помощью различных механизмов защиты. Приводятся ключевые факты по инциденту 28 июля 2025 года, связанных со сбоями в информационных системах ПАО «Аэрофлот», оцениваются последствия кибератаки.

Ключевые слова: *воздушный транспорт, киберугроза, экономическая безопасность, кибератака, ПАО «Аэрофлот», гражданская авиация, киберинцидент, риски, ущерб.*

ВВЕДЕНИЕ

Современная гражданская авиация представляет собой одну из наиболее капиталоемких и высокотехнологичных отраслей экономики, так как устойчивость информационной структуры оказывает прямое влияние на безопасность перелетов, репутацию перевозчиков и финансовую стабильность. Развитие интернета, стремительное распространение цифровых технологий провоцирует рост уровня цифровизации авиационных процессов (от on-line-бронирований и системы управления до обслуживания воздушных судов), что, естественно, сопровождается увеличением уязвимости для кибератак.

По информации центра мониторинга и реагирования на кибератаки RED Security SOC, в 2024 году количество киберинцидентов в российских компаниях увеличилось в 2,5 раза по сравнению с 2023 годом и достигло почти 130 тысяч. [1] Европейское агентство по авиационной безопасности (EASA) подчёркивает, что цифровизация авиационной отрасли значительно расширяет поверхность возможных кибератак и требует интеграции мер информационной безопасности во все уровни авиационной экосистемы - от проектирования и сертификации воздушных судов до организационных процессов и обмена информацией об инцидентах. Аналогичные выводы представлены в отчётах Европейского агентства по кибербезопасности (ENISA) и Международной организации гражданской авиации (ICAO), где отмечается рост числа киберинцидентов и необходимость формирования устойчивых механизмов защиты критической авиационной инфраструктуры (EASA, 2023; ENISA, 2024; ICAO, 2023). [2]

Современные киберугрозы являются общей проблемой в обеспечении экономической безопасности [3], а в сфере воздушного транспорта они характеризуются особой разнообразием и сложностью, представляя собой серьезный вызов для безопасности и стабильности отрасли. Эти угрозы включают в себя, например, кибершпионаж, нацеленный на несанкционированный доступ к конфиденциальной информации, такой как планы полетов и данные пассажиров. Также актуален кибервандализм, который проявляется в деструктивном воздействии на критически важные системы, например, путем вывода из строя важного оборудования. Нельзя игнорировать и кибертерроризм, стремящийся дестабилизировать работу авиационной отрасли через захват контроля над воздушными судами, что было

актуально десятки лет назад. Имеет место быть и кибермошенничество, направленное на совершение финансовых преступлений, вроде кражи личных данных пассажиров. [4]

Уязвимые места авиационной инфраструктуры включают системы управления полетами, подверженные риску сбоев из-за уязвимостей в программном и информационном обеспечении. Наземные станции, в том числе системы управления аэропортами, и коммуникационные сети, обеспечивающие связь между самолетами и землей, также являются потенциальными точками проникновения.

Атаки на эти системы могут привести к серьезным последствиям, в первую очередь речь идет об угрозе жизни и здоровью пассажиров и экипажа. Экономический ущерб также неизбежен, ведь финансовые потери из-за задержек рейсов и необходимости восстановления систем могут достигать миллиардов долларов. Нарушение работы аэропортов, с парализацией их деятельности и срывом расписания полетов, дополнительно подчеркивает серьезность этих угроз. В комплексе все перечисленное может подорвать доверие к авиационной отрасли.

ОБЪЕКТ ИССЛЕДОВАНИЯ

Объектом исследования выступает сфера гражданской авиации: риски кибербезопасности, причины их возникновения и последствия их реализации.

ЦЕЛЬ И ЗАДАЧИ ИССЛЕДОВАНИЯ

Цель – исследовать киберугрозы в сфере гражданской авиации с позиции анализа возможных экономических последствий для авиаперевозчиков на примере инцидента с ПАО «Аэрофлот» летом 2025 года, выявить ключевые факторы уязвимости и предложить направления минимизации финансовых потерь и укрепления экономической безопасности.

Для достижения поставленной цели были решены следующие задачи:

— определить тенденции развития киберугроз в сфере гражданской авиации;

— провести анализ конкретного киберинцидента и оценить его экономические последствия для финансовой и операционной устойчивости компании;

— обобщить прогнозируемые последствия кибератак для авиаперевозчиков;

— предложить направления по снижению рисков киберугроз с помощью различных механизмов защиты.

МЕТОДЫ ИССЛЕДОВАНИЯ

В процессе исследования использовались такие общенаучные методы, как контент-анализ, сравнительный анализ, экономико-математическое моделирование и экспертная оценка.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

По информации компании «Информзащита», в первом полугодии 2025 года число кибератак на авиационный сектор выросло на 42% по сравнению с аналогичным периодом 2024 года. Особенно резко (более чем на 500%) увеличилось количество атак с использованием программ-вымогателей (ransomware). [5]

Авиационная отрасль остаётся одной из самых привлекательных для злоумышленников по нескольким причинам:

— высокая ценность данных: персональные данные пассажиров, маршруты, платёжные реквизиты и внутренняя документация;

— финансовая устойчивость компаний: авиакомпании склонны к выплате выкупа для избежания простоев;

— критическая роль в логистике и пассажирских перевозках: особенно в отдалённых регионах, где авиация - единственный способ сообщения;

Таким образом, сектор авиации становится привлекательной целью как для хактивистов, так и для организованных киберпреступных группировок, включая те, что действуют по государственным заказам.

Проблематика кибербезопасности в сфере гражданской авиации получила развитие в работах зарубежных и российских исследователей, где киберугрозы рассматриваются как часть общей системы экономической безопасности транспортного комплекса. В некоторых исследованиях Международной организации гражданской авиации (ИКАО) подчёркивается, что киберустойчивость авиакомпаний должна рассматриваться в том числе и с точки зрения экономической безопасности, так как нарушения в цепочке авиационного сервиса способны вызвать мультипликативный эффект потерь на уровне всей национальной транспортной системы. [6] Аналогичный подход поддерживает Европейское агентство по кибербезопасности, указывая в отчете ENISA Threat Landscape 2024, что прямые экономические последствия инцидентов в авиации часто сопоставимы с убытками от традиционных техногенных рисков. [7]

В основном выделяют следующие группы кибератак на авиацию: [6]

1. Взлом электронных бортовых систем/Заражение ВПО, когда хакеры используют уязвимости в программном обеспечении и внедряют вредоносное ПО через устройства USB или другие каналы связи;
2. Взлом через беспроводные сети, где применяются специализированные программы для перехвата трафика и получения доступа к защищённым данным, передаваемым по сетям Wi-Fi или Bluetooth;
3. Кибертерроризм - атака авиационных систем, включая полетные управляющие системы, системы навигации и коммуникации;
4. Кибершпионаж (попытка получить доступ к конфиденциальной информации, такой как планы полётов, технологии и системы управления воздушным движением).

Особую актуальность для России проблематика киберугроз приобрела летом 2025 года, когда российская авиакомпания ПАО «Аэрофлот» подверглась масштабной кибератаке, приведшей к сбоям в ИТ-инфраструктуре и массовой отмене рейсов. По официальным данным и сообщениям СМИ, 28 июля 2025 г. было отменено и задержано свыше 100 рейсов (42%), временно нарушена работа систем регистрации и обслуживания пассажиров. [8]

Научный интерес представляет оценка практического сценария последствий киберинцидента для ПАО «Аэрофлот». Опираясь на официальные данные, необходимо рассчитать и сложить три блока потерь:

1) прямые операционные потери (D_1) – стоимость отмененных рейсов (включая расходы на экипаж, компенсацию пассажирам, перерасход топлива и т.д.);
2) восстановительные и капитальные затраты (D_2) – восстановление IT-систем, замена оборудования, усиление безопасности и аудит;
3) косвенные и долгосрочные потери (D_3) – расчет потерянной выручки на будущие периоды (репутационная потеря) и эффект на рыночную капитализацию - снижение общей стоимости акций компании, рассчитанной путём умножения количества акций на текущую рыночную цену за акцию.

По данным журнала «Forbes» 28 июля 2025 года было отменено 108 рейсов, что коснулось порядка 20 тысяч пассажиров. Стоимость одного отмененного рейса по евростандарту – 20 930 евро, [9] с учетом курса рубля на 28 июля 2025 (94,3 рубля) – 1 974 088 рублей. [10] Рыночная капитализация компании оценивается ориентировочно в 200 млрд. рублей (опираясь на публичные финансовые агрегаторы). [11] Предположительно, падение капитализации из-за новостей достигло 3,5% (среднее между 3-4%, зафиксированными в новостных источниках). Приближенно расходы на восстановление IT оценены в 150 млн. рублей (с учетом особенностей авиационной отрасли). Результаты расчетов оформлены в таблицу 1.

Таблица 1 – Сценарная оценка экономического ущерба ПАО «Аэрофлот» в результате кибератаки 28.08.2025г.

Компонент причиненного ущерба	Содержание	Расчёт/Допущение	Сумма, млн. руб.
Прямые потери от отмены рейсов (D_{11})	Произведение числа отмен рейсов и стоимости отмены одного рейса	1 974 088 руб. × 108 рейсов	213
Поддержка пассажиров (~30%) (D_{12})	Питание, компенсация, размещение	30% × 213 млн. руб.	63,9
Итого D_1			**276,9**
IT-восстановление (D_2)	Закупка нового оборудования, восстановление, аудит	Экспертная оценка	150
Итого D_2			**150**
Потеря рыночной капитализации (D_{31})	Произведение процента падения на рыночную капитализацию компании (снижение стоимости акций)	3,5% × 200 млрд. руб.	7 000
Репутационные потери (D_{32})	Выручка компании за 6 месяцев, сниженная на 0,5% (наилучший предполагаемый исход)	0,5% × 350,2 млрд. руб.	1 751
Итого D_3			**8 751**
Общий ущерб* (L - total)		$D_1 + D_2 + D_3$	**~ 9 177, 9***

Составлено авторами на основе [7, 9, 10, 11, 12, 13]

*при увеличении репутационного эффекта с 0,5% до 1%, итоговая сумма ущерба достигает 11 000 млн. руб.

Таким образом, практический расчет последствий кибератаки на информационную систему ПАО «Аэрофлот» 28 июля 2025 года показывает, что совокупный экономический ущерб мог составить 9,4-11 миллиарда рублей. Из полученной суммы около 0,44 миллиарда рублей приходится на реальные краткосрочные денежные потери (прямые операционные расходы и восстановление IT), а остальная часть (9-10 млрд. руб.) связана с косвенным эффектом (падение капитализации и репутационные издержки). Распределение долей основных компонентов ущерба в общем убытке подтверждает, что основным финансовым риском кибератак в авиации становятся не прямые операционные убытки, а эффекты от падения спроса и снижения репутации (рисунок 1).

Рисунок 1 – Доля основных компонентов ущерба в общем финансовом убытке, % (составлено и рассчитано авторами на основе таблицы 1).

Продемонстрируем зависимость совокупного ущерба от величины падения рыночной капитализации компании при фиксированных прочих параметрах (108 отмененных рейсов, стоимость восстановления 150 млн. руб. и низкий репутационный эффект 0,5%). Нам известно, что при падении рыночной капитализации на 3,5% совокупный ущерб составляет 9, 177 млрд. руб. Используем формулу простого линейного уравнения (1) для расчета коэффициента. Вычислив коэффициент k, составим график (рисунок 2):

$$y = kx \qquad (1)$$

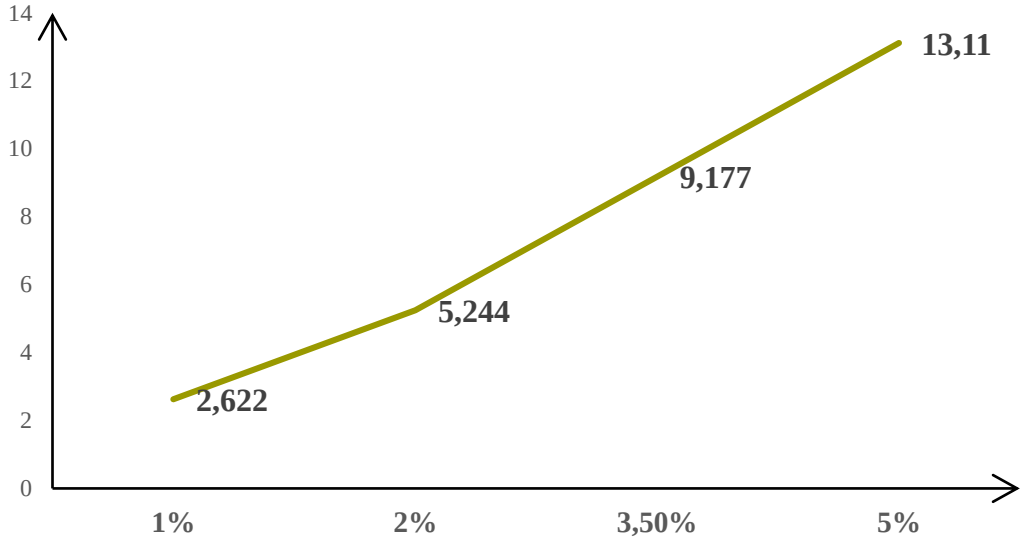

Рисунок 2 – Чувствительность совокупного ущерба к уровню падения рыночной капитализации, млрд. руб. (составлено и рассчитано авторами на основе таблицы 1).

По данным финансовой отчетности компании ПАО «Аэрофлот» скорректированная чистая прибыль (с учетом курсового эффекта от аренды и эффекта от страхового урегулирования отношений с иностранными лизингодателями) компании за первые 6 месяцев 2025 года составила 4,3 млрд. руб. [11] Чтобы оценить долю ущерба воспользуемся формулой (2).

$$\text{Доля ущерба, \%} = \frac{\text{Общий ущерб от кибератаки}}{\text{Скорректированная чистая прибыль,млрд.руб.}} \times 100\% \qquad (2)$$

Воспользовавшись формулой, можно рассчитать долю ущерба в чистой прибыли при низком и высоком репутационном эффекте (0,5 и 1% соответственно):

$$\text{Доля ущерба (низкий эффект)} = \frac{9{,}178}{4{,}3} \times 100\% = 213\%$$

$$\text{Доля ущерба (высокий эффект)} = \frac{11}{4{,}3} \times 100\% = 256\%$$

Таким образом, киберинцидент летом 2025 год мог бы превысить двукратное значение скорректированной чистой прибыли компании, то есть операционные, рыночные и IT-потери от кибератаки значительно превышают прибыль основного бизнеса за рассматриваемый период. Результат подчеркивает критическую значимость мер по киберустойчивости, так как даже краткосрочная атака способна нивелировать прибыль и вызвать финансовые потери.

Инцидент «Аэрофлота» по масштабу можно сопоставить с атакой на один из крупнейших авиаперевозчиков в Европе British Airways в 2018 году, приведшей к штрафу в размере 183 млн. фунтов. Однако в случае с «Аэрофлотом» суть атаки не в краже данных, а в парализации бизнес-процессов, что подчеркивает именно экономическую составляющую риска, а не информационную.

Киберинциденты оказывают значительное влияние на финансовую устойчивость хозяйствующих субъектов: они увеличивают расходы на страхование, инвестиции в резервные мощности IT. На фоне увеличения числа инцидентов страховые компании, развивающие направление покрытия ущерба от последствий кибератак, в 2023 году увеличили сбор страховых премий на 80%. [14] А на фондовом рынке подобные случаи вызывают колебания капитализации, приводящие к росту репутационных рисков.

Репутационный ущерб приводит к снижению доверия контрагентов. Усиливается контроль со стороны государственных органов, ужесточаются требования к отчетности и сертификации систем кибербезопасности, что также приводит к транзакционным издержкам, которые, в свою очередь, влияют на эффективность хозяйствующего субъекта. Следовательно, кибератаки в сфере авиации оказывают системное воздействие на экономическую безопасность авиаперевозчиков.

Учитывая характер и последствия рассмотренной кибератаки на ПАО «Аэрофлот», можно предложить некоторые меры защиты, направленные на снижение рисков киберугроз:

1. Регулярное тестирование систем на предмет уязвимости («Испытание на проникновение»/«Пентест») – специально обученный человек (пентестер) или команда пентестеров проверяют защищенность системы путем взлома;
2. Обмен информацией об инцидентах между авиакомпаниями (через Росавиацию и Минцифры);
3. Разработка многоуровневой защиты с применением сегментации сетей, резервных каналов связи и систем раннего обнаружения угроз;
4. Обучение сотрудников всех подразделений основам цифровой «гигиены» и быстрого реагирования на инциденты (так как человеческий фактор считается наиболее уязвимым).

ЗАКЛЮЧЕНИЕ

В ходе проведенного анализа выявлено, что киберугрозы в сфере гражданской авиации носят комплексный характер и оказывают существенное влияние на экономическую безопасность авиаперевозчиков. Оценка финансовых последствий киберинцидента «Аэрофлота» показала, что суммарный ущерб ПАО «Аэрофлот» в 2025 году мог составить от 9, 177 до 11 млрд. руб. даже при умеренном предположении о масштабе операционных потерь. При этом последствия атаки превышают 213-256% фактической прибыли авиаперевозчика за период.

Таким образом, проведенное исследование показывает, что кратковременное нарушение информационной инфраструктуры способно сформировать серьезный финансовый разрыв, который требует пересмотра стратегии управления рисками и внедрения систем киберустойчивости.

СПИСОК ЛИТЕРАТУРЫ

1) Информационно-аналитический центр по информационной безопасности [Электронный ресурс]. URL: https://www.anti-malware.ru/ (дата обращения: 28.10.2025)

2) European Union Aviation Safety Agency (EASA). Кибербезопасность – Обзор. – Cologne: EASA, 2023. [Электронный ресурс]. URL: https://www.easa.europa.eu/en/domains/cyber-security/overview (дата обращения: 02.11.2025)

3) Черных, Л. В. Актуальные угрозы обеспечения экономической безопасности в киберпространстве / Л. В. Черных, В. Б. Горбунова // Вестник молодежной науки. – 2022. – № 3(35). – DOI 10.46845/2541-8254-2022-3(35)-7-7.

4) Соколов, И. В. Влияние киберугроз на безопасность воздушного транспорта: вызовы и перспективы / И. В. Соколов, Д. А. Костылев. — Текст: непосредственный // Молодой ученый. — 2024. — № 24 (523). — С. 99-102. [Электронный ресурс]. URL: https://moluch.ru/archive/523/115748 (дата обращения: 02.11.2025)

5) Сайт Ассоциации организаций, осуществляющих деятельность в области обеспечения транспортной безопасности «Транспортная безопасность. [Электронный ресурс]. URL: https://atb-tsa.ru/ (дата обращения: 30.10.2025)

6) Родионов М.А., Панкратова А.К., Самотаев М.М. Обеспечение кибербезопасности в авиатранспортной отрасли // Международный журнал гуманитарных и естественных наук. 2025. №5-1 (104). [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/obespechenie-kiberbezopasnosti-v-aviatransportnoy-otrasli (дата обращения: 01.11.2025)

7) SOCKET.DEV. Отчет ENISA 2024 об угрозах предупреждает об учащающихся спонсируемых государством атаках на цепочки поставок. Socket Blog, 2024. [Электронный ресурс]. URL: https://socket.dev/blog/enisa-2024-threat-landscape-report-warns-of-increasing-state-sponsored-supply-chain-attacks (дата обращения: 30.10.2025)

8) Журнал Forbes. [Электронный ресурс]. URL: https://www.forbes.ru/ (дата обращения: 28.10.2025)

9) EUROCONTROL. Standard Inputs for Economic Analyses. Edition 10.0. – Brussels: EUROCONTROL, 2024. – 142 с. – ISBN 978-2-87497-129-7. [Электронный ресурс]. URL: https://www.eurocontrol.int/sites/default/files/2024-05/eurocontrol-standard-inputs-economic-analyses-ed-10.pdf (дата обращения: 03.11.2025)

10) Центральный Банк Российской Федерации. [Электронный ресурс]. URL: https://cbr.ru/ (дата обращения: 30.10.2025)

11) Аэрофлот (AFLT) капитализация МСФО (годовые значения). [Электронный ресурс]. URL: https://smart-lab.ru/q/AFLT/MSFO/market_cap/en/?utm_ (дата обращения: 03.11.2025)

12) ПАО «Аэрофлот». Консолидированная отчётность за 6 мес. 2025 г. : [электронный ресурс] / ПАО «Аэрофлот». – М., 2025. – 56 с. – Режим доступа: https://ir.aeroflot.ru/fileadmin/user_upload/files/mfso2025/Konsolidirovannaja_otchetnost_6m2025.pdf (дата обращения: 03.11.2025)

13) ПАО «Аэрофлот». Консолидированная отчётность за 3 мес. 2025 г.: [электронный ресурс] / ПАО «Аэрофлот». – М., 2025. – 48 с. – Режим доступа: https://ir.aeroflot.ru/fileadmin/user_upload/files/mfso2025/Konsolidirovannaja_otchetnost_3m2025.pdf (дата обращения: 03.11.2025)

14) Киберстрахование: как бизнесу компенсировать убытки после взлома и утечки данных. [Электронный ресурс]. URL: https://pravo.ru/story/254796/ (дата обращения: 02.11.2025)

CYBER THREATS IN CIVIL AVIATION: RISKS TO THE ECONOMIC SECURITY OF AIR CARRIERS

A.T. Melnik, 3rd year student
email: melnikanastasia.t2004@gmail.com
Kaliningrad State Technical University

V.B. Gorbunova, Candidate of Economics, Associate Professor
e-mail: viktoriya.gorbunova@klgtu.ru
Kaliningrad State Technical University

The article examines the impact of cyber threats on air transport security, analyzes the main types of cyber attacks, evaluates potential vulnerabilities in the aviation infrastructure based on official data, and suggests some ways to reduce the risks of cyber threats using various protection mechanisms. The key facts of the incident on July 28, 2025, related to failures in the information systems of PJSC Aeroflot are presented, and the consequences of the cyber attack are assessed.

Keywords: *air transport, cyber threat, economic security, cyber attack, PJSC Aeroflot, civil aviation, cyber incident, risks, damage.*