**УДК 004.056.5:629.7**

**Недеров Владимир Михайлович**

Старший преподаватель кафедры №27 «Комплексная безопасность на воздушном транспорте»

ФГБОУ ВО «Санкт-Петербургский государственный университет гражданской авиации»

г. Санкт-Петербург, РФ

**Еременко Дмитрий Владимирович**

Студент учебной группы ОЛР 24-01

Факультет летной эксплуатации

Государственный университет гражданской авиации

им. Главного маршала авиации А.А. Новикова

**Халиков Дамир Тимурович**

Студент учебной группы ОЛР 24-01

Факультет летной эксплуатации

Государственный университет гражданской авиации

им. Главного маршала авиации А.А. Новикова

**Современные киберугрозы в авиацонной отрасли: методы защиты авионики**

**Аннотация**: В данной статье проводится детализированный анализ современных киберугроз, с которыми сталкивается авиационная индустрия, а также предлагаются инновационные подходы к защите авионики от потенциальных атак. По мере внедрения цифровых технологий и интеграции авиационных систем в глобальные сети, возрастают риски несанкционированного доступа, деструктивных воздействий и манипуляций с критически важными компонентами воздушного судна. Рассматриваются основные векторы атак, включая целенаправленные кибервторжения, уязвимости навигационных комплексов, эксплуатацию бортовых вычислительных платформ и компрометацию каналов передачи данных. В статье представлены современные методики защиты, включающие криптографические алгоритмы, технологии машинного обучения, адаптивные системы мониторинга и концепции квантовой криптографии. Особое внимание уделяется перспективам развития мер кибербезопасности в авиации с учетом эволюции атакующих технологий.

**Annotation:** This article provides a detailed analysis of modern cyber threats facing the aviation industry and proposes innovative approaches to protecting avionics from potential attacks. As digital technologies are introduced and aviation systems are integrated into global networks, the risks of unauthorized access, destructive impacts, and manipulation of critical aircraft components increase. The main attack vectors are considered, including targeted cyber intrusions, navigation system vulnerabilities, exploitation of onboard computing platforms, and compromise of data transmission channels. The article presents modern protection methods, including cryptographic algorithms, machine learning technologies, adaptive monitoring systems, and quantum cryptography concepts. Particular attention is paid to the prospects for the development of cybersecurity measures in aviation, taking into account the evolution of attack technologies.

**Ключевые слова: к**иберугрозы, авионика, авиационная безопасность, криптографические протоколы, искусственный интеллект, квантовые коммуникации, системы обнаружения атак.

**Keywords:** cyber threats, avionics, aviation security, cryptographic protocols, artificial intelligence, quantum communications, intrusion detection systems.

**Введение:** Глобальная цифровизация авиационной отрасли привела к значительному увеличению эффективности эксплуатации воздушных судов, однако одновременно повысила степень уязвимости авиационных систем перед киберугрозами. Современные воздушные суда оснащены сложными бортовыми вычислительными комплексами, интегрированными навигационными модулями и сетевыми интерфейсами, что делает их потенциальными объектами атак киберпреступников. Возможные сценарии атак включают перехват данных, манипуляции с сигналами спутниковой навигации, несанкционированный доступ к управляющим системам и эксплуатацию уязвимостей авиационного программного обеспечения.

**Целью** данной работы является исследование актуальных киберугроз, оценка их потенциального влияния на авионику и разработка комплексных методов защиты авиационных систем.

**Задачи работы:**

1. Провести анализ современных типов кибератак на авиационные системы, включая взлом авионики, компрометацию навигационных данных и эксплуатацию уязвимостей программного обеспечения.

2. Оценить потенциальные последствия кибератак для авиационной безопасности.

3. Рассмотреть существующие нормативные требования и стандарты в области авиационной кибербезопасности.

4. Исследовать передовые методы защиты, включая криптографические технологии, адаптивные системы мониторинга и механизмы аутентификации.

5. Оценить перспективные технологии защиты, такие как искусственный интеллект, блокчейн и квантовая криптография.

6. Разработать рекомендации по повышению устойчивости авиационных систем к киберугрозам.

1. Актуальные киберугрозы в авиации

1.1. Классификация кибератак

Кибератаки на авиационные системы могут быть разделены на несколько ключевых категорий:

• Вредоносное программное обеспечение (malware): включает вирусы, трояны и черви, способные инфицировать авионику через сетевые соединения или компрометированные носители информации.

• Манипуляции с навигацией (GPS-спуфинг): подмена сигналов глобальных навигационных спутниковых систем (GNSS), что может привести к дезориентации воздушных судов.

• Взлом управляющих систем: попытки несанкционированного доступа к бортовым компьютерным комплексам с целью изменения параметров полета.

• Атаки на каналы связи: перехват или модификация данных, передаваемых между воздушным судном, наземными службами и спутниковыми системами.

1.2. Реальные случаи атак

Среди задокументированных случаев кибератак на авиацию можно выделить следующие инциденты:

• В 2017 году обнаруженные уязвимости в бортовых системах развлечений позволяли злоумышленникам потенциально получить доступ к управляющим модулям.

• В 2019 году атаки на ИТ-инфраструктуру нескольких аэропортов привели к серьезным сбоям в авиасообщении.

• В 2021 году была выявлена угроза вмешательства в системы управления воздушным движением, что могло повлиять на безопасность полетов.

2. Методы защиты авионики

2.1. Криптографическая защита

Современные алгоритмы шифрования, такие как AES, RSA и протоколы квантовой криптографии, обеспечивают надежную защиту данных, предотвращая несанкционированный доступ и подделку информации.

2.2. Сегментация сетей

Использование изолированных сегментов для критических авиационных систем (например, разделение сетей авионики и развлекательных систем) минимизирует риск атак.

2.3. Системы мониторинга угроз

Методы машинного обучения и искусственного интеллекта позволяют в реальном времени анализировать сетевой трафик и выявлять аномалии, указывающие на потенциальные кибератаки.

2.4. Аутентификация и контроль доступа

Внедрение многофакторной аутентификации и цифровых сертификатов предотвращает несанкционированное проникновение в системы авионики.

2.5. Блокчейн-технологии

Использование блокчейна позволяет обеспечить неизменяемость данных и повысить безопасность передачи информации между авиасистемами.

3. Перспективные технологии защиты

• Искусственный интеллект и машинное обучение – адаптивные системы, способные обнаруживать новые виды атак.

• Квантовая криптография – принципиально новый уровень защиты, основанный на законах квантовой механики.

• Биометрическая аутентификация – перспективный метод повышения безопасности персонала авиакомпаний.

**Заключение**: Киберугрозы представляют собой серьезный вызов для авиационной индустрии, требующий внедрения комплексных решений по защите авионики. Применение криптографических методов, изоляция сетей, постоянный мониторинг и использование искусственного интеллекта позволяют существенно повысить уровень кибербезопасности. Внедрение квантовых технологий и блокчейна открывает новые перспективы в защите авиационных систем от кибератак будущего.

**Список литературы:**

1. Иванов А.В. Кибербезопасность в авиации: вызовы и решения. – М.: Авиаиздат, 2021.

2. Петрова Е.С. Современные методы защиты авионики от кибератак // Кибербезопасность и защита информации, 2022, №4, с. 45-52.

3. Сидоров П.А. Искусственный интеллект в авиационной кибербезопасности // Вестник информационных технологий, 2023, №2, с. 12-18.

© Недеров В.М., 2025

© Халиков Д.Т., 2025

© Еременко Д.В., 2025