УДК 004.056

БЕЗОПАСНОСТЬ БОРТОВОГО РАЗВЛЕКАТЕЛЬНОГО ОБОРУДОВАНИЯ ВОЗДУШНЫХ СУДОВ ГРАЖДАНСКОЙ АВИАЦИИ

♦♦♦♦♦

SAFETY OF IN-FLIGHT ENTERTAINMENT EQUIPMENT OF CIVIL AVIATION AIRCRAFT

Ялтонская Екатерина Максимовна
студентка кафедры основ радиотехники
и защиты информации,
Московский государственный технический университет
гражданской авиации
ekaterinayaltonskaya03@gmail.com

Сбитнев Александр Васильевич
кандидат технических наук,
доцент кафедры основ радиотехники
и защиты информации,
Московский государственный технический университет
гражданской авиации
a.sbitnev@mstuca.aero

Аннотация. В статье анализируются проблемы безопасности бортовых развлекательных систем, характеризующихся высокой функциональностью и сложной архитектурой. Выделяются ключевые уязвимости, способные привести к утечкам информации и сбоям в работе системы, а также предлагаются комплексные меры по защите, позволяющие обеспечить стабильную и надёжную работу оборудования во время эксплуатации воздушного судна.

Ключевые слова: безопасность, уязвимости, методы защиты, киберугрозы, авиация.

Yaltonskaya Ekaterina Maximovna
Student of the Department
of Fundamentals of Radio Engineering
and Information Security,
Moscow State Technical University
of Civil Aviation
ekaterinayaltonskaya03@gmail.com

Sbitnev Alexander Vasilyevich
Candidate of Technical Sciences,
Associate Professor of the Department
of Fundamentals of Radio Engineering
and Information Security,
Moscow State Technical University
of Civil Aviation
a.sbitnev@mstuca.aero

Annotation. The article analyzes the safety problems of on-board entertainment systems characterized by high functionality and complex architecture. Key vulnerabilities that can lead to information leaks and system failures are highlighted, and comprehensive protection measures are proposed to ensure stable and reliable operation of the equipment during aircraft operation.

Keywords: security, vulnerabilities, protection methods, cyber threats, aviation.

В последние десятилетия авиационная отрасль претерпела значительные изменения, связанные с внедрением новых технологий, которые значительно улучшили комфорт и удобство пассажиров. Одним из таких нововведений стали бортовые информационно-развлекательные системы (БИРС), которые предоставляют пассажирам доступ к различным мультимедийным услугам, включая фильмы, музыку, игры и информацию о полете. Однако с ростом популярности и функциональности этих систем возникает и ряд новых вызовов, связанных с их безопасностью. В условиях современного мира, где киберугрозы становятся все более комплексными, безопасность БИРС становится критически важной для обеспечения не только комфорта, но и безопасности полетов.

Актуальность данной работы обусловлена растущим числом уязвимостей в бортовых развлекательных системах, которые могут быть использованы злоумышленниками для получения несанкционированного доступа к важной информации о полете, а также для вмешательства в нормальную работу систем, что может привести к серьезным последствиям. Игнорирование вопросов безопасности БИРС может поставить под угрозу не только безопасность пассажиров, но и репутацию авиакомпаний, а также целую отрасль в целом.

Структура БИРС обычно включает в себя несколько основных компонентов: серверную часть, интерфейсы для пользователей и выходные устройства, такие как экраны и звукозаписывающее оборудование [1]. Серверы хранят и обрабатывают данные, в то время как интерфейсы обеспечивают взаимодействие с пассажирами. За последние годы произошло значительное развитие в области технологий передачи дан-

ных, например, системы Wi-Fi на борту, что позволяет пассажирам подключаться к сети Интернет во время полета. Эта функция становится неотъемлемой частью опыта полета, но она также открывает возможности для кибератак [2].

С учетом роста популярности цифровых устройств, таких как смартфоны и планшеты, пассажиры ожидают от бортовых систем не только развлечений, но и интерактивных функций. Это может включать в себя возможность персонализировать контент, взаимодействовать с другими пассажирами или даже управлять некоторыми аспектами их путешествия, такими как заказ еды или покупка товаров без необходимости покидать кресло [3]. Подобная функциональность требует от бортовых систем высокой степени надежности и защиты.

Одним из ключевых аспектов безопасности БИРС является соблюдение стандартов, направленных на защиту авиационных систем от киберугроз. Основные требования регламентируются стандартами RTCA DO-326A и DO-356A, которые определяют методы анализа киберрисков, меры защиты и процедуры тестирования.

DO-326A называется «Airworthiness Security Process Specification» («Спецификация процесса обеспечения защиты лётной годности»). В нём изложены ключевые цели и требования по управлению угрозами безопасности при разработке и сертификации воздушных судов, а также методы поддержания уровня безопасности на протяжении всего жизненного цикла самолёта.

DO-356A называется «Airworthiness Security Methods and Considerations» («Методы обеспечения кибербезопасности лётной годности»). Документ в основном посвящён процессам и целям формального соответствия и проверки. В нём описаны принципы архитектуры безопасности, которые также применимы к программному обеспечению.

К основным уязвимостям БИРС можно отнести:

– **Уязвимости программного обеспечения и сетевые атаки.** Развлекательные системы часто содержат веб-интерфейсы и беспроводные модули, подверженные типовым уязвимостям веб-приложений. Исследования показывают, что во многих БИРС выявляются уязвимости из OWASP Top 10 – например, обход аутентификации и эскалация привилегий до уровня администратора. Нередко не проводится должная валидация на серверной стороне: исследователи обнаруживали возможность входа в систему под видом бортпроводника без реальных учетных данных. Также выявлены случаи хранения чувствительных данных без шифрования, что позволило перехватывать информацию о транзакциях [4]. Беспроводные сети БИРС могут быть неправильно сегментированы – отсутствующая изоляция Wi-Fi-сети позволяет злоумышленнику, подключившись, пассивно перехватывать трафик других пассажиров и компонентов борта.

– **Несанкционированный физический доступ пассажиров.** Некоторые атаки требуют физического подключения к компонентам БИРС. Исследователь Крис Робертс сообщал о несанкционированном доступе к внутренней сети самолёта посредством подключения ноутбука к разъёму, расположенному под креслом. В экспериментах отмечалось, что такой доступ потенциально позволяет модифицировать программный код компьютера управления тягой двигателя и инициировать команду набора высоты [5]. Несмотря на сомнения относительно достоверности этих данных и опровержения со стороны Boeing и других экспертов [6], этот случай демонстрирует реальную угрозу, связанную с наличием сервисных портов и кабелей БИРС, которые находятся в зоне досягаемости пассажиров.

– **Недостаточная изоляция от критических систем.** Ключевой принцип безопасности авиации – строгая изоляция пассажирской сети от авионики. В современных лайнерах архитектура сетей поделена на домены: Aircraft Control Domain (ACD) – системы управления полётом, Airline Information Services Domain (AISD) – информационные системы авиакомпании, и Passenger Entertainment Services Domain (PIESD) – пассажирские развлечения и сервисы [7]. При корректной реализации, связь между ними односторонняя (например, данные навигации передаются в БИРС только для отображения карты полёта). Однако, уязвимости в сетевых шлюзах или ошибочная конфигурация могут размыть эту границу. При нарушении сегментации между развлекательной

сетью и системами обеспечения безопасности (например, АЗН-В [8]) злоумышленник, получив доступ к БИРС, может не только перехватывать трафик пассажиров, но и воздействовать на данные, используемые для контроля и управления полётом. Следует отметить, что даже незначительное смешение сетей может привести к утечке или искажению критически важной информации, что, в свою очередь, снизит надёжность работы системы АЗН-В и повлияет на общую безопасность воздушного судна. В 2018 г. в результате тестирования безопасности Boeing 737 были обнаружены уязвимости, теоретически позволявшие через сеть развлечений проникнуть в управляющие системы самолёта [9]. Этот сценарий крайне сложен, но в случае успеха атаки последствия были бы катастрофическими – вплоть до потери контроля над лайнером. Таким образом, даже редкие сбои изоляции рассматриваются как серьёзная угроза. Другой пример – исследование IOActive, выявившее возможность перехода с взломанного бортового интернет-модема на другие устройства в сегменте сети самолёта [10].

– **Другие потенциальные угрозы.** БИРС могут стать целью атак типа отказ в обслуживании (DoS) – злоумышленник, получив доступ, способен отключить систему развлечений, оставив пассажиров без связи и информации [11]. Это не несёт прямой угрозы безопасности полёта, но создает стрессовую обстановку и может отвлекать экипаж. Ещё одна категория – кража контента и мошенничество.

Безопасность бортовых информационно-развлекательных систем (БИРС) требует интеграции множества методов защиты, каждый из которых направлен на предотвращение кибератак, защиту информации и обеспечение полной работоспособности системы во время полета.

Учитывая описанные выше уязвимости, можно выделить следующие методы защиты БИРС:

– **Сегментация и изоляция сетей.** Главное средство защиты – строгая архитектурная изоляция БИРС от критичных систем. Реализуются аппаратные и программные шлюзы с белыми списками: даже при компрометации пассажирской сети, команды не могут повлиять на авионику. В ряде случаев применяются системы односторонней передачи данных – например, навигационная информация передаётся в БИРС (для карты маршрута), но обратная передача исключена [12]. Wi-Fi для пассажиров размещается в отдельном VLAN/сегменте; точки доступа сконфигурированы так, чтобы устройства пассажиров не могли напрямую видеть бортовые серверы.

– **Шифрование и защита данных.** Все критичные данные, циркулирующие через БИРС, должны передаваться в зашифрованном виде. Производители обновляют устаревшие протоколы: если раньше некоторые БИРС могли использовать небезопасные протоколы без шифрования, то новые версии прошивок требуют HTTPS и проверку сертификатов. Например, уязвимость в приложении FlySmart для пилотов, связанная с отключённой проверкой сертификатов, была устранена обновлением, включившим ATS-защиту (App Transport Security). Также практикуется шифрование хранилищ: данные о пассажирах, список контента и другие данные – все эти файлы на бортовых серверах шифруются, чтобы злоумышленник не смог их прочесть даже при получении доступа.

– **Мониторинг и обнаружение вторжений.** Круглосуточный мониторинг сети – ещё один слой защиты. Крупные поставщики БИРС (напр. Panasonic Avionics) создали центры мониторинга безопасности (SOC), которые в реальном времени следят за сетевым трафиком на борту и подключёнными устройствами. Анализируются аномалии: необычная сетевая активность между пассажирским устройством и сервером, попытки сканирования портов, множественные ошибки аутентификации и т.п. При выявлении подозрительных событий SOC оповещает авиакомпанию; экипаж может получить рекомендацию перезагрузить БИРС или отключить клиентский доступ. На уровне самолёта устанавливаются системы обнаружения вторжений (IDS/IPS) адаптированные под авиационные сети. Они контролируют трафик и блокируют любые пакеты, нарушающие заданные правила.

– **Управление обновлениями и патчами.** Поскольку многие уязвимости возникают из-за устаревшего ПО, критически важно своевременно обновлять БИРС. Авиакомпании всё чаще заключают соглашения с поставщиками на регулярное обновление прошивок по безопасному каналу. Например, новая схема предусматривает ав-

томатическое обновление контента и ПО БИРС через Wi-Fi при приземлении, вместо ручной загрузки флеш-накопителей. Конечно, такой онлайн-доступ также должен быть защищён – через VPN и цифровую подпись пакетов, чтобы исключить внедрение вредоносного кода. Производители реализуют механизмы secure boot – сервер БИРС загружает только подписанное ПО. При выпуске патчей для обнаруженных уязвимостей оперативно рассылаются бюллетени службам техобслуживания, и в ближайший плановый техосмотр самолёта включается обновление.

– **Аутентификация и контроль доступа.** Защита БИРС включает строгую систему авторизаций. Доступ к административным панелям БИРС (для бортпроводников или техников) требует многофакторной аутентификации – например, ввода PIN-кода и использования аппаратного токена. Все пароли по умолчанию в системе должны быть изменены на уникальные при установке. Экипаж имеет ограниченный по времени и функциям доступ. Логи доступа постоянно пишутся и шифруются, что позволяет отследить все действия. Пассажирам же открыты только доступы с минимальными привилегиями. Идентификация аномалий также связана с управлением доступом – например, если пассажирский терминал вдруг пытается выполнить команду, разрешённую только для уровня экипажа, система должна сразу это заблокировать и сгенерировать сигнал тревоги.

В заключение, безопасность бортовых развлекательных систем – это важный элемент обеспечения безопасности полётов. Современные системы, помимо предоставления развлекательного контента, собирают и обрабатывают множество данных, что открывает дополнительные возможности для киберугроз. Для защиты этих систем от несанкционированного доступа и возможных сбоев применяются комплексные меры – от разделения сетей и шифрования данных до постоянного контроля и регулярного обновления программного обеспечения. Соблюдение международных стандартов и адаптация их к национальным требованиям помогает создать надёжную защиту, которая обеспечивает безопасность как пассажиров, так и работы всего воздушного судна.

Литература

1. RU27373U1 – Бортовая информационная... – Яндекс.Патенты // yandex.ru. – URL : https://yandex.ru/patents/doc/ru27373u1_20030127, свободный. – Загл. с экрана (дата обращения 22.03.2025).
2. Какими бывают и что в себя включают бортовые... | Арсис. www.arsis.ru. – URL : https://www.arsis.ru/blog/birs, свободный. – Загл. с экрана (дата обращения 02.03.2025).
3. Авиационный супермаркет: выбираем систему... // alexcheban.livejournal.com. – URL : https://alexcheban.livejournal.com/334826.html, свободный. – Загл. с экрана (дата обращения 02.03.2025).
4. InFlight Entertainment systems security analysis // dcodx.com. – URL : https://dcodx.com/inflight-entertainment-systems-security-analysis, свободный. – Загл. с экрана (date of application 08.04.2025).
5. Boeing, IFE experts hit back at hacker claims in FBI report // runwaygirlnetwork.com. – URL : https://runwaygirlnetwork.com/2015/05/boeing-ife-experts-hit-back-at-hacker-claims-in-fbi-report, свободный. – Загл. с экрана экрана (date of application 02.04.2025).
6. How Secure Are IFEC Systems? // interactive.aviationtoday.com. – URL : https://interactive.aviationtoday.com/avionicsmagazine/december-2017-january-2018/how-secure-are-ifec-systems, свободный. – Загл. с экрана экрана (date of application 12.03.2025).
7. FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks // www.gao.gov. – URL : https://www.gao.gov/assets/gao-21-86.pdf, свободный. – Загл. с экрана экрана (date of application 28.03.2025).
8. Антонов А.А. Исследование эффективности методов шифрования в системе автоматического зависимого наблюдения-вещания / А.А. Антонов, М.А. Повалишина // Научные труды КубГТУ. – 2024. – № 2. – С. 111–121.
9. The State of Cybersecurity in Commercial Aviation // silentbreach.com. – URL : https://silentbreach.com/BlogArticles/the-state-of-cybersecurity-in-commercial-aviation, свободный. – Загл. с экрана экрана (date of application 05.04.2025).
10. Airplane Modems Not Vulnerable to ‘Backdoor’ Cyber Attacks / Хабр // www.aviationtoday.com. – URL : https://www.aviationtoday.com/2018/08/24/backdoor-hacking-airplane-modems-no-longer-risk, свободный. – Загл. с экрана экрана (дата обращения 02.03.2025).

11. In Flight Entertainment systems security analysis // dcodx.com. – URL : https://dcodx.com/inflight-entertainment-systems-security-analysis, свободный. – Загл. с экрана экрана (дата обращения 02.04.2025).
12. Causing incidents with in-flight entertainment systems // www.pentestpartners.com. – URL : https://www.pentestpartners.com/security-blog/causing-incidents-with-in-flight-entertainment-systems, свободный. – Загл. с экрана экрана (дата обращения 03.03.2025).

References

1. RU27373U1 – On-board information... – Yandex.Patents // yandex.ru – URL : https://yandex.ru/patents/doc/ru27373u1_20030127, free. – Caption from the screen (date of application 03/22/2025).
2. What are the types and what do the onboard ones include? | Arsis // www.arsis.ru. – URL : https://www.arsis.ru/blog/birs, free. – Caption from the screen (date of application 03/02/2025).
3. Aviation supermarket: choosing a system... // alexcheban.livejournal.com. – URL : https://alexcheban.livejournal.com/334826.html, free. – Cover from the screen (date of application 03/02/2025).
4. InFlight Entertainment systems security analysis // dcodx.com. – URL : https://dcodx.com/inflight-entertainment-systems-security-analysis, free. – Caption from the screen (date of application 04/08/2025).
5. Boeing, IFE experts hit back at hacker claims in FBI report // runwaygirlnetwork.com. – URL : https://runwaygirlnetwork.com/2015/05/boeing-ife-experts-hit-back-at-hacker-claims-in-fbi-report, free. – Caption from the screen (date of application 04/02/2025)
6. How Secure Are IFEC Systems? // interactive.aviationtoday.com. – URL : https://interactive.aviationtoday.com/avionicsmagazine/december-2017-january-2018/how-secure-are-ifec-systems, free. - Caption from the screen (date of application 12.03.2025).
7. FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks // www.gao.gov. – URL : https://www.gao.gov/assets/gao-21-86.pdf, free. – Caption from the screen (date of application 03/28/2025).
8. Antonov A.A. Investigation of the effectiveness of encryption methods in the system of automatic dependent surveillance-broadcasting / A.A. Antonov, M.A. Povalishina // Scientific works of KubSTU. – 2024. – № 2. – P. 111–121.
9. The State of Cybersecurity in Commercial Aviation // silentbreach.com. – URL : https://silentbreach.com/BlogArticles/the-state-of-cybersecurity-in-commercial-aviation, free. – Caption from the screen (date of application 04/05/2025).
10. Airplane Modems Not Vulnerable to ‘Backdoor’ Cyber Attacks / Habr // www.aviationtoday.com. – URL : https://www.aviationtoday.com/2018/08/24/backdoor-hacking-airplane-modems-no-longer-risk, free. – Caption from the screen (date of application 03/02/2025).
11. InFlight Entertainment systems security analysis // dcodx.com. – URL : https://dcodx.com/inflight-entertainment-systems-security-analysis, free. - Caption from the screen (date of application 04/02/2025).
12. Causing incidents with in-flight entertainment systems // www.pentestpartners.com. – URL : https://www.pentestpartners.com/security-blog/causing-incidents-with-in-flight-entertainment-systems, free. – Caption from the screen (date of application 03.03.2025).