Международная организация гражданской авиации

A42-WP/324[1]
EX/138
29/7/25

РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 42-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 13 повестки дня. Авиационная безопасность. Политика

СУЩЕСТВУЮЩАЯ ПРАКТИКА И УСОВЕРШЕНСТВОВАНИЯ В ВОПРОСАХ КИБЕРБЕЗОПАСНОСТИ ДЛЯ МЕЖДУНАРОДНОЙ ГРАЖДАНСКОЙ АВИАЦИИ

(Представлено Сальвадором от имени государств – членов КОСЕСНА[2])

КРАТКАЯ СПРАВКА

Технологии жизненно важны для авиационного сектора, они способствуют развитию туризма, торговли и глобальной связности, стимулируют экономический рост и повышают качество жизни. Достижения в области авионики позволили значительно улучшить аэронавигационное обслуживание, повысить безопасность полетов и эффективность эксплуатации самолетов. Технологические инновации в этом секторе необходимы для поддержания конкурентоспособности и удовлетворения растущих потребностей в авиаперевозках.

Кибербезопасность гражданской авиации стала краеугольным камнем с точки зрения обеспечения безопасности полетов и эффективности аэронавигации. В настоящее время отрасль функционирует в динамичной среде, характеризующейся постоянно развивающимися киберугрозами, что требует стратегического и скоординированного подхода для обеспечения защиты ключевых объектов инфраструктуры.

В данном рабочем документе представлен анализ существующей практики обеспечения кибербезопасности в авиационном секторе и предложены ключевые аспекты, которые следует рассмотреть для ее совершенствования и внедрения в будущем в целях повышения устойчивости авиационной системы к возникающим киберугрозам.

Действия: Ассамблее предлагается:

a) принять к сведению представленную информацию;
b) поручить ИКАО оценить и усовершенствовать стратегии обеспечения кибербезопасности, применяя подходы, основанные на передовом международном опыте, обмене информацией и новых технологиях;
c) поручить ИКАО продолжать оказывать поддержку государствам в области создания и внедрения нормативной базы для регулирования вопросов кибербезопасности, обучения и повышения квалификации персонала в этой области, а также в области разработки планов обеспечения киберустойчивости, которые предусматривают включение кибербезопасности в Национальные планы обеспечения авиационной безопасности (НПАБ).

Стратегические цели	Данный рабочий документ связан со следующими стратегическими целями: *a) Каждый полет безопасен и защищен* *b) Ни одна страна не остается без внимания* *c) Экономическое развитие воздушного транспорта обеспечивает экономическое процветание и социальное благополучие для всех*

[1] Текст на испанском языке представлен Сальвадором.
[2] Белиз, Гватемала, Гондурас, Коста-Рика, Никарагуа и Сальвадор.

Финансовые последствия	
Справочный материал	Нормативно-правовая база Национального института стандартов и технологий (НИСТ) Doc 9985, *"Руководство по безопасности системы организации воздушного движения"* Doc 10075, *Действующие резолюции Ассамблеи (по состоянию на 6 октября 2016 года)* Doc 10161, *"Глобальная дорожная карта обеспечения безопасности полетов"* Приложение 17 *"Авиационная безопасность"*

1. ВВЕДЕНИЕ

1.1. Технологии жизненно важны для авиационного сектора, а технологические достижения принесли огромную пользу в вопросах предоставления аэронавигационных услуг. Такие системы, как навигация, основанная на характеристиках (PBN), радиовещательное автоматическое зависимое наблюдение (ADS-B) и системы управления воздушным движением (ОрВД), изменили способ управления полетами, повысив точность, безопасность и эффективность полетов. Эти системы позволяют лучше планировать маршруты, сокращать задержки и оптимизировать использование воздушного пространства.

1.2. Кибербезопасность приобретает особое значение для гражданской авиации, поскольку ее деятельность все больше зависит от взаимосвязанных цифровых систем, в которых технологические ресурсы имеют решающее значение для безопасной и эффективной работы гражданской авиации. Технологический прогресс принес с собой серьезные проблемы, в том числе кибератаки на системы управления воздушным движением, эксплуатантов аэропортов и воздушных судов. Поэтому стратегически важно защитить их от киберугроз. Необходимо обеспечивать безопасность и доступность этих систем, чтобы избежать сбоев в работе, которые могут сказаться на безопасности эксплуатации и бесперебойности авиаперевозок. Кибербезопасность в этом смысле не только защищает данные и системы, но и укрепляет доверие к глобальной аэронавигационной инфраструктуре.

1.3. Для реагирования на такие угрозы государства принимают различные меры кибербезопасности, основанные на международных стандартах, например стандарты, разработанные ИКАО, ИАТА и ЕАБП. Однако все еще остаются пробелы в плане обеспечения комплексной защиты авиационной экосистемы, которые необходимо устранить.

1.4. Настоящий документ подготовлен в соответствии с резолюцией **A39-19** Ассамблеи ИКАО, в которой международное сообщество признает, что обеспечение кибербезопасности является первоочередной задачей для гражданской авиации; Резолюцией **A40-10** о Стратегии авиационной кибербезопасности ИКАО с ее коллегиальным и междисциплинарным подходом; и резолюцией **A41-19**, в которой подтверждается неотложная необходимость решения вопросов кибербезопасности и киберустойчивости.

2. ТЕКУЩИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В КОСЕСНА

2.1 Важность внедрения Системы кибербезопасности ИКАО учитывается при выявлении и обнаружении киберинцидентов, а также защите от них, реагировании на них и восстановлении после них. В регионе и за его пределами ведется обмен передовым опытом с такими международными организациями, как ИАТА, ЕВРОКОНТРОЛЬ и ЕАБП.

2.2 Что касается управления киберрисками, то в настоящее время КОСЕСНА закладывает основы для применения методологии анализа рисков (ИСО 27001, НИСТ и MITRE ATT&CK). Внедрение этих методик позволит непрерывно оценивать уязвимость авиационных систем и комплексно обеспечивать кибербезопасность систем аэронавигационного обслуживания в регионе Центральной Америки. Кроме того, КОСЕСНА намерена создать Центр управления безопасностью (SOC), что позволит организациям укреплять свою безопасность за счет непрерывного наблюдения, расширенного анализа угроз и оперативного реагирования на инциденты. С помощью этого инструментария мы стремимся применять на практике стратегический и действенный подход к защите систем, данных и пользователей, минимизируя риски и гарантируя бесперебойную работу бизнеса и соответствие нормативным требованиям.

2.3 Что касается обучения и повышения осведомленности, то в настоящее время мы разрабатываем базовые курсы по кибербезопасности для всех сотрудников корпорации, а также будут созданы специализированные курсы для обучения отдельных сотрудников передовым методам и тенденциям в вопросах кибербезопасности.

3. АСПЕКТЫ, КОТОРЫЕ НЕОБХОДИМО УЧИТЫВАТЬ ДЛЯ ПОВЫШЕНИЯ УРОВНЯ АВИАЦИОННОЙ КИБЕРБЕЗОПАСНОСТИ

3.1 Сотрудничество и обмен информацией с другими поставщиками аэронавигационного обслуживания могут быть налажены путем создания безопасных платформ для обмена информацией об угрозах и уязвимостях в режиме реального времени. Этого можно достичь путем укрепления регионального сотрудничества в области кибербезопасности на основе многосторонних соглашений.

3.2 Необходимо создать и внедрить нормативно-правовую базу для регулирования вопросов кибербезопасности. Такая база должна содержать четкие рекомендации и стандарты, которым организации могут следовать для защиты своих цифровых активов и обеспечения конфиденциальности данных. Внедрение надежной нормативной базы поможет снижать риски, предотвращать инциденты с безопасностью и обеспечивать бесперебойную работу.

3.3 Программы подготовки по вопросам кибербезопасности должны включать технические и практические аспекты, например управление инцидентами, анализ рисков и применение защитных мер. Кроме того, важно развивать навыки общения и сотрудничества, чтобы сотрудники могли работать в команде и обмениваться знаниями по вопросам кибербезопасности. Инвестиции в обучение – это экономически эффективная стратегия, которая повышает устойчивость организации к киберугрозам.

3.4 Повышение осведомленности сотрудников о кибербезопасности помогает снижать количество ошибок из-за человеческого фактора, которые являются основной причиной инцидентов в плане безопасности. По данным таких исследований, как *"Global Risks Report 2022"* от Глобального экономического форума, 95 % проблем с кибербезопасностью вызваны человеческим фактором. Осведомленность об угрозах и передовая практика по вопросам кибербезопасности помогают сформировать в организации культуру, ориентированную на обеспечение цифровой безопасности.

3.5 Нам следует разработать план обеспечения киберустойчивости, который позволит интегрировать вопросы кибербезопасности в Национальные планы обеспечения авиационной безопасности (НПАБ). Такие планы должны включать стратегии восстановления после кибератак, чтобы минимизировать операционные последствия.

3.6 Мы должны активно выявлять и устранять уязвимости, чтобы защитить технологическую инфраструктуру и обеспечить безопасность данных.

3.7 Сотрудничество с экспертами по кибербезопасности из различных отраслей, например технологической, банковской и других, может стать источником ценных знаний и дать доступ к специализированным ресурсам, которые позволят повысить защищенность авиационных систем.

3.8 Внедрение новых технологий, например искусственного интеллекта и облачных вычислений, открывает возможности для повышения эффективности и безопасности гражданской авиации. Однако крайне важно, чтобы при внедрении этих технологий применялись надежные меры обеспечения кибербезопасности для защиты от потенциальных уязвимостей и угроз. Безопасное внедрение этих технологий может изменить облик отрасли, но потребует тщательного планирования и надлежащего управления рисками.

4. ВЫВОДЫ

4.1 Кибербезопасность является ключевым элементом эксплуатационной безопасности и эффективности гражданской авиации. Защита авиационных систем от киберугроз необходима для обеспечения безопасности полетов и бесперебойной работы воздушного транспорта. Несмотря на значительный прогресс, достигнутый в осуществлении защитных мер, по-прежнему остаются проблемы, требующие немедленного решения.

4.2 Укрепление международного сотрудничества и обмена информацией между организациями авиационного сектора с помощью безопасных платформ и многосторонних соглашений имеет жизненно важное значение для повышения уровня кибербезопасности, а также интеграции передовых технологий и применения инициативного подхода к управлению киберрисками в международной гражданской авиации.

4.3 Внедрение таких международных стандартов, как ISO/IEC 27001 и НИСТ CSF, позволит получать четкие рекомендации по защите цифровых активов и обеспечению конфиденциальности данных и поможет снизить риски и предотвращать инциденты.

4.4 Обучение персонала и повышение осведомленности о кибербезопасности снижает количество ошибок из-за человеческого фактора, расширяет возможности реагирования на угрозы и повышает устойчивость организаций.

4.5 Для защиты технологической инфраструктуры крайне важно, работая на упреждение, выявлять и устранять уязвимости с помощью оценки рисков, обновлений, тестирования на проникновение и постоянного мониторинга.

4.6 Сотрудничество с экспертами по кибербезопасности из различных отраслей и использование специализированных услуг, например SOC и MSSP, позволяет осуществлять непрерывный мониторинг и оперативно реагировать на инциденты, обеспечивая более надежную защиту авиационных систем.

4.7 Внедрение таких технологий, как искусственный интеллект и облачные вычисления с надежными мерами кибербезопасности создает возможности для повышения безопасности полетов и эффективности гражданской авиации, обеспечивая безопасное и эффективное внедрение таких технологий.

— КОНЕЦ —