



РАБОЧИЙ ДОКУМЕНТ

АССАМБЛЕЯ — 42-Я СЕССИЯ

ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

Пункт 13 повестки дня. Авиацонная безопасность. Политика

ЦЕЛОСТНЫЙ ПОДХОД К АВИАЦИОННОЙ КИБЕРБЕЗОПАСНОСТИ: ОТ КОНЦЕПЦИИ К РЕАЛЬНОСТИ

(Представлено Данией от имени Европейского союза и его государств-членов¹, других государств - членов Европейской конференции гражданской авиации² и ЕВРОКОНТРОЛЕМ и при поддержке Бразилии, Казахстана и Перу)

КРАТКАЯ СПРАВКА

По мере того как гражданская авиация становится все более взаимосвязанной, киберугрозы создают все более серьезные факторы риска для авиационной безопасности, безопасности полетов и эффективности. В настоящем документе подчеркивается необходимость целостного подхода к кибербезопасности в целях решения проблемы разрозненности усилий по снижению связанных с кибербезопасностью факторов риска.

Этот целостный подход должен применяться к ключевым принципам кибербезопасности, таким как создание структур управления, внедрение концепции безопасности в системы на этапе разработки, проактивное управление факторами киберриска, согласованное с протоколами обеспечения безопасности полетов и авиационной безопасности, а также квалификационная подготовка по вопросам кибербезопасности во всех областях авиации. Этот подход подчеркивает устойчивость жизненного цикла, глобальную координацию и интеграцию с существующими стратегиями. ИКАО предлагается обновлять политику, расширять сотрудничество и продвигать инициативы по наращиванию потенциала в целях достижения единообразия практики обеспечения кибербезопасности во всем мире.

Действия: Ассамблее предлагается:

- а) призвать ИКАО продолжать совершенствовать свою политику, Стандарты и Рекомендуемую практику для поддержки целостного подхода к кибербезопасности и сотрудничества всех ее рабочих органов в целях интеграции кибербезопасности с другими нормативными базами, способствуя всестороннему и скоординированному осуществлению мер кибербезопасности в гражданской авиации;

¹ Австрия, Бельгия, Болгария, Венгрия, Германия, Греция, Дания, Ирландия, Испания, Италия, Кипр, Латвия, Литва, Люксембург, Мальта, Нидерланды, Польша, Португалия, Румыния, Словакия, Словения, Финляндия, Франция, Хорватия, Чехия, Швеция и Эстония.

² Азербайджан, Албания, Армения, Босния и Герцеговина, Грузия, Исландия, Монако, Норвегия, Республика Молдова, Сан-Марино, Северная Македония, Сербия, Соединенное Королевство, Турция, Украина, Черногория и Швейцария

б) настоятельно призывать государства-члены и все соответствующие заинтересованные стороны в области авиации принять комплексный подход к обеспечению кибербезопасности в рамках всей экосистемы гражданской авиации для использования согласованного, проактивного и основанного на жизненном цикле подхода к управлению факторами риска, связанными с киберугрозами, и их снижению; с) призвать ИКАО продвигать инициативы по наращиванию потенциала в целях оказания поддержки государствам-членам в принятии целостного подхода к кибербезопасности, максимально эффективно используя проводимые мероприятия по наращиванию потенциала и свои собственные ресурсы; д) признать в резолюции A42-XX, предлагаемой для обновления резолюции A41-19 Ассамблеи "Решение проблемы кибербезопасности в гражданской авиации", необходимость комплексного устранения киберугроз и факторов риска для гражданской авиации.	
<i>Стратегические цели</i>	Настоящий рабочий документ касается стратегической цели <i>"Каждый полет безопасен и надежен."</i>
<i>Финансовые последствия</i>	<i>Действия, указанные в настоящем документе, будут зависеть от наличия ресурсов в бюджете Регулярной программы и/или от внебюджетных взносов.</i>
<i>Справочный материал:</i>	Резолюция A41-19 Ассамблеи

1. ВВЕДЕНИЕ

1.1 По мере того как гражданская авиация становится все более взаимосвязанной и цифровизированной, киберугрозы создают все более серьезные факторы риска для безопасности полетов, авиационной безопасности и эффективности. Это усугубляется скоростью развития событий в области больших данных и усовершенствованными функциями и сервисами обработки данных. Помимо прочего, по мере того как системы и приложения, как передовые, так и устаревшие, становятся все более интегрированными и взаимосвязанными за счет расширения сетевых возможностей и использования "умных" компонентов, гражданская авиация эволюционирует в очень прогрессивную и сложную экосистему.

1.2 Такая взаимосвязанность ставит новые задачи в области защиты конфиденциальности, обеспечения целостности и доступности информации. Эти задачи необходимо решать комплексно, обеспечивая безопасность всех аспектов авиационной экосистемы от проектирования и эксплуатации систем до стратегического управления в целях последовательного применения во всем мире.

1.3 Во избежание фрагментарных и изолированных усилий целостный подход расширяет концепции кибербезопасности во всех аспектах организационной практики, упреждающие и ответные меры и возможности полномочных органов и отрасли. Такой комплексный подход обеспечивает согласование усилий по обеспечению кибербезопасности во всех видах деятельности гражданской авиации, что позволяет согласованно управлять факторами риска и обеспечения устойчивости. Такой подход способствует интеграции традиционных аспектов обеспечения безопасности полетов и авиационной безопасности с вопросами кибербезопасности в системах и стратегиях организационного управления, повышая их общую эффективность и действенность.

1.4 Создание Советом ИКАО в трехлетний период 2022-2025 годов Специального координационного комитета по кибербезопасности (АНССС) представляет собой позитивный и важный шаг на пути к более скоординированному решению проблемы обеспечения

кибербезопасности. Эта инициатива открывает широкие возможности для дальнейшего продвижения действительно целостного и интегрированного подхода к кибербезопасности. Системное внедрение принципов кибербезопасности во все виды деятельности, нормативно-правовую базу и стратегические приоритеты ИКАО будет способствовать повышению глобальной устойчивости и обеспечению готовности авиационного сектора к противостоянию киберугрозам с их сложным и меняющимся характером.

2. ОБСУЖДЕНИЕ

2.1 Целостный подход обеспечивает оценку киберугроз и уменьшение факторов риска в рамках всей экосистемы, а не в рамках изолированных компонентов. Внедрение принципов кибербезопасности в процесс разработки и функционирования систем может позволить государствам-членам и заинтересованным сторонам в сфере авиации повысить устойчивость и способствовать созданию безопасного и надежного авиационного сектора, готового к будущему.

Такой целостный подход должен направлять процесс применения таких основных кибер-принципов, как:

2.1.1 **Управление кибербезопасностью:** целостный подход к управлению совершенствует процесс принятия решений, распределения ресурсов и сотрудничества между секторами авиации. Благодаря эффективному управлению обеспечивается согласование киберзадач со стратегическими и операционными целями, создается структурированная основа для управления ресурсами. В его рамках определяются ключевые заинтересованные стороны, процессы принятия решений, нормативно-правовая база и политика для руководства действиями в области кибербезопасности, что содействует процессу выявления угроз и факторов риска. Кроме того, управление кибербезопасностью должно органично интегрироваться с вопросами обеспечения безопасности полетов и авиационной безопасности и устойчивости деятельности.

2.1.2 **Кибербезопасность на этапе разработки:** целостный подход по принципу "кибербезопасность на этапе разработки" рассматривает кибербезопасность в качестве основного элемента авиационной экосистемы, а не дополнения к ней. Такой подход полезен, поскольку позволяет организациям проактивно устранять уязвимые места и повышать устойчивость путем внедрения принципов кибербезопасности на каждом этапе развития. В сочетании с методологией "безопасности по умолчанию" такой подход совершенствует авиационную инфраструктуру и процессы от концепции до эксплуатации. Эффективное внедрение предусматривает моделирование угроз на ранней стадии, безопасные инженерные принципы и оценки факторов риска жизненного цикла для упреждающего устранения уязвимых мест. Непрерывный мониторинг, регулярное обновление и автоматизированные механизмы реагирования еще больше повышают гибкость системы в борьбе с возникающими киберугрозами, способствуя обеспечению надежной кибербезопасности в рамках всей авиационной экосистемы.

2.1.3 **Управление факторами киберриска:** на фоне быстро меняющихся технологий и процессов обработки данных в гражданской авиации крайне важно выявлять, обеспечивать защиту и устойчивость критически важных активов и инфраструктур (например, ОрВД) от кибератак, в том числе от новых угроз, таких как ИИ. Взаимосвязанный характер современных систем расширяет спектр киберугроз, что обуславливает необходимость комплексного подхода к управлению факторами киберриска. Увязывая управление факторами киберриска с другими областями управления факторами риска, авиация может создать комплексную и устойчивую структуру,

которая обеспечивает баланс между безопасностью полетов, авиационной безопасностью и эффективностью. Такая стратегия расширяет возможности уменьшать факторы риска и повышает устойчивость к возникающим киберугрозам.

2.1.4 Знания и компетенции в области кибербезопасности: разработка целостного подхода к обучению по вопросам кибербезопасности в авиации имеет важное значение для формирования надежных навыков. Эта комплексная стратегия гарантирует, что люди приобретут необходимые навыки эффективного управления факторами риска и мерами обеспечения кибербезопасности. Обучение должно быть практическим, ориентированным на конкретные функции и сочетать в себе теоретические знания с практическим опытом. Культура непрерывного образования помогает авиационному персоналу быть в курсе последних практических методов и тенденций, применять передовую практику, что позволяет персоналу выявлять уязвимые места и реализовывать эффективные стратегии по их устранению. Регулярные программы, практикумы и моделирование должны быть ориентированы на все уровни, не ограничиваясь ИТ-персоналом, а охватывая всех сотрудников. Такой подход к обучению не только укрепляет общую киберустойчивость авиационной экосистемы, но и дает всем сотрудникам возможность предвосхищать киберугрозы и лучше реагировать на них, повышая уровень кибербезопасности сектора.

2.2 Являясь мировым лидером в области распространения передового опыта в сфере авиации, ИКАО играет решающую роль в укреплении кибербезопасности авиации. Учитывая различия в уровнях зрелости и ресурсов государств, ИКАО следует содействовать инициативам по наращиванию потенциала, чтобы оказывать поддержку государствам-членам для принятия целостного подхода к кибербезопасности. При этом ИКАО следует наилучшим образом использовать проводимые мероприятия по наращиванию потенциала (например, межрегиональные семинары по инновациям и кибербезопасности, организуемые в рамках проектов CASE, которые финансируются Европейской комиссией и осуществляются Европейской конференцией гражданской авиации (ЕКГА), учебные курсы ЕКГА по кибербезопасности) и свои собственные ресурсы. Эти инициативы должны способствовать применению последовательного и скоординированного подхода к укреплению потенциала в области кибербезопасности при одновременном расширении международного сотрудничества на основе обмена передовым опытом.

2.3 Кроме того, ИКАО должна обеспечить, чтобы ее Стандарты и Рекомендуемая практика, политика и инструменты постоянно обновлялись, предоставляя государствам-членам необходимую основу для эффективного управления киберугрозами и применения целостного подхода к кибербезопасности. Кроме того, рабочие органы ИКАО должны укреплять свое сотрудничество для того, чтобы эффективно объединять положения о кибербезопасности с другими нормативными требованиями. В этом контексте Специальный координационный комитет по кибербезопасности (АНССС) играет определенную роль в оказании содействия и руководстве этим процессом координации в поддержку реализации комплексной и согласованной стратегии в рамках всего авиационного сектора.

2.4 Для продвижения этого комплексного подхода 42-ой сессии Ассамблеи ИКАО предлагается признать в резолюции A42-XX, обновляющей резолюцию A41-19 Ассамблеи, необходимость комплексного подхода к устранению киберугроз и факторов риска для гражданской авиации. Такое признание на уровне Ассамблеи укрепит приверженность государств-членов принципу системного включения вопросов кибербезопасности во все виды авиационной деятельности, обеспечивая глобальное согласование и повышая коллективную устойчивость сектора.

3. **ДЕЙСТВИЯ**

Ассамблее предлагается принять изложенные выше меры.

- КОНЕЦ -