



РАБОЧИЙ ДОКУМЕНТ

ЧЕТЫРНАДЦАТАЯ АЭРОНАВИГАЦИОННАЯ КОНФЕРЕНЦИЯ

Монреаль, Канада, 26 августа – 6 сентября 2024 года

Пункт 4 повестки дня. Гиперсвязность аэронавигационной системы
4.2. Кибербезопасность и устойчивость информационных систем

ИСПОЛЬЗОВАНИЕ ГИБКИХ МЕТОДОЛОГИЙ ДЛЯ ЗАПОЛНЕНИЯ ПРОБЕЛА В ПОЛИТИКЕ КИБЕРБЕЗОПАСНОСТИ

(Представлено Соединенными Штатами)

КРАТКАЯ СПРАВКА

Являясь сквозной дисциплиной, кибербезопасность оказывает воздействие на всю систему, поскольку она влечет последствия для каждого аспекта системы, включая людей, процессы и технологии. Появляются новые технологии, влияние которых на пропускную способность и эффективность гражданской авиации будет огромным. При этом преимущества этих новых технологий усугубляют проблемы в выстраивании киберзащиты, поскольку злоумышленники также воспользуются этими преимуществами для совершенствования своих средств и методов атак. Учитывая характер кибербезопасности, необходимы инновационные и более гибкие подходы, ускоряющие предоставление инструктивных материалов по кибербезопасности ИКАО государствам – членам ИКАО и заинтересованным сторонам в авиации.

Действие: Конференции предлагается согласиться с рекомендацией, представленной в п. 3.

1. ВВЕДЕНИЕ

1.1 Авиационная экосистема — это уникальная глобальная эксплуатационная система, состоящая из систем, услуг, процессов, технологий и людей, целостно связанных друг с другом, для непрерывных пассажирских и грузовых перевозок с соблюдением требований безопасности полетов и авиационной безопасности. Подборка участников, совокупно формирующих эту экосистему, представлена на **рисунке 1**.

1.2 Кибербезопасность, как и безопасность полетов и физическая безопасность, представляет собой сквозную дисциплину, которая охватывает всю авиационную экосистему для обеспечения ее защиты и сохранения ее способности функционировать. Кибербезопасность также отвечает за срочную защиту авиационных систем и услуг от угроз, являющихся динамичными (например, вредоносные программы), непредсказуемыми (например, события "нулевого дня") и

способными быстро распространяться по всей экосистеме (например, распределенные атаки типа "отказ в обслуживании"). На **рисунке 2** демонстрируется встроенность кибербезопасности во все компоненты авиационной экосистемы. Когда все эти компоненты, в том числе кибербезопасность, интегрированы "бесшовным" образом, обеспечивается безопасность полетов и достигается эффективность.



Рис. 1. Компоненты систем, услуг и технологий, формирующих авиационную экосистему

1.3 Новые и передовые технологии, например, генеративный искусственный интеллект (ИИ), квантовые вычисления и биометрия, интегрируются в авиационную экосистему для повышения ее пропускной способности и эффективности. Угрозы кибербезопасности для авиационных систем и услуг также развиваются и адаптируются, чтобы использовать новые технологии для разработки более изощренных и искусных средств нанесения ущерба критической инфраструктуре и конфиденциальным данным. Злоумышленники также расширяют ландшафт, используя новые технологии для разработки новых способов эксплуатации старых уязвимостей, считавшихся давно устраненными.

1.4 При рассмотрении существующих угроз для авиационной экосистемы и темпов появления новых технологий, которые повышают присущие ей риски, скорость разработки инструктивных материалов и их предоставления государствам – членам ИКАО и заинтересованным сторонам в авиации важна как никогда ранее.

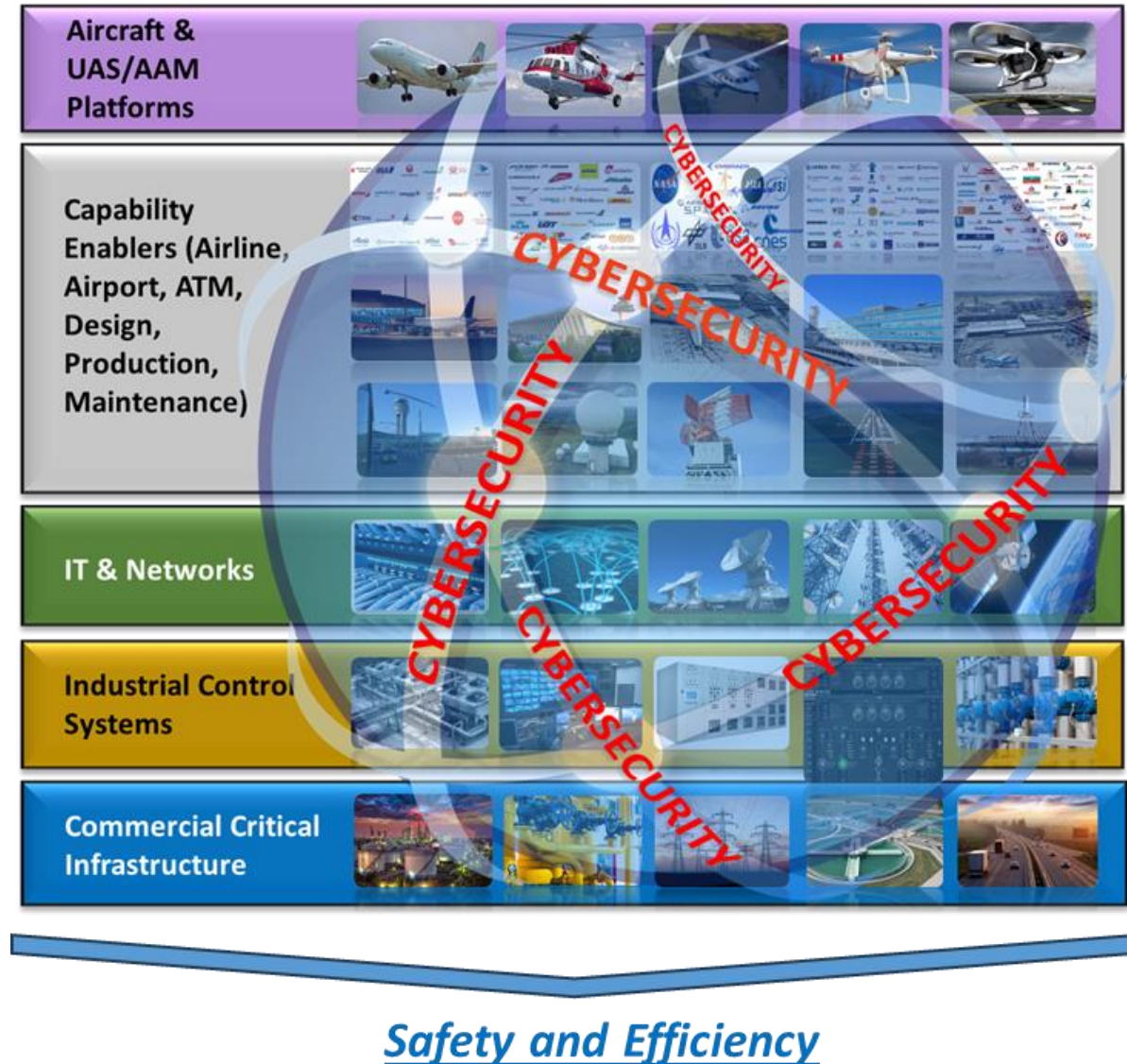


Рис. 2. Средства защиты в сфере кибербезопасности, встроенные в авиационную экосистему

2. РАССМОТРЕНИЕ ВОПРОСА

2.1 Кибербезопасность является фактором, способствующим выполнению основных авиационных функций (например, связи, навигации и наблюдения), и она включает в себя фундаментальный набор инфраструктур, систем и услуг, служащий целостным барьером для защиты от местных, региональных и/или глобальных угроз. Эти угрозы стремительно меняются в своей изощренности, разрушительности и способности причинять вред в любое время и в любой точке экосистемы.

2.2 Новые технологии, например, генеративный ИИ, квантовые вычисления, биометрия и прочие, также создают уникальные возможности для злоумышленников, стремящихся применять более изощренные методы и средства, чтобы нанести вред работе систем и данным гражданской авиации, создавая новые вызовы для заинтересованных сторон в авиации, государств – членов ИКАО и регулирующих органов в области гражданской авиации, принимающих меры противодействия для постоянного совершенствования своей защиты.

2.3 Быстро возникающие угрозы формируют необходимость применения все более инновационных и не терпящих промедления подходов к разработке и предоставлению инструктивных материалов по кибербезопасности заинтересованным сторонам в авиации и государствам – членам ИКАО в целях обеспечения защиты и отказоустойчивости нашей авиационной экосистемы.

2.4 В отдельных инициативах, например, в процессе прямого представления ИКАО, признается необходимость ускорения темпов выпуска материалов, однако сфера применения данного процесса ограничена организациями, тематика которых связана со Стратегическими целями ИКАО по безопасности полетов, аэронавигационному потенциалу и эффективности. Инструктивные материалы, предназначенные для укрепления кибербезопасности авиационной экосистемы, должны разрабатываться и выпускаться с использованием более оперативных и гибких процессов при сохранении контроля качества и конфигурации.

2.5 С учетом вышеизложенных пунктов ИКАО предлагается изучить средства и методы, ускоряющие разработку, пересмотр и распространение инструктивных материалов по кибербезопасности среди заинтересованных сторон в авиации и государств – членов ИКАО в соответствии с потребностями в сфере кибербезопасности.

3. **ВЫВОД**

3.1 Конференции предлагается согласиться со следующей рекомендацией:

Рекомендация 4.2/х. Оценить целесообразность утверждения принципов использования гибких методик

ИКАО предлагается:

- а) признать, что инструктивные материалы по кибербезопасности требуют своевременных, актуальных и действенных подходов к их предоставлению государствам – членам ИКАО и заинтересованным сторонам в авиации;
- б) изучить средства и методы, ускоряющие разработку, пересмотр, выпуск и распространение среди заинтересованных сторон в авиации и государств – членов ИКАО инструктивных материалов по кибербезопасности в соответствии с потребностями в сфере кибербезопасности.