К вопросу о КИБЕРБЕЗОПАСНОСТИ

Киберугрозы

Внешние угрозы:

- вирусы;
- удалённый взлом;
- фишинг;
- DoS/DDoS-атаки;
- хищение и порча устройств;
- другие внешние угрозы.

Внутренние угрозы:

- уязвимости аппаратуры и ПО;
- утечка данных;
- другие внутренние угрозы.

Основные источники угроз на борту воздушного судна:

- недекларированные возможности ПО и устройств КБО и наземных служб;
- уязвимость бортовых сетей и устройств КБО;
- атаки внешних злоумышленников по беспроводным каналам передачи данных.

Особенности Авиационной отрасли

- повышенные требования к обеспечению безопасности и надёжности всех видов техники;
- увеличение функциональной нагрузки и сложности КБО;
- резкий рост сложности контрольно-измерительной инфраструктуры перспективных самолетных систем, включающих распределенные сети интеллектуальных датчиков;
- тесная интеграция бортового и наземного оборудования информационного обеспечения в рамках концепции УВД;
- децентрализация архитектуры систем автоматизированного управления самолетными системами;
- значительная доля импортного радиоэлектронного оборудования со встроенным ПО;
- возможность получения доступа к интерфейсам и системам самолета из внешних каналов связи;
- возможность заражения бортовых систем вредоносным кодом;
- постановка радиопомех на борту ВС и глушение каналов обмена информации.

Проект Дорожной карты ICCAIA

- разработка единого понимания киберугроз и рисков;
- обмен данными по оценке рисков;
- согласование общего языка и терминологии;
- разработка совместных позиций и рекомендаций;
- подготовка единого унифицированного подхода к решению вопросов управления киберугрозами и рисками, доступного общественности;
- продвижение совместного плана работ представителей промышленности и госорганов для создания скоординированной стратегии и планов обеспечения кибербезопасности;
- оказание содействия в развитии культуры киберзащиты у всех участников авиационной деятельности;
- оказание содействия в применении существующих стандартов информационной безопасности, киберзащиты, принципов проектирования;
- создавать механизмы и средства обмена информацией, содержащей сведения об идентификации угроз, статистике атак, способах и средствах защиты;
- сообщать о возможных угрозах и своевременно информировать об обстановке;
- по мере необходимости совершенствовать практические рекомендации, принципы работы и защитные системы.