

ОДИННАДЦАТАЯ АЭРОНАВИГАЦИОННАЯ КОНФЕРЕНЦИЯ

Монреаль, 22 сентября – 3 октября 2003 года

**Пункт 2 повестки дня. Безопасность полетов и авиационная безопасность при
организации воздушного движения (ОрВД)**

Пункт 2.5 повестки дня. Безопасность полетов и безопасность инфраструктуры ОрВД

ЗАЩИТА СВЯЗИ В ЦЕЛЯХ ОрВД

(Представлено Италией)

АННОТАЦИЯ

Воздушный транспорт считается "критической национальной инфраструктурой (CNI)" и поэтому связь в целях ОрВД, включающая мобильные и фиксированные подсети, необходимо считать "критической информационной инфраструктурой (CII)". В настоящем документе представлены некоторые конкретные аспекты систем CNI-CII, касающиеся шифрования, связанности, качества обслуживания и других вопросов.

Италия предлагает использовать стратегические инициативы ЕВРОКОНТРОЛЯ и разработать рекомендации для повышения защиты связи в целях организации воздушного движения.

Действия Конференции изложены в п. 4.

1. ВВЕДЕНИЕ

1.1 В настоящее время развитие и внутренняя организация государств и международных организаций всё больше зависят от сложных и комплексных систем инфраструктуры, например от распределения электроэнергии, транспорта, связи и т. д. Они предполагают тесную взаимосвязь между защитой и уязвимостью данных инфраструктур и эффективностью системы в целом.

1.2 Кроме того, после нападения 11 сентября организациям, которые выполняют основную роль на национальном и международном уровнях, следует пересмотреть свой подход к защите и живучести инфраструктур.

1.3 Данная критическая инфраструктура была определена как критическая национальная инфраструктура (CNI), и ее необходимая "защита" является срочной необходимостью.

1.4 Воздушный транспорт необходимо считать важным компонентом вышеупомянутой CNI и, в рамках организации воздушного движения (ОрВД), соответствующая электросвязь и информационные сети, фиксированные и подвижные, следует рассматривать единой CNI или, более точно, так называемую критическую информационную инфраструктуру (CII).

1.5 Италия предлагает в данной системе использовать стратегические инициативы ЕВРОКОНТРОЛЯ и разработать набор согласованных действий, направленных на повышение степени защиты эксплуатации связи в целях организации воздушного движения.

2. ФИКСИРОВАННАЯ И ПОДВИЖНАЯ СII

2.1 Фиксированная связь

2.1.1 Основными элементами, необходимыми для обеспечения защиты СII, являются:

- a) **Избыточная топология.** СII должна планироваться таким образом, чтобы обеспечивать высокую связанность как между основными узлами (рекомендуется минимальная степень 3), так и между доступом и основными узлами (рекомендуется двойной доступ);
- b) **Средства, обеспечивающие высокое качество передачи.** СII должна обеспечивать точную и своевременную передачу информации при любых условиях, штатных и аварийных. Пользователям необходимо предоставлять требуемую полосу частот и согласованное качество обслуживания (QoS). Поэтому необходимо использовать канал связи с высокой пропускной способностью и программные ("интеллектуальные") узлы связи. В целях выполнения требований избыточности, необходимо использовать различные типы каналов передач, включая радиосвязь высокой пропускной способности (передача на расстояние прямой видимости (LoS), через спутники (SAT) и волоконно-оптические кабели (FOC). Для обеспечения эффективного управления радиочастотами, линии связи должны принадлежать СII и по возможности быть отделенными от общественных линий связи;
- c) **Распределённые "интеллектуальные" ресурсы сети.** СII должна быть в состоянии обеспечивать передачу речевых сообщений и цифровой информации необходимого качества. Она должна динамично оптимизировать распределение ресурсов всей сети, найти наименее перегруженные пути и по возможности использовать избыточность в линиях связи и сетевую топологию. Кроме того, СII должна контролировать потоки сообщений с различным порядком очереди, в зависимости от различных классов услуг, и обеспечивать введение ограничений на соединения с более низким приоритетом в случае аварийной ситуации или снижать полосу частот. Технология асинхронного режима передачи, которая включает почти все данные характеристики, считается наилучшим решением для основной инфраструктуры передачи и плана контроля эксплуатации сети;

- d) **Защитные меры.** Помимо защиты от "физического" проникновения, СИ содержит критическую информацию СНИ, которая должна быть защищена от несанкционированного ознакомления или изменения. Этот вопрос должен решаться при помощи шифрования и системы защиты доступа. Системы защиты доступа должны быть установлены на границах местных доменов и иметь соответствующую конфигурацию. Это особенно важно в случае дистанционного доступа к станциям управления, и они могут включать надежные механизмы идентификации, специально быть настроенными на различные уровни доступа (согласно военному принципу *служебной необходимости*). Кроме того, настоятельно рекомендуется, чтобы поток критических сообщений (таких, как пароль для опознавания или ключи и управление системой информации) передавался по сети в зашифрованном виде, чтобы исключить внешнее обнаружение внутренней топологии СНИ и критического расположения ресурсов путем анализа потока сообщений; и
- e) **Эффективная совместимость и возможности интеграции.** СИ должна быть максимально совместимой со стандартами внутренней связи и интегрироваться с установленными подвижными и фиксированными системами.

2.2 Подвижные средства связи

2.2.1 Основными элементами, необходимыми для защиты компонента связи "воздух – земля" СИ, являются:

- a) **Предотвращение несанкционированного прослушивания.** Средства связи "воздух – земля" могут легко прослушиваться при помощи бытовых приемников, которые продаются для населения. Данную проблему следует решать путем шифрования и опознавания источника информации или другими удобными способами;
- b) **Способность к работе в условиях радиопомех (глушения).** Средства связи "воздух – земля" можно легко глушить при помощи бытовых передатчиков. Данную проблему следует решать путем переключения частот или расширения спектра передач или другими удобными способами;
- c) **Способность к работе в условиях радиопомех (намеренное искажение информации).** Средства связи "воздух – земля" можно легко дезориентировать (или преднамеренно исказить информацию) при помощи бытовых передатчиков. Данную проблему следует решать путем передачи сообщения об аутентификации; изменение частот или расширение спектра также являются эффективными средствами;
- d) **Сохранность данных.** Наличие дополнительной линии связи "воздух – земля" (например, спутниковая линия связи) позволит обеспечить высокую степень сохранности критической и закрытой информации подвижной СИ; и
- e) **Физическое разделение.** В целях обеспечения эффективной эксплуатации связи для ОрВД, средства связи "воздух – земля" необходимо по возможности отделить от других средств связи "воздух – земля", таких, как: Интернет, e-mail, общественная связь, кабельное телевидение и средства связи компании

(бортовая система связи адресации и передачи данных (ACARS) и авиационный оперативный контроль (АОС)).

3. ПРЕДЛОЖЕННАЯ СТРАТЕГИЧЕСКАЯ ИНИЦИАТИВА

3.1 Предлагается разработать и утвердить, даже с учетом аспектов затрат/выгод, рекомендации по защите связи, которые определяют минимальные требования к аспектам защиты фиксированной и подвижной связи в целях ОрВД, таким, как: наземная и бортовая архитектура, избыточность, связанность, защита информации, совместимость, сохранение данных и проблемы радиопомех.

4. ДЕЙСТВИЯ КОНФЕРЕНЦИИ

4.1 Конференции предлагается:

- а) подтвердить, что фиксированные и подвижные сети связи в целях ОрВД являются "критическими информационными инфраструктурами", и в этой связи рассмотреть соответствующие вопросы защиты; и
- б) просить ИКАО разработать и утвердить рекомендации для защиты фиксированной и подвижной связи CNI-CII в целях ОрВД, с учетом аспектов затрат/выгод.

– КОНЕЦ –