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**

МЕТОДИКА ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ ЗАЩИТЫ В ОПЕРАТИВНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ УПРАВЛЕНИЯ АЭРОНАВИГАЦИИ ФРАНЦИИ

(Представлено Францией)

АННОТАЦИЯ

В настоящее время компьютерные системы широко используются при обеспечении аэронавигации и их надежность и защищенность имеют жизненно важное значение для выполнения функций, осуществляемых аэронавигационными службами.

Целью настоящего рабочего документа является представление методики решения проблемы обеспечения безопасности оперативной информационной системы Управления аэронавигации Франции.

Действия Конференции приведены в п. 5.

1. ИСХОДНАЯ ИНФОРМАЦИЯ: ПРОБЛЕМА ЗАЩИЩЕННОСТИ И НАДЕЖНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ АЭРОНАВИГАЦИИ ФРАНЦИИ

1.1 Поддержание надежности информационной системы может быть определено как обеспечение ее сохранности, целостности и конфиденциальности. Безопасность, которая может рассматриваться как подэлемент защиты информационной системы, подразумевает, в частности, защиту надежности информационной системы от злонамеренных действий.

В настоящее время компьютерные системы широко применяются при обеспечении аэронавигации и поэтому надежность и безопасность информационной системы имеют жизненно важное значение в работе аэронавигационных служб.

Еще несколько лет назад аэронавигационная информационная система была закрытой и практически никак не взаимодействовала с внешним миром. Она имела низкую уязвимость перед угрозой взлома просто лишь в силу того обстоятельства, что трудно было получить электронный доступ к информационной системе откуда-либо извне. В таких условиях **безопасность** могла быть обеспечена всего лишь с помощью защиты физического доступа к информационной системе.

1.2 В последние годы, однако, мы видим, что наряду с ростом значения информационной системы для аэронавигации сама система постепенно становится более сложной и все шире начинает взаимодействовать с другими системами и сетями, находящимися вне контроля со стороны аэронавигационной службы. Это взаимодействие необходимо в силу потребности во взаимных контактах и обмене данными с партнерами аэронавигационных служб (европейские партнеры, авиакомпании и т. д.). Вместе с тем "частные" технологии постепенно уступают место стандартным технологиям, таким, как IP (протокол Интернета) для функций сетевого уровня или UNIX для операционных систем.

Все эти факторы делают информационную систему более уязвимой и повышают ее подверженность угрозам извне. В результате значительно возрастает риск нарушения безопасности информационной системы вследствие действий злоумышленников.

1.3 Таким образом, для Управления аэронавигации Франции стало очевидно, что ему следует уделять больше внимания проблеме поддержания надежности и безопасности своей информационной системы, а точнее ее защиты от внешних угроз.

2. РЕШЕНИЕ ПРОБЛЕМЫ

2.1 Для того чтобы уменьшить риск вскрытия информационной системы до приемлемого уровня, необходимо определить технические, организационные и процедурные меры, способные устранить уязвимость информационной системы. Такие меры должны быть разработаны на основе правил, которые:

- обеспечивают рассмотрение проблемы исчерпывающим образом;
- устанавливают единообразные меры защиты;
- определяют такие меры защиты, которые являются выполнимыми, признаются и фактически выполняются.

2.1.1 Исчерпывающее рассмотрение проблемы означает, что в поле зрения должны находиться все аспекты, которые могут влиять на безопасность, включая: взаимодействие компьютерной системы с внешним миром, ее внутренние межсоединения (между сайтами), использование, эксплуатация и обслуживание компьютерного оборудования, технические и функциональные изменения, организация и ответственность людских ресурсов, а также анализ инцидентов и происшествий, связанных с безопасностью.

Исчерпывающее рассмотрение также означает, что необходимо принимать во внимание все элементы информационной системы, которые должны соответствовать "требованию безопасности", или в отношении которых нарушение безопасности может повлиять на выполнение аэронавигационных задач.

2.1.2 Меры защиты должны быть одинаковыми для всех компонентов компьютерной системы. Защита информационной системы настолько эффективна, насколько хорошо защищено ее самое слабое

звено. Бесполезно применять крайне сложные и дорогостоящие меры защиты в отношении одной части системы, если другая, в такой же степени уязвимая ее часть, не будет адекватно защищена.

2.1.3 Меры защиты должны быть выполнимыми, в них должны учитываться ограничения и специфика контекста. При составлении правил безопасности следует принимать во внимание используемую технологию, оперативные ограничения для безопасности, привычки и практику пользователей и операторов и т. д. Наконец, для того чтобы эти правила выполнялись на деле, чрезвычайно важно, чтобы они признавались операторами и пользователями компьютерной системы, которые должны быть ознакомлены с ними, и чтобы они выполнялись аналогично тому, как выполняются уже существующие правила функционирования и использования системы.

2.2 Принимая во внимание все эти факторы, Франция приступила к разработке официальной общей политики в области компьютерной безопасности. Проект, сокращенно именуемый PSINA *(Политика в области безопасности информатики Управления аэронавигации)*, имеет целью определить общие правила компьютерной безопасности для всех "действующих" аэронавигационных систем, входящих в Информационную систему управления воздушным движением (SICTA).

Эта общая политика безопасности должна быть отражена в документе, который будет состоять из следующих разделов:

– Задачи и охват PSINA: используемое определение информационной системы, принятые принципы, рассматриваемые угрозы и место PSINA по отношению к другим существующим правилам.

– Классификация компонентов информационной системы: будут определены четыре уровня уязвимости для функциональных и физических компонентов информационной системы вместе с критериями классификации компонентов на различных уровнях. Классификация будет проводиться по трем направлениям: готовность, целостность и конфиденциальность.

– Доступ пользователей к информационной системе: правила, касающиеся предоставления разрешений, аккредитации, аутентификации, прослеживаемости действий, а также правила для внешнего персонала, привлекаемого к работе в Генеральном директорате гражданской авиации.

– Физическая защита: правила защиты чувствительных информационных средств (съемные или портативные средства и т. д.), защита и физическое размещение компьютерных систем.

– Обслуживание и административное управление информационной системой: правила, касающиеся предоставления разрешений, аутентификации персонала обслуживания, использования внешних технических специалистов по обслуживанию и прослеживаемости операций по техническому обслуживанию и административному управлению системой.

– Межсоединения и обмен данными внутри информационной системы: принятие "гарантирующих" положений, определяющих единообразные параметры и правила безопасности, касающиеся использования частных и открытых компьютерных сетей для внутреннего подсоединения.

– Межсоединения и обмен данными с внешними организациями: правила доступа к информационной системе извне и доступа от информационной системы к внешним системам; правила использования частных или открытых сетей для внешнего подсоединения; правила предоставления и получения компьютерных данных при взаимодействии информационной системы с внешними организациями.

– Эволюция информационной системы: повторная оценка классификации компонентов и уровней защиты в случае модификации информационной системы; правила, касающиеся интеграции новых или изъятия старых компонентов.

– Инциденты и происшествия, связанные с безопасностью: определение инцидента или происшествия, связанного с безопасностью; классификация и обнаружение инцидентов; предпринимаемые действия в случае обнаружения инцидента, связанного с безопасностью; правила, касающиеся внутренней и внешней связи в случае инцидентов и происшествий, связанных с безопасностью; определение принципов, касающихся наказаний и разбирательств в отношении злоумышленников внутри и вне Генерального директората гражданской авиации.

– Мобилизация людских ресурсов на обеспечение безопасности информационной системы: повышение осведомленности пользователей и лиц, принимающих решения, относительно вопросов надежности/безопасности; назначение "ответственных" за безопасность, правила обслуживания и административного управления, связанные с обеспечением безопасности, и т. д.

2.3 Для обеспечения применимости правил, разрабатываемых в рамках описываемой политики безопасности, и незамедлительного ознакомления с ними всех работающих с информационной системой, была сформирована рабочая группа, которой было поручено подготовить предложение относительно указанной политики. Рабочая группа состоит из представителей различных оперативных подразделений аэронавигационных служб. Кроме того, для обеспечения фактического признания политики различными операторами и пользователями PSINA будет принята Руководящим комитетом Управления аэронавигации и тем самым будет иметь официальный характер.

2.4 Ниже приведены несколько примеров правил обеспечения безопасности, разрабатываемых в рамках PSINA.

– Любое подключение к внешним системам должно быть официально санкционировано сотрудником безопасности на основе досье безопасности, в котором должны быть конкретно указаны результаты ранее проведенной оценки риска.

– Любое соединение с внешними системами должно быть проверено с помощью технических средств. В данном случае цель заключается в обеспечении того, чтобы в любое время доступ был возможен только к тем службам, которые имеют разрешение на такое межсоединение, и чтобы только санкционированные корреспонденты (пользователи или системы) могли им пользоваться и т. д. Кроме того, проверка также должна быть в состоянии показать, что при межсоединении использовались только те технические функции (например, сетевые протоколы), которые строго необходимы для работы санкционированных служб.

– Применительно к самым чувствительным элементам информационной системы запрещается устанавливать любое межсоединение с использованием открытых сетей (RTC, Интернет и т. д.).

3. СТРАТЕГИЯ ВНЕДРЕНИЯ ПРИНЯТОГО МЕТОДА

3.1 Учитывая масштаб проекта PSINA и необходимость со временем охватить все его аспекты, в рамках поставленных задач были определены приоритеты.

В качестве первоочередной задачи было решено обеспечить безопасность периметра аэронавигационной информационной системы, с тем чтобы легче решать проблемы, связанные с внешними рисками. Для этого будут определены функции и правила безопасности, которые должны выполняться на "границах" информационной системы.

После того как будет обеспечена безопасность периметра, можно будет рассмотреть вопрос обеспечения внутренней безопасности. Меры противодействия внутренним рискам намного труднее определить и средств для этого требуется намного больше, так как всю систему "заблокировать" невозможно; информационная система должна всегда оставаться в рабочем состоянии и сохранять свою эффективность, в силу чего невозможно использовать те радикальные и относительно простые меры защиты, которые используются против внешних рисков. По этой причине, среди прочего, было решено обратиться к этому аспекту после того, как будут решены вопросы, связанные с внешней угрозой.

3.2 В рамках такой последовательности действий конечной целью является органичное обеспечение безопасности информационной системы, при котором меры обеспечения безопасности периметра будут включать использование контролирующей технологии, которая будет держать под наблюдением сети и сетевые межсоединения, а механизм внутренней защиты будет опираться на технологию безопасности, контролирующую внутреннюю сеть и все ее системы.

4. ЗАКЛЮЧЕНИЕ

4.1 В настоящее время Франция продолжает работу над первым проектом политики обеспечения компьютерной безопасности. Предложение, включающее текст первых основных разделов этой политики (цели и сфера действия политики, правила классификации компонентов информационной системы), уже подготовлено рабочей группой, которая в настоящее время ведет разработку правил взаимодействия с внешними организациями. Это первое предложение вскоре будет представлено Руководящему комитету.

4.2 После того как эти первые разделы будут дополнены разделом по организации людских ресурсов и компьютерной безопасности, можно будет говорить об официальном внедрении начального варианта политики обеспечения компьютерной безопасности в Управлении аэронавигации Франции.

4.3 Для выполнения этой долговременной задачи требуются неослабные усилия, с тем чтобы всеобъемлющая политика обеспечения безопасности была на уровне стоящих задач.

5. ДЕЙСТВИЯ КОНФЕРЕНЦИИ

5.1 Конференции предлагается:

a) принять во внимание риски, представляющие собой угрозу для аэронавигационных компьютерных систем;

b) разработать Стандарты и Рекомендуемую практику (SARPS) для обеспечения безопасности компьютерных систем; и

c) поставить перед соответствующей группой экспертов задачу разработать общее руководство для оказания помощи государствам в деле внедрения их политики обеспечения информационной безопасности, например, в виде контрольного перечня, включающего элементы и вопросы, которые должны содержаться в политике обеспечения безопасности, а также средства обеспечения безопасности информационных систем.

– КОНЕЦ –