УДК 004.950.430
© В. Черныш[1], 2014

МЕТОД ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ОРГАНИЗАЦИИ ВОЗДУШНОГО ДВИЖЕНИЯ

У статті розглядається проблематика оцінки ризиків інформаційної безпеки в системі організації повітряного руху. Проводиться аналіз стану захищеності інформаційних ресурсів провайдера аеронавігаційного обслуговування та визначається роль інформаційної безпеки в системі управління безпекою польотів.

The article deals with the problems of assessing information security risks in the system of air traffic management. The analysis of the state of security of information resources provider of air navigation services and defines the role of information security in the management of safety.

1. ВВЕДЕНИЕ И ПОСТАНОВКА ЗАДАЧИ

За последнее время авиация достигла значительного развития. Этот прогресс был бы невозможен без достижений в области радиотехники, метеорологии, производства, информационных систем и технологий.

Управление различными технологическими процессами в авиации базируется на использовании информационно-телекоммуникационных систем (ИТС), к которым относятся источники информации, средства ее передачи, обработки, отображения, хранения, общесистемное и специальное программное обеспечение. Во всех информационных технологических процессах, а также процессах управления, важную роль играет человеческий фактор [1].

Обеспечение безопасности информационных технологий (ИТ) представляет собой комплексную проблему, которая включает: правовое регулирование применения ИТ; совершенствование технологий разработки ИТ и защиты информации в информационно-телекоммуникационных системах (ИТС); развитие системы сертификации; обеспечение соответствующих организационно-технических условий эксплуатации информационных систем и ИТ.

В авиации проблема защиты информации (ЗИ) является составной частью авиационной безопасности.

[1]Харьковский национальный университет радиоэлектроники

Концепция безопасности полетов в гражданской авиации может иметь различную интерпретацию, а именно:

1) стремление к достижению нулевого уровня авиационных происшествий;

2) приемлемый уровень риска;

3) процесс выявления источников опасности, контроль факторов риска и реализация мероприятий по их предупреждению;

4) недопущение потерь вследствие авиационных происшествий (человеческих потерь, ущерба имуществу и окружающей среде).

Хотя недопущение авиационных происшествий является желаемым результатом деятельности отрасли и предприятия, абсолютный уровень безопасности является в некоторой степени недостижимой целью. Несмотря на все усилия по предотвращению сбоев и ошибок, они все же могут иметь место с некоторой (пусть очень малой) вероятностью.

2. РОЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ПОЛЕТОВ

Информационная безопасность, как составная часть общей системы обеспечения безопасности полетов, в последнее время все активнее привлекает к себе внимание из-за постоянно возникающих проблем, обусловленных внедрением информационных технологий (ИТ) во все сферы авиационной индустрии.

Безопасность полетов – состояние, при котором риски, связанные с авиационной деятельностью, относящейся к эксплуатации воздушных судов или непосредственно обеспечивающей такую эксплуатацию, снижены до приемлемого уровня и контролируются.

Концепция информационной безопасности уполномоченного государственного органа по аэронавигационному обслуживанию (провайдер АНО) должна представлять организованную совокупность средств, методов и мероприятий, обеспечивающих надежную защиту информации от несанкционированного доступа (НСД).

Кроме того, Концепция информационной безопасности провайдера АНО определяет основные принципы и раскрывает основные направления обеспечения безопасности информации, а также содержит систематизированное изложение целей, задач, базовых правил защиты информации и способов достижения надлежащего уровня безопасности информации в ИТС ОрВД.

Важнейшими условиями обеспечения информационной безопасности провайдера АНО являются законность, соблюдение

баланса интересов личности, общества и государства, компетентность сотрудников, отвечающих за вопросы обеспечения информационной безопасности. Без соблюдения данных условий не может быть обеспечен требуемый уровень защиты от потенциальных и существующих угроз.

Таким образом, в основу концепции информационной безопасности провайдера АНО должны быть положены все возможные методы и средства, направленные на эффективное обеспечение безопасности информации, как составной части системы управления безопасности полетов.

Система обеспечения ИБ провайдера АНО, включает в себя создание политики ИБ, внедрение комплексной системы защиты информации (КСЗИ) и предполагает решение следующих задач [2]:

1) определение основных взглядов на обеспечение безопасности информации провайдера АНО в условиях широкого использования ИТС ОрВД в хозяйственной деятельности;

2) формирование единой корпоративной политики в области обеспечения безопасности информации;

3) выработка подходов к обеспечению безопасности информации в условиях как умышленных так и непреднамеренных воздействий нарушителя;

4) оценка рисков информационной безопасности и реализацию комплекса адекватных, экономически обоснованных мер по снижению рисков и предотвращению угроз безопасности информации, устранению уязвимостей ИТС ОрВД и ликвидации последствий воздействий угроз на информационное пространство объектов гражданской авиации;

5) координация деятельности органов управления и подразделений защиты информации (например, отдела информационной безопасности, отдела технической защиты объектов и информации);

6) обоснование экономической целесообразности обеспечения безопасности информации;

7) внедрение эффективных методов и моделей управления рисками ИБ;

8) создание системы подготовки и переподготовки кадров в области обеспечения безопасности информации;

9) разработка механизмов страхования рисков ИБ.

На рис.1 представлена концепция информационной безопасности провайдера АНО.

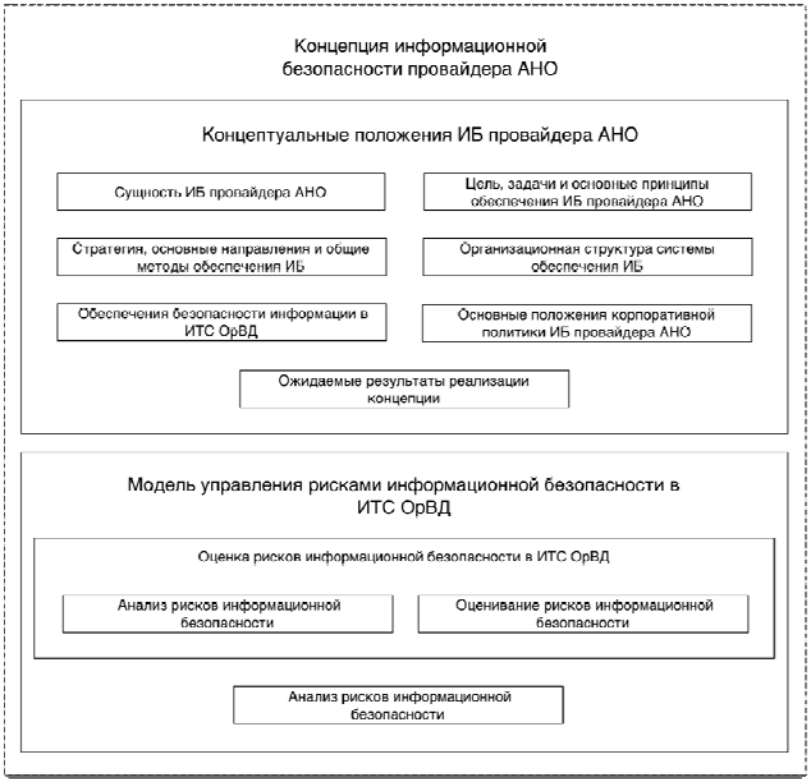

Рис. 1. Суть Концепции информационной безопасности провайдера АНО

Для реализации концепции ИБ провайдера АНО необходимо также использовать рекомендации международных стандартов и регламентирующих требований по безопасности полетов [3-4], реализация которых позволит более эффективно организовать защиту информационных ресурсов провайдера АНО.

3. АНАЛИЗ СОСТОЯНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ПРОВАЙДЕРА АЭРОНАВИГАЦИОННОГО ОБСЛУЖИВАНИЯ

Развитие ИТ и процессов автоматизации обслуживания воздушного движения и полетно-информационного обслуживания сопровождается проблемами, связанными с ростом уязвимостей информационных систем и технологий, увеличением рисков нарушения конфиденциальности, целостности и доступности информации [5-6].

Большинство информационных процессов в системе ОрВД являются критическими. Серьезной проблемой безопасности ИТС ОрВД является несанкционированный доступ субъектов к процессам обслуживания воздушного движения и полетно-информационного обслуживания.

Возможность незаконного вмешательства посторонних лиц в процессы обслуживания воздушного движения и полетно-информационного обслуживания приводит к тому, что проблема безопасности услуг ОрВД должна рассматриваться в двух плоскостях [5]:

1) обеспечение безопасности функционирования ИТС ОрВД в нормальных условиях эксплуатации;

2) защита ИТС ОрВД в условиях возрастающей агрессивности среды эксплуатации.

Безопасность системы ОрВД достигается за счет обеспечения безопасности всех ресурсов, которые используются при предоставлении услуг обслуживания воздушного движения. Поэтому перечень задач защиты систем ОрВД и обеспечения безопасности полетов необходимо дополнить задачами обеспечения информационной безопасности в процессе обслуживания воздушного движения.

Основными задачами обеспечения безопасности информации являются [6]:

1) создание безопасного информационного пространства для осуществления провайдером АНО своей деятельности как самостоятельно, так и в сотрудничестве с органами государственной власти, ведомствами, организациями, учреждениями и другими субъектами транспортной отрасли;

2) соблюдение интересов провайдера АНО в информационной сфере, региональных структурных подразделений, дочерних компаний и служб, входящих в состав провайдера АНО, сотрудничающих с

провайдером АНО по вопросам обеспечения безопасности информации;

3) формирование корпоративной культуры ИБ, индивидуальных и групповых навыков и умений безопасного поведения с информационными ресурсами и ресурсами ИТС ОрВД;

4) обеспечение, с необходимым уровнем гарантий конфиденциальности, целостности, доступности информации и услугой наблюдаемости ИТС ОрВД с целью поддержки всех сфер деятельности провайдера АНО, устойчивого функционирования и развития провайдера АНО;

5) управление рисками информационной безопасности;

6) поддержание постоянной готовности к проведению эффективных мер по выявлению инцидентов и противодействию нарушениям безопасности информации и восстановлению безопасного состояния функционирования провайдера АНО, как объекта гражданской авиации;

7) поддержка непрерывной надежной работы ИТС ОрВД и ее компонентов.

Обеспечение безопасности информации в ИТС ОрВД предлагается осуществлять в рамках комплексной системы защиты информации, которая представляет собой совокупность организационных и инженерных мер обеспечения безопасности информации, технических, криптографических программно-аппаратных комплексов и средств защиты информации.

Под безопасностью информации в ИТС ОрВД понимают состояние защищенности информации, обрабатываемой в ИТС провайдера АНО, в котором обеспечивается выполнение свойств информации как конфиденциальность, целостность, доступность.

4. КОНЦЕПТУАЛИЗАЦИЯ СИСТЕМЫ ОРГАНИЗАЦИИ ВОЗДУШНОГО ДВИЖЕНИЯ

Система организация воздушного движения (ОрВД) представляет собой сложную систему, включающую информационно-телекоммуникационную систему организации воздушного движения (ИТС ОрВД) и субъектов системы ОрВД (персонал). На рис. 2 представлены компоненты системы ОрВД.

Рис. 2. Компоненты системы ОрВД

Для построения модели управления рисками ИБ системы ОрВД необходимо концептуализировать основные компоненты системы. Создание концепции, определяющей стратегические направления обеспечения безопасности информации в ИТС ОрВД, представляется важным для предотвращения возможности проявления дестабилизирующих факторов.

Для построения модели управления рисками ИБ системы ОрВД и оценки рисков в ИТС ОрВД необходимо рассмотреть основные компоненты системы ОрВД.

Информационные активы провайдера АНО являются объектом для многих видов угроз. Угроза может стать причиной нежелательного инцидента, в результате которого провайдеру будет причинен ущерб. Этот ущерб может возникнуть в результате атаки на программные и аппаратные ресурсы ИТС ОрВД, что приведет к несанкционированному раскрытию, модификации, повреждению, уничтожению информации в ИТС ОрВД. Угрозы ИБ могут быть осуществлены посредством использования уязвимостей системы.

Уязвимости представляют собой слабости защиты, ассоциированные с информационными активами провайдера АНО. Эти слабости могут использоваться одной или несколькими угрозами, являющимися причиной нежелательных инцидентов, которые могут стать причиной нестабильного функционирования компонентов ИТС ОрВД. Уязвимости – это любые факторы, делающие возможной успешную реализацию угроз. Можно с уверенностью констатировать, что уязвимости являются основной причиной возникновения атак. Наличие же слабых мест в ИТС ОрВД может быть обусловлено самыми различными факторами, начиная с простой халатности сотрудников и заканчивая преднамеренными действиями злоумышленников.

Управление рисками ИБ в системе ОрВД как научная и управленческая деятельность представляет собой совокупность последовательных этапов научно-практических исследований, направленных на определение достоверных и обоснованных характеристик риска, а также на выявление эффективных мер по его сокращению [7-8].

5. ВЫВОДЫ

Риск информационной безопасности ИБ информационно-телекоммуникационной системы представляет собой интегральную оценку того, насколько эффективно существующие средства защиты способны противостоять информационным атакам. Процесс анализа рисков включает три основных этапа: этап сбора исходной информации об ИТС, этап оценки рисков на основе собранных данных и этап разработки рекомендаций по управлению выявленными рисками информационной безопасности ИТС.

Предложенный в статье метод оценки рисков информационной безопасности ИТС ОрВД может быть внедрен в концепцию информационной безопасности аэронавигационного провайдера как унифицированный.

Направление дальнейших исследований связано с разработкой модели управления рисками информационной безопасности в системе организации воздушного движения.

1. Замула, О.А. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О.А. Замула, В.І. Черниш // Системи обробки інформації: збірних наукових праць ХУПС. – Вип.2(92). – Харків: ХУ ПС, 2011. – С.53-56. 2. Черныш, В.И. Методы оценивания информационных рисков

компании / В.И.Черныш // Материалы XV Международного юбилейного молодёжного форума «Радиоэлектроника и молодежь в XXI веке»: Сб. тезисов, 18–20 апреля 2011 р., Т.5. - Харьков: ХНУРЭ. 2011. – С. 195. 3. ISO 27005 ISO/IEC 27005:2010. Information technology. Security techniques. Information security risk management – ISO / IEC, 2010. – 70 с. 4. Сердюк В.А. Анализ современных тенденций построения моделей информационных атак / В.А. Сердюк // Информационные технологии. – 2004. – No 5. – С. 94 – 101. 5. Замула А.А. Концептуализация информационных процессов в системе организации воздушного движения / А.А. Замула, В.И. Черныш, Ю.В. Землянко // Вісник Національного університету «Львівська політехніка»: «Автоматика, вимірювання та керування». – Львів, Львівська політехніка, 2013. - №774. - С.21-27. 6. Сердюк В.А. Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий Москва, Высшая Школа Экономики (Государственный Университет), 2011г. - 576с. 7. Замула А.А. Автоматизация процессов обслуживания воздушного движения / А.А. Замула, А.В. Северинов, В.И. Черныш // Наука і техніка Повітряних Сил Збройних Сил України. Науково-технічний журнал. Вип 2(6) – Харків: ХУ ПС, 2013. – С. 161-165. 8. Замула А.А. Эффективность информационных процессов и технологий при обслуживании воздушного движения / А.А. Замула, В.И. Черныш, Ю.В. Землянко // Збірник наукових праць Харківського університету Повітряних Сил. – Харків, ХУПС, 2013. – № 2(35). –С.89 – 93.