УДК 004.950.430

А. А. Замула[1], В. И. Черныш[1], Ю. В. Землянко[2]
[1]Харьковский национальный университет радиоэлектроники,
[2]Харьковский государственный университет питания и торговли

КОНЦЕПТУАЛИЗАЦИЯ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ И ТЕХНОЛОГИЙ В МЕТОДЕ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Запропоновано метод оцінювання ризиків інформаційної безпеки з використанням методу Байєса. Концептуалізуються параметри оцінювання системи організації повітряного руху.

Ключові слова: інформаційна безпека, ризик, обслуговування повітряного руху.

The paper discusses a method of information security risk assessment using Bayes' method. Assessment parameters for the air traffic management system are conceptualized.

Key words: information security, risk, air traffic management.

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 информационных систем (ИС), 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].

Существование и функционирование воздушного транспорта связано с эффективностью использования аэронавигационной системы (АНС) и системы организации воздушного движения (ОрВД). Однако сегодня в литературе недостаточно четко определены положения, которые бы позволили разграничить понятия об этих системах. В большинстве случаев для определения терминов ОрВД и АНС используют одинаковые интерпретации [1].

Для разработки метода оценки рисков информационной безопасности на первом этапе необходимо иметь концептуализированное представление о системе организации воздушного движения . На втором этапе необходимо систематизировать элементы и определения для этой системы.

Основные понятия и определения

Информационная технология (ИТ) [2] – процесс, использующий совокупность средств и методов сбора, обработки и передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса или явления (информационного продукта).

Информационные ресурсы – совокупность данных, представляющих ценность для организации (предприятия) и выступающих в качестве материальных ресурсов. К ним относятся файлы данных, документы, тексты, графики, знания, аудио- и видеоинформация. Процесс обработки данных в ИС невозможен без использования технических средств и программного обеспечения [4–5].

Аэронавигационная система (АНС) – это система, которая представляет собой совокупность организаций, персонала, инфраструктуры, технических средств, правил и информации. Целью создания и функционирования АНС является обеспечение безопасности, регулярности и

эффективности воздушной навигации.

Концептуализация системы организации воздушного движения

Поскольку система организация воздушного движения является достаточно сложной, то необходимо ее структурировать. Выделим четыре составляющих системы ОрВД (рис. 1):

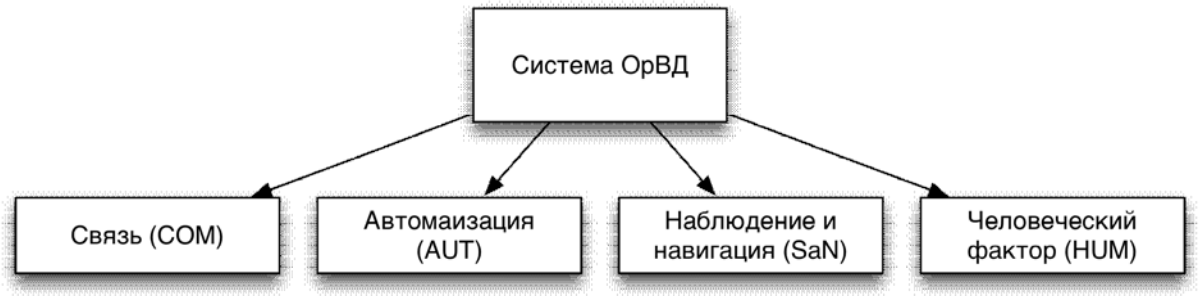

Рис. 1. Иерархия системы организации воздушного движения

Связь (Com) в системе ОрВД состоит из воздушной и наземной составляющих.

Авиационная электросвязь предназначена для [6]:

1) обмена сообщениями между органами обслуживания воздушного движения (ОВД) и воздушного судна (ВС) на протяжении всего полета;

2) обмена сообщениями между экипажами ВС в воздухе;

3) взаимодействия органов ОВД во время планирования использования воздушного пространства Украины и обслуживания воздушного движения;

4) взаимодействия между службами предприятий, организаций и учреждений гражданской авиации во время передачи (приема) административной и производственной информации;

5) автоматизированного обмена данными с экипажами ВС и наземными пользователями, которые обеспечивают полеты;

6) передачи (приема) сообщений, которые содержат оперативную метеорологическую информацию;

7) приема сигналов радиомаяков с места бедствия;

8) взаимодействия с подразделениями соответствующих органов Минобороны, МЧС, МВД и других центральных органов исполнительной власти.

Авиационная наземная электросвязь является основным средством обеспечения взаимодействия органов ОВД. Она организовывается согласно принятой структуре ОВД Украины.

Для организации авиационной наземной электросвязи применяются средства проводной электросвязи, радиосвязи, радиорелейной и тропосферной связи, спутниковой электросвязи и другие средства [6].

Авиационная наземная электросвязь делится на такие виды:

1) авиационная телефонная электросвязь;

2) авиационная телеграфная электросвязь;

3) авиационная электросвязь автоматизированного обмена данными.

Авиационная воздушная электросвязь является основным средством связи органов ОВД с экипажами ВС (двусторонняя электросвязь “воздух – земля”) и между экипажами ВС, которые находятся в полете, а также средством получения сигналов радиомаяков с места бедствия.

Авиационная воздушная электросвязь в гражданской авиации Украины организовывается с использованием радиотелефонных (речевых) каналов связи и с использованием аппаратуры передачи данных для автоматизированного обмена данными. Она делится на следующие виды (группы сетей):

1) авиационная воздушная электросвязь для районного диспетчерского обслуживания воздушного движения;

2) авиационная воздушная электросвязь для диспетчерского обслуживания подхода;

3) авиационная воздушная электросвязь для аэродромного диспетчерского обслуживания воздушного движения;

4) авиационная воздушная электросвязь для полетно-информационного обслуживания;

5) авиационная воздушная электросвязь для аварийно-спасательных и поисково-спасательных работ;

6) авиационная воздушная электросвязь для производственно-коммерческой деятельности.

Автоматизация – это высший этап в развитии техники, для которого характерным является осуществление производственных, управленческих и других процессов без непосредственного участия в них человека. При автоматизации процессы сбора (получения), преобразования (обработки) и использование информации выполняются автоматически. Процесс управления предусматривает наличие объекта управления (объекта, которым управляют) и управляющего объекта (объекта, который осуществляет управление). Основными средствами автоматизации ОВД есть автоматизированные системы управления воздушным движением (АС УВД).

Следующим параметром оценивания системы ОрВД является навигация и наблюдение.

Навигация при ОВД – это совокупность методов и средств для определения действительных и желаемых положения и движения летательного аппарата, рассматриваемого как материальная точка. К основным навигационным системам относят:

1. Ненаправленные радиомаяки NDB (Non-Directional Beacon) – служат для создания ненаправленного в горизонтальной плоскости излучения радиоволн. За счет ненаправленного приема этих радиоволн автоматическими радиокомпасами на ВС определяется курсовой угол радиостанции.

2. Всенаправленный азимутальный радиомаяк ОВЧ (VOR) – служит для измерения на ВС азимута ВС относительно меридиана места установки радиомаяка.

3. Всенаправленный дальномерный радиомаяк диапазона ультравысоких частот (DME) – служит для измерения на ВС наклонной дальности (Д) относительно места установки маяка DME.

4. Радиомаячная система обеспечения процедур точного захода на посадку (ILS) – служит для определения на самолете его положения относительно заданной радиомаяками траектории посадки и определения моментов его пролета над маркированными точками на предпосадочной прямои.

В качестве систем наблюдения используются системы, основанные на передаче сообщений, получении координатной информации с помощью первичных обзорных радиолокаторов и получении координатной и полетной информации с помощью вторичных обзорных радиолокаторов (ВОРЛ), систем зависимого наблюдения (ADS-B) и многопозиционных систем наблюдения (MLAT).

Используемые при обслуживании воздушного движения системы наблюдения ОВД обладают очень высокой степенью надежности, готовности и целостности. Вероятность отказов системы или существенного ухудшения ее характеристик, которые могут явиться причиной полного или частичного нарушения обслуживания, является незначительной.

Человеческий фактор – это термин, описывающий возможность принятия человеком ошибочных или алогичных решений в конкретных ситуациях [7].

Отсутствие единого понимания сущности понятия человеческого фактора затрудняет разработку и внедрение механизмов, целью которых является повышение безопасности полетов. Человеческий фактор необходимо рассматривать во всех сферах, которые имеют отношение к авиации:

1. Разработчики и тестировщики программных продуктов для ОВД.
2. Инженерно-технический персонал, участвующий в обслуживании и поддержании работоспособности систем.
3. Руководящий и административный персонал.
4. Авиадиспетчеры.
5. Летный состав.

Следовательно, исследование человеческого фактора является сложной процедурой, поскольку необходимо принимать во внимание множество обстоятельств.

Метод оценки рисков информационной безопасности на основе байесовского подхода

Одним из основных этапов оценки рисков информационной безопасности является анализ информационных процессов системы (рис. 2).

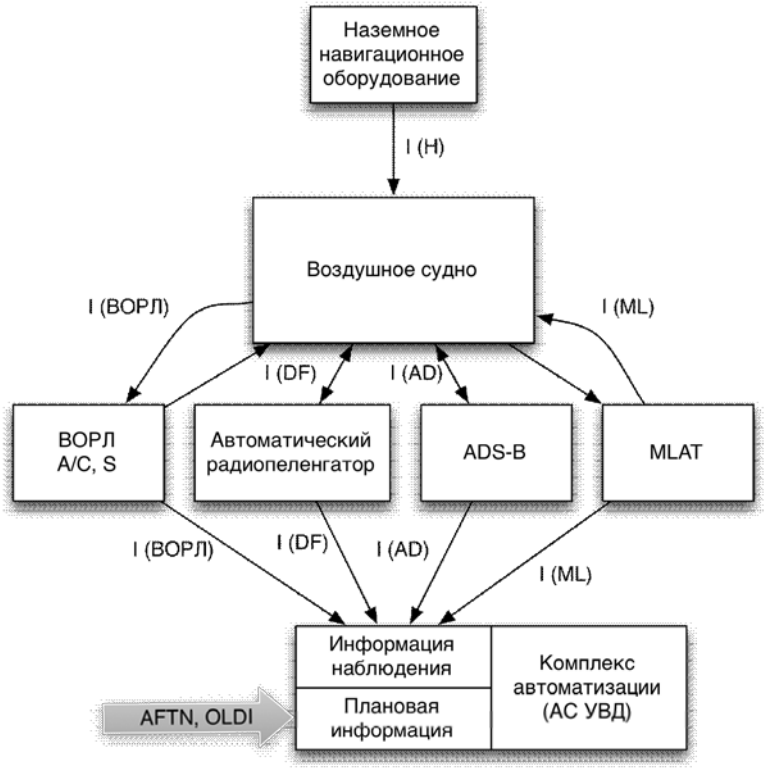

Рис. 2. Структураная схема информационных процессов при ОВД

На рис. 2 I(H) – информация, поступающая от наземного навигационного оборудования на ВС, I(ВОРЛ) – информация от вторичного обзорного радиолокатора, I(DF) – информация от автоматического радиопеленгатора, I(AD) – информация от систем зависимого наблюдения, I(ML) – информация от многопозиционных систем наблюдения. Таким образом, АС УВД обрабатывает два вида информации:

1. Информация наблюдения I(Sur)=I(ВОРЛ)+I(DF)+I(AD)+I(ML).
2. Плановая информация I(Pl)=I(AFTN)+I(OLDI).

Следовательно, информация, обрабатываемая на АС УВД, имеет вид I(Aut)=I(Pl)+I(Sur).

Метод оценки рисков информационной безопасности на основе байесовского подхода

Риск информационной безопасности – это потенциальная возможность использования уязвимостей актива или группы активов конкретной угрозы для причинения ущерба [8].

Риск можно определить следующим выражением:

$$R=P \cdot S, \quad (1)$$

где R – риск информационной безопасности, P – вероятность реализации угрозы, S – величина последствий осуществления угроз.

Многие статистические задачи независимо от методов их решения обладают общим свойством: до того как получен конкретный набор данных, в качестве потенциально приемлемых для изучаемой ситуации рассматривают несколько вероятностных моделей. После того как получены данные, получают выраженное в некотором виде знание об относительной приемлемости этих моделей. Одним из способов “пересмотра” относительной приемлемости вероятностных моделей является байесовский подход, основанный на теореме Байеса.

Основное отличие байесовского подхода от других статистических подходов состоит в том, что до того, как будут получены данные, лицо, принимающее решение, рассматривает степени своего доверия к возможным моделям и представляет их в виде вероятностей.

Объективные статистические данные зачастую отсутствуют в реальных задачах анализа риска

и принятия решений, что делает использование традиционных частотных подходов неправомерным. Имеющаяся в распоряжении информация об оцениваемой системе может содержать только субъективные оценки в виде экспертных оценок и суждений. Более того, ситуация, в которой принимается решение, может быть вообще новой и никогда ранее не анализируемой. Данная особенность усложняет процесс принятия решений и может поставить под сомнение какие-либо выводы и заключения. Поэтому в данной ситуации байесовский подход может оказаться эффективным.

В соответствии с формулой Байеса (2) условная вероятность P(θ|y) (вероятность гипотезы θ при наступлении события y) определяется из соотношения:

$$P(\theta \mid y) = \frac{P(y \mid \theta) \bullet P(\theta)}{P(y)}, \qquad (2)$$

где P(θ) – априорная вероятность гипотезы θ; P(y|θ) – вероятность наступления события y при истинности гипотезы θ.

Обозначим возможную угрозу информационной безопасности системы как T(ОрВД). Соответственно для параметров оценивания системы угрозы будут иметь вид: T(COM), T(AUT), T(SaN), T(HUM). Вероятность успешной реализации угрозы обозначим как p(T); имеющиеся уязвимости для каждого параметра оценивания обозначим как: VCOM1,..,VCOMn; VAUT1,..,VAUTn; VSaN1,..,VSaNn; VHUM1,..,VHUMn; вероятности успешной эксплуатации уязвимости обозначим как p(V1,...,Vn); условную величину “потенциал атаки” через переменную A (A ∈ [0,1], распределение случайной величины A – f(A)).

Величины уязвимостей параметров оценивания: VCOM1,..,VCOMn ∈ [0,1], VAUT1,..,VAUTn ∈ [0,1]; VSaN1,..,VSaNn ∈ [0,1] , VHUM1,..,VHUMn ∈ [0,1]. Обобщенные величины уязвимостей обозначим как Vi= VCOM1+...+VCOMn+ VAUT1+..+ VAUTn+ VSaN1+..+ VSaNn+ VHUM1+..+ VHUMn.

Угроза в общем виде T не реализуется, если A≤p(Vi), и реализуется, если A>p(Vi). Исходя из этого введем две новые переменные Vi (pos) –факт использования уязвимости, Vi(neg) – отсутствие факта эксплуатации уязвимости. Построим условную зависимость событий в виде графа (рис. 3).

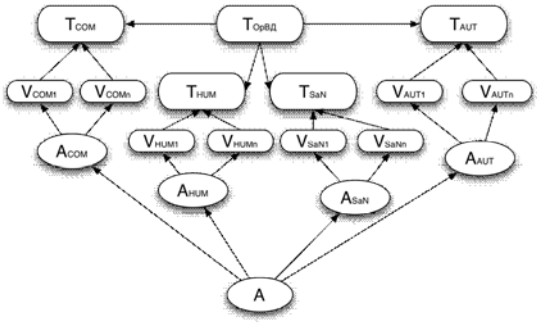

Рис. 3. Байесовская сеть реализации угрозы информационной безопасности системы ОрВД

При помощи байесовских сетей можно проанализировать закономерности в данных параметров оценивания системы. Множество ребер, представляющее собой все пути между некоторыми двумя вершинами, соответствует условной зависимости между этими вершинами.

Выводы

В статье проанализированы информационные процессы и параметры оценивания системы организации воздушного движения. Концептуализируются основные составляющие системы. Предлагается метод оценки рисков информационной безопасности на основе байесовского подхода.

Оценки риска тем более надежны, чем большее число наблюдений использовано для их вычисления. Очевидно, что накопление информации в процессе изучения объекта, например, последствий чрезвычайных ситуаций, позволяет уточнять ранее полученные оценки последствий воздействия чрезвычайных ситуаций. Уточнение оценок осуществляется с помощью формулы Байеса.

Формула Байеса – это формула вероятности гипотез, она используется для коррекции имеющейся информации о вероятности событий на основе результатов новых испытаний.

Направление дальнейших исследований связано с развитием метода оценки рисков информационной безопасности и построением математической модели оценок рисков информационной безопасности системы организации воздушного движения.

1. Биковець І.С. Захист інформації в системі організації повітряного руху / І.С. Биковець, В.О. Клименко, С.Г.Кравцов, Ю.А. Чередніченко та ін. – К.: ДП ОПР України, 2008. – 235 с. 2. Кулик Н.С Энциклопедия безопасности авиации / Н.С. Кулик, В.П. Харченко, М.Г. Луцкий и др.; Под ред. Н.С. Кулика. – К.: Техника, 2008. – 1000 с. 3. Кастельс М. Информационная эпоха: экономика, общество и культура / М. Кастельс. – М. : ГУ ВЩЭ. –2000. – 608 с. 4. Жуков И.А., Дрововозов В.И. Способы повышения надежности и безопасности сбора информации в системах управления реального времени // Проблеми інформатизації та управління: Зб. наук. пр. – К.: НАУ, 2008. – Вип. 1(23). – С. 263–277. 5. Автоматизированные системы управления воздушным движением / под ред. В.И. Савицкого. – М.: Транспорт. 1986. – 192с. 6. Концепция розвитку цивільної авіації України. Затверджено постановою Кабінету Міністрів України від 28 грудня 1996 р. № 1587. 7. Руководство по обучению в области человеческого фактора.(Doc.9683-AN/950). – Издание первое. – Канада, Монреаль, ICAO, 1998. – 333 с. 8. ISO 27005 ISO/IEC 27005:2008. Informationtechnology. Securitytechniques. Informationsecurityriskmanagement – ISO / IEC, 2008. – 70 с.