УДК 004.4,272

Многокритериальный алгоритм принятия решения в системе обеспечения информационной безопасности объектов гражданской авиации

Короткова Т.И.

Московский авиационный институт (национальный исследовательский университет), МАИ, Волоколамское шоссе, 4, Москва, А-80, ГСП-3, 125993, Россия

e-mail: tatyanamail11@yandex.ru

Аннотация

Рассматривается задача защиты информации в авиационных системах. Приведено системное описание источников и угроз информационной безопасности объектов гражданской авиации. Выявлена иерархическая система принятия решения по синтезу системы защиты. Предложен алгоритм на базе экспертного оценивания. Особенностями системы являются многокритериальность, условия неопределенности и дискретность.

Ключевые слова: авиационная система, алгоритм, система защиты информации, условия неопределенности, иерархическая структура, многокритериальность.

Введение

Проблема защиты авиационных систем от случайных и преднамеренных воздействий естественного и искусственного характера относится к приоритетным направлениям исследований. Надёжное обеспечение информационной безопасности

объектов гражданской авиации является одной из гарантий высокого уровня безопасности полётов в целом. Большое внимание к этой проблеме подтверждают разработанные стандарты на уровень угроз, на факторы опасности, допустимые риски, управление риском и т.п. [1]. Известны исследования, связанные с наличием случайных факторов и разработкой методов управления рисками в условиях случайности при актах незаконного вмешательства на воздушном транспорте [2]. Система обеспечения информационной безопасности объектов гражданской авиации относится к сложным системам, управление безопасностью которых сопряжено с целым рядом не решённых на данный момент задач. К ним, в частности, относятся многие вопросы, связанные с принятием решений в условиях большой размерности и наличии нескольких показателей качества, определяющих уровень безопасности.

Системный анализ проблемы и постановка задачи

Создание механизма, обеспечивающего информационную безопасность в авиационной отрасли и в системах управления воздушным движением, предполагает: классификацию информации и информационных систем с целью формирования надлежащего уровня информационной безопасности, создание директив с рекомендациями по обработке информации и выбору категории информационной системы, а также разработку минимальных требований к информационной безопасности в зависимости от потенциала возможного ущерба и типа нарушителя в чрезвычайных ситуациях. При этом предполагается создание

методических указаний по управлению рисками и по организации системы информационной безопасности.

Обеспечение сохранности конфиденциальной информации необходимо начинать с определения системы угроз, то есть негативных процессов, способствующих утечке информации. По цели воздействия можно выделить 3 типа угроз безопасности автоматизированным системам обработки информации: угрозы нарушения конфиденциальности информации; угрозы нарушения целостности информации; угрозы нарушения работоспособности системы.

Опасные воздействия можно разделить: случайные и преднамеренные. Причины случайных: аварийные ситуации из-за стихийных бедствий, отказы и сбои аппаратуры, ошибки в программном обеспечении, ошибки в работе обслуживающего персонала и пользователей, помехи в линии связи из-за воздействия внешней среды.

В общем виде все угрозы делятся на две группы: внутренние и внешние. Внутренние угрозы инициируются персоналом объекта, на котором установлена система, содержащая конфиденциальную информацию. Из-за неудовлетворительной зарплаты или отношения руководства, отдельные сотрудники с высоким уровнем самооценки могут предпринимать действия по выдаче информации лицам, заинтересованным в её получении. Внешние угрозы возникают благодаря деятельности недобросовестных конкурентов, преступных элементов, иностранных разведывательных служб, из-за неумелой постановки взаимоотношений с представителями госструктур и общественных организаций. Действия извне могут

быть направлены на пассивные носители информации следующим способом: похищение или снятие копий с различных носителей информации; снятие информации в процессе коммуникации или передачи по сети связи; уничтожение информации или повреждение её носителей; случайное или преднамеренное доведение до сведения конкурентов документов и материалов, содержащих секретную информацию. Действия извне могут быть также направлены на персонал и выражаться в формах подкупа, шантажа, выведывания с целью получения информации, переманивания ведущих специалистов на конкурирующую фирму и т.п.

Системный подход к описанию информационной безопасности выделяет в качестве важнейшей составляющей математическую модель принятия решения в задаче синтеза системы защиты информации. Проблема синтеза системы защиты информации в информационной системе связана с решением целого ряда задач, к которым, в частности, относятся: выявление защищаемой информации, системы угроз и каналов утечки информации, проведение оценки уязвимости и рисков, определение требований к системе защиты информации, осуществление выбора средств защиты и управление защитой.

Задача синтеза системы защиты информации в информационной системе основывается на экспертном оценивании возможных вариантов, количество которых достаточно велико. При этом оценка проводится по векторным критериям тоже достаточно большой размерности. Учитывая сложность поставленной задачи,

естественным приёмом решения является иерархический подход и формирование многоуровневой системы принятия решения (рис.1).

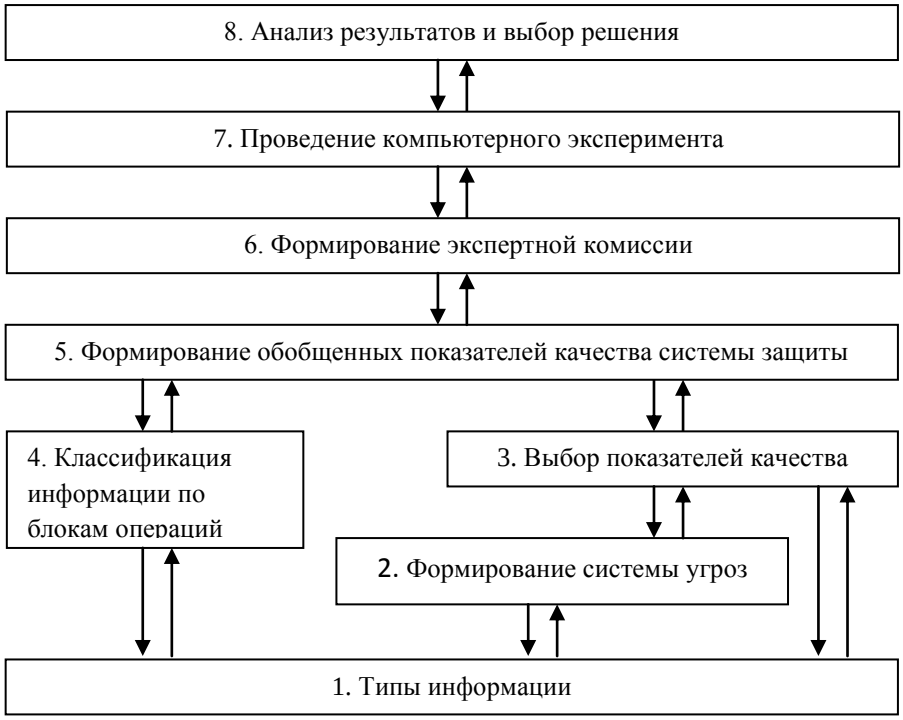

Рис.1. Блок-схема принятия решения.

Формализация нижних уровней

Рассматривается информационная система, в которой хранится, передается и обрабатывается информация p типов $u_1,\ldots,u_p$.

К выявленным угрозам информационной безопасности и нейтрализующим контрмерам в авиационной отрасли и системах управления воздушным движением относятся: идентификация и аутентификация субъектов доступа к объектам доступа; чрезмерное межсетевое взаимодействие; слабые пароли; слабый контроль над управлением доступом к ключевым системам управления воздушным движением;

несоответствие права доступа и объёма полномочий; необходимость зашифровки данных во время обработки или сохранения информации; мониторинг и оценка состояния текущего уровня информационной безопасности; наличие квалифицированного и подготовленного персонала; разработка правил реагирования на инциденты информационной безопасности; прохождение персоналом, обслуживающим критичные системы относительно механизмов обеспечения информационной безопасности, повышения квалификации в сфере информационной безопасности в нужном объёме в соответствии с их ответственностью за обеспечение информационной безопасности; обеспечение эффективных мер по обнаружению инцидентов информационной безопасности в системах управления воздушным движением и реагированию на них.

Допустим, что информация может быть подвержена системе q угроз видов $s_1,\ldots,s_n$ $s_1,\ldots,s_n$. По блокам операций информация классифицируется на n подсистем:

$$u^1=(u_1^1,\ldots,u_{p_1}^1),...,u^n=(u_1^n,\ldots,u_{p_n}^n),$$

например, по блокам хранения, передачи и обработки информации. Каждый вид s_i системы угроз характеризуется векторным показателем:

$$G^i=(G^{i1},...,G^{ir_i}),\quad i=\overline{1,q}$$

компонентами, которых могут быть риски и т.п. Каждый G^{ij} для всех $i=\overline{1,q}$ и $i=\overline{1,r_i}$ является функцией $u_1,...,u_p,s_1,...,s_q,\alpha_1,...,\alpha_e$, где $\alpha_1,...,\alpha_e$ некоторые неопределенные факторы. В соответствии с классификации информации по блокам операций классифицируется системы угроз и векторные показатели.

В результате формируется система обобщенных n векторных показателей: $G_i = (G_i^1, ..., G_i^q)$, $i = \overline{1,n}$ для системы защиты.

Описанная формализация представлена на рис.2.

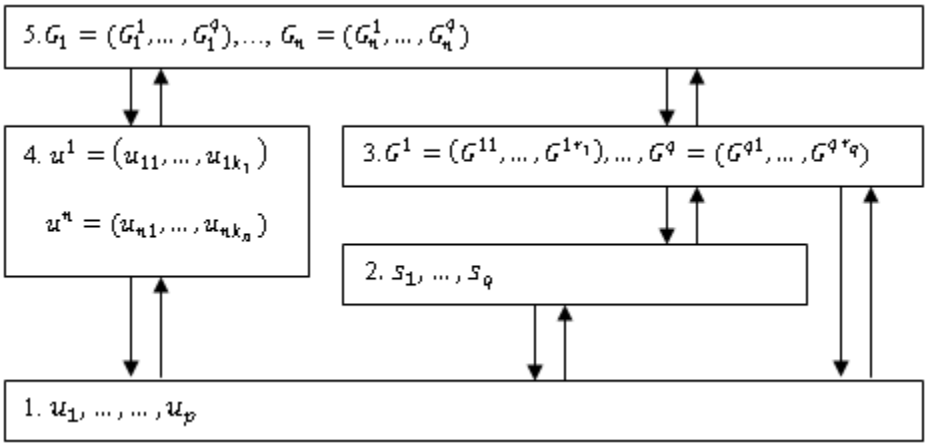

Рис.2. Формализация нижних уровней.

Классификация информации по блокам операций производится путём выборки n векторов из $u_1, ..., u_p$ размерности соответственно $k_1, ..., k_n$.

Алгоритм принятия решения

Принципиальной особенностью задачи выбора наиболее рационального варианта системы защиты информации является её многокритериальность. Кроме того, условия функционирования систем защиты информации характеризуются высокой степенью неопределенности. Эти неопределенности связаны с

недостаточной изученностью среды функционирования системы защиты информации и нечетким описанием показателей эффективности. Более того, описание системы защиты информации имеет большую размерность. Поэтому решение задачи принятия решения осуществляется через декомпозицию структуры информационной системы. Этот многоуровневый иерархический принцип поддержки принятия решения рассмотрен в работе [3] и применён для рассматриваемой системы.

Задачей экспертной комиссии является формирование оптимизационной модели в виде критериальной матрицы А, состоящей из векторных критериев G_i^j, где $i=\overline{1,n}$, $j=\overline{1,q}$. Каждый критерий G_i^j представляет из себя для каждого i-го блока операции выборку компонентов критерия G_j составленного для j-ой угрозы. В блоке формирования системы угроз каждому j-му типу угрозы s_j, $j=\overline{1,q}$, ставится в соответствие вектор x_j вариантов защиты . Для каждого i-го блока операций делается из компонентов этого вектора выборка

$$X_{ij}=(x_{ij}^1,\ldots,x_{ij}^{m_{ij}}),$$

количество компонентов, которой соответствует верхнему индексу m_{ij}. Эти выборки усложняют формализацию задачи принятия решения, но существенно снижают размерность и количество переборов при работе экспертной комиссии.

В соответствии с вышесказанным, критериальная матрица А имеет вид:

$$A=\begin{pmatrix} G_1^1(u_{11},...,u_{1,k1},x_{11},\alpha_{11}) & .. & . & G_1^q(u_{11},...,u_{1,k1},x_{1q},\alpha_{1q}) \\ ... & .. & . & ... \\ ... & .. & . & ... \\ G_n^1(u_{n1},...,u_{n,kn},x_{n1},\alpha_{n1}) & .. & . & G_n^q(u_{n1},...,u_{n,kn},x_{nq},\alpha_{nq}) \end{pmatrix}$$

В этой матрице векторные показатели качества G_i^j зависят от векторов неопределенности a_{ij}, $i=\overline{1,n}$, $j=\overline{1,q}$. По параметрам a_{ij} используется операция максимизации, а по управляющим переменным x_{ij} - операция минимизации. Оптимальный вариант защиты обеспечивается по принципу гарантированного результата минимаксной матричной оценкой. Минимаксная матричная оценка проводилась для векторных критериев G_i^j с использованием кооперативного равновесия по Парето.

Результаты компьютерного эксперимента

Верификация алгоритма проводилась на базе компьютерного эксперимента с применением набора процедур метода экспертного оценивания Delphi. Эта среда программирования имеет удобный интерфейс, достаточно быстрый браузер классов, мгновенный вывод подсказки авто завершения кода и самый быстрый компилятор. Метод ориентирован на три составляющих: интуитивно-логический анализ задачи; решение и выдача количественных и качественных оценок; обработка данных в программном модуле и вывод итоговой оценки степени защиты информации. К основным модулям программы относятся: модуль Подключения, в котором идёт в частности, загрузка логина и пароля; модуль Администратора, который необходим для занесения списка оценок и ведения работы с таблицами по распределению

оцениваемых вариантов и результатов экспертных оценок; модуль Пользователей, в котором реализуется возможность управления пользователями, имеющими доступ к базе данных; модуль Оценок, в котором идёт обработка результатов экспертного оценивания; модуль Отчётов, в котором идёт фильтрование и сортировка оценок; модуль Аутентификации проверяет соответствие всех данных; модуль Результатов отвечает за вывод результатов на экран и выход из программы. Рабочий экран Delphi имеет 4 основных окна: главное окно, окно формы Form 2, окно инспектора объектов Object Inspector окно редактора кода Unit1.pas. На рис.3 приведен скриншот по окончательным опросам экспертов.

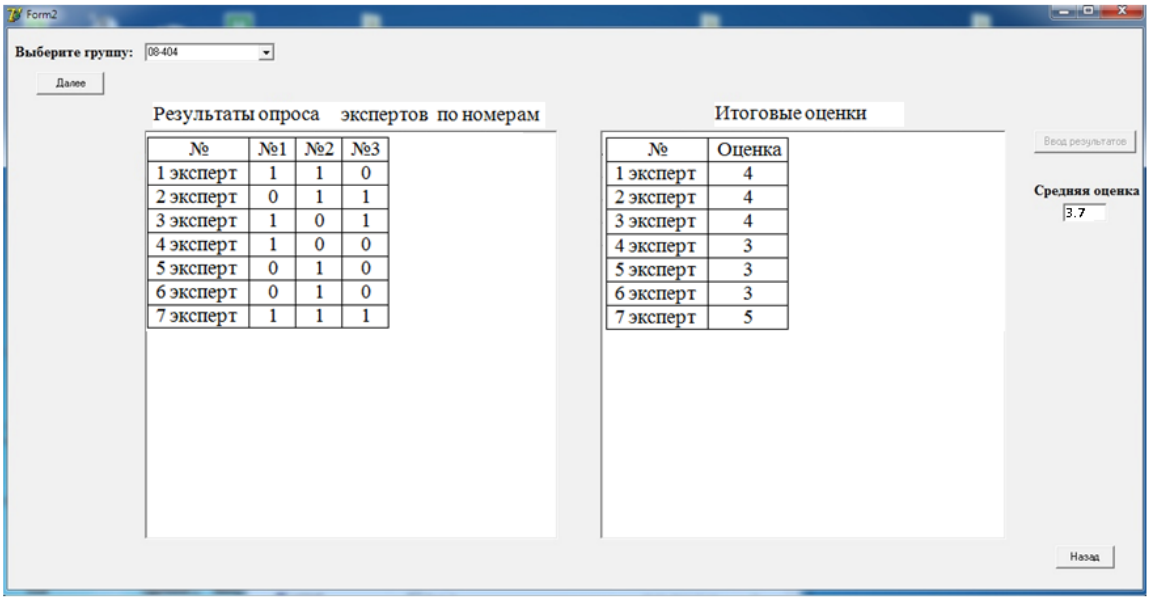

Рис.3. Результаты опроса экспертов.

Библиографический список

1. Руководство по обеспечению безопасности полётов (РУБП) / Пер. с англ. Doc. 9859, AN/460, ИКАО (Монреаль). - М.: Минтранс РФ, 2009.-293 с.

2. Куклев Е.А., Волынский Ю.М. Обеспечение авиационной безопасности объектов гражданской авиации на основе методов управления рисками возникновения актов незаконного вмешательства. Наука и транспорт // Гражданская авиация. 2013. № 3(7). С. 16-21.
3. Короткова Т.И., Чагина А.С. Алгоритм управления степенью защиты многоуровневой информационной системы в задаче синтеза системы защиты информации // Информационные и телекоммуникационные технологии. 2014. № 22. С. 52-55.