УДК 004.051 DOI: 10.18698/2308-6033-2020-7-2000

Принципы организации защиты информации в автоматизированной системе подготовки данных полета летательных аппаратов

© А.Г. Андреев[1], В.Н. Захаров[1], Г.В. Казаков[1], В.В. Корянов[2]

[1]ФГБУ «4 ЦНИИ» Минобороны России,
Московская область, г. Королёв, 141091, Россия
[2]МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

При проектировании автоматизированных систем подготовки данных полета летательных аппаратов многие практические задачи решают с помощью введения недостаточных либо избыточных средств защиты. Это порождает уязвимость системы защиты информации. Согласно анализу ряда публикаций, основы теории защиты информации сводят к формулировке аксиом, что позволяет сделать вывод об отсутствии в настоящее время законченной теории информационной безопасности компьютерных систем. Вследствие этого существует множество вопросов, в том числе и общего характера, которые необходимо проработать. Рассмотрен комплекс вопросов, связанных с обеспечением информационной безопасности автоматизированной системы подготовки данных полета летательных аппаратов. Раскрыто содержание двух основных принципов организации защиты информации в этой системе. Первый принцип требует изучения всех аспектов, относящихся к проблеме обеспечения информационной безопасности системы, второй — оптимального управления средствами обеспечения защиты информации автоматизированной системы подготовки данных полета летательных аппаратов.

Ключевые слова: *автоматизированная система, защита информации, данные достижимости, данные полета, летательный аппарат, подготовка данных, политика информационной безопасности*

Введение. Для современного этапа информатизации различных областей деятельности государства характерна устойчивая тенденция использования новейших достижений в области информационных технологий. Однако многие практические задачи при проектировании автоматизированных систем подготовки данных (АСПД) полета летательных аппаратов (ЛА) решают введением либо недостаточных средств защиты, либо избыточных. Такие ситуации порождают уязвимость системы защиты информации (СЗИ) АСПД.

Очевидно, что процесс проектирования СЗИ, основанный только на решении задачи защиты информации АСПД от известных угроз, недостаточен для целей АСПД, поскольку для функционирования любой подсистемы (в том числе и СЗИ) требуются дополнительные временны́е и энергетические ресурсы, что снижает эффективность функционирования системы в целом.

Цель настоящей работы — на основании анализа современных методов теории безопасности информации разработать основные принципы построения защищенных систем для практического решения задач обеспечения информационной безопасности (ИБ) АСПД при проектировании СЗИ.

Обзор публикаций. Следует отметить, что до сих пор теория безопасности информации сводится преимущественно к формулировке основных аксиом. Так, в [1–3] изложены теоретические основы моделирования политик информационной безопасности (ПИБ) системы. Оценка качества СЗИ в [2] определена следующим образом: СЗИ хорошая, если она надежно поддерживает политику информационной безопасности, в противном случае — неудовлетворительная. Язык, на котором выражается ПИБ, базируется на вычислении функций принадлежности, логического выражения и оператора «если…, то», образующих язык $Я_1$. Для поддержания языка $Я_1$ необходимо иметь язык $Я_2$, для которого необходимо использовать язык $Я_3$ более низкого уровня, и т. д.

Если модель ПИБ формальная [1, 3], то вероятно доказать или опровергнуть утверждение о том, что множество предоставленных услуг полностью и однозначно определяет эту политику. Изложенный в [2] подход определяет методологию анализа СЗИ. При этом иерархия языков может быть неоднозначной. Главное — удобство представления и анализа. Проведение подобного анализа для каждой СЗИ является дорогостоящей процедурой. Выход был найден в том, чтобы условия теорем, доказывающих поддержку ПИБ, формулировать без доказательства в виде стандартов. В 1983 г. такой стандарт был создан в США — так называемая Оранжевая книга, в которой содержались требования гарантированной поддержки двух классов политик: дискреционной и политики MLS (MultiLevel Security) [4, 5]. В 1987 г. этот метод применен к распределенным сетям, в 1991 г. — для баз данных. Впоследствии был опубликован документ «Общие критерии безопасности», на основе его анализа в Российской Федерации разработан ГОСТ [6–8].

В [9, 10] основное внимание уделено общим вопросам защиты информации в правовом и организационном аспектах; в [1, 11, 12] — вопросам описания моделей ПИБ и методам криптографической защиты информации. Особый вид разрушающего программного воздействия на информацию АС оказывают программные закладки [13].

Следует отметить, как только принимаются меры по использованию известных методов теории безопасности информации для практического решения задач обеспечения ИБ АСПД при проектировании СЗИ, сразу выявляется значительное число ошибок семантического и синтаксического плана. В [14, 15] сделана попытка практического применения методов теории безопасности к защите информации

в центрах управления полетами космических аппаратов. Новизна этих работ состоит в разработке модели угроз и связанной с ней модели защиты на основе использования математического аппарата теории плоских графов.

Таким образом, пока нет законченной теории информационной безопасности компьютерных систем, поэтому существует множество вопросов общего характера, которые необходимо подвергнуть определенной проработке.

Основная проблема защиты информации. Анализ мировой практики эксплуатации систем различного класса и назначения позволил сделать вывод: независимо от уровня защищенности системы нет гарантии, что рано или поздно она не будет подвергнута успешной кибератаке с нанесением ей определенного уровня ущерба — от ощутимого до катастрофического. Необходимо иметь в виду два важных обстоятельства. Во-первых, чтобы нанести ущерб атакуемой системе, достаточно реализовать лишь одну преднамеренную угрозу. Во-вторых, известные ПИБ устанавливают лишь определенные правила, обеспечивающие безопасное функционирование системы в условиях воздействия преднамеренных угроз. Однако необходимо разрабатывать и ПИБ, учитывающие и случайные угрозы (в основном человеческий фактор).

Преднамеренная угроза также связана с человеческим фактором, но в этом случае весь потенциал злоумышленника направлен на реализацию выбранной им угрозы нарушения безопасного функционирования системы. В этом плане его усилия направлены на то, чтобы формально действующая СЗИ не заметила, что условия безопасности нарушены.

Для конкретной системы с учетом ее структурных особенностей и особенностей эксплуатации возможно обеспечить такой уровень защиты, который злоумышленнику с его потенциалом нападения не преодолеть. При этом в процессе разработки ПИБ следует уделить особое внимание возможности нелегального использования злоумышленником правил доступа, подменив их своими, и обхода средств защиты. При решении задачи обеспечения защиты информации АСПД как минимум необходимо соблюдать принципы построения защищенных систем.

Принципы обеспечения требуемого уровня защиты информации. Известны основные группы средств обеспечения качества любой информационной продукции:

- технические — конструктивные, технологические, метрологические;
- информационные — программные, аппаратные, системные;
- экономические — финансовые, нормативные, материальные;
- социальные — организационные, правовые, кадровые и т. д.

С использованием этих средств можно выделить следующие принципы обеспечения защиты подготавливаемых АСПД данных:

- данные достижимости (ДД);
- данные полета ЛА (ДПЛА).

Первый принцип «Установление всех аспектов, относящихся к проблеме защиты информации АСПД». К указанным аспектам относятся (табл. 1):

- информационный,
- нормативно-правовой,
- организационный,
- программный,
- технический,
- физический,
- эргатический.

Таблица 1

Содержание аспектов проблемы защиты информации автоматизированных систем подготовки данных

Наименование	Содержание
Информационный	Установление состава, целей и задач информационно-баллистического обеспечения (ИБО) АСПД
Нормативно-правовой	Соблюдение всех требований к СЗИ АСПД. Формирование требований к защите информации, циркулирующей в АСПД, осуществляется Заказчиком с учетом ГОСТ [16, 17] и стандартов организации и включает [18]: обоснование решения о необходимости защиты информации в АСПД; обоснование класса защищенности АСПД по существующей системе классификации уровней защищенности системы
Организационный	Скоординированное взаимодействие всех организаций, имеющих отношение к проектированию, разработке и эксплуатации АСПД
Программный	Обоснование разрабатываемых алгоритмов подготовки и контроля реализуемости ДД и ДПЛА, полное документирование и разработка на их основе специального программного обеспечения (СПО) на языках высокого уровня с соответствующими комментариями
Технический	Использование в АСПД наиболее эффективных технических средств вычислительной техники отечественного производства
Физический	Обеспечение безопасности для любых несанкционированных физических действий на территории контрольной зоны АСПД
Эргатический	Решение задачи обеспечения безошибочности взаимодействия системы человек — машина

Установление состава, целей и задач ИБО АСПД (информационный аспект) выполняется в соответствии со схемой на рис. 1.

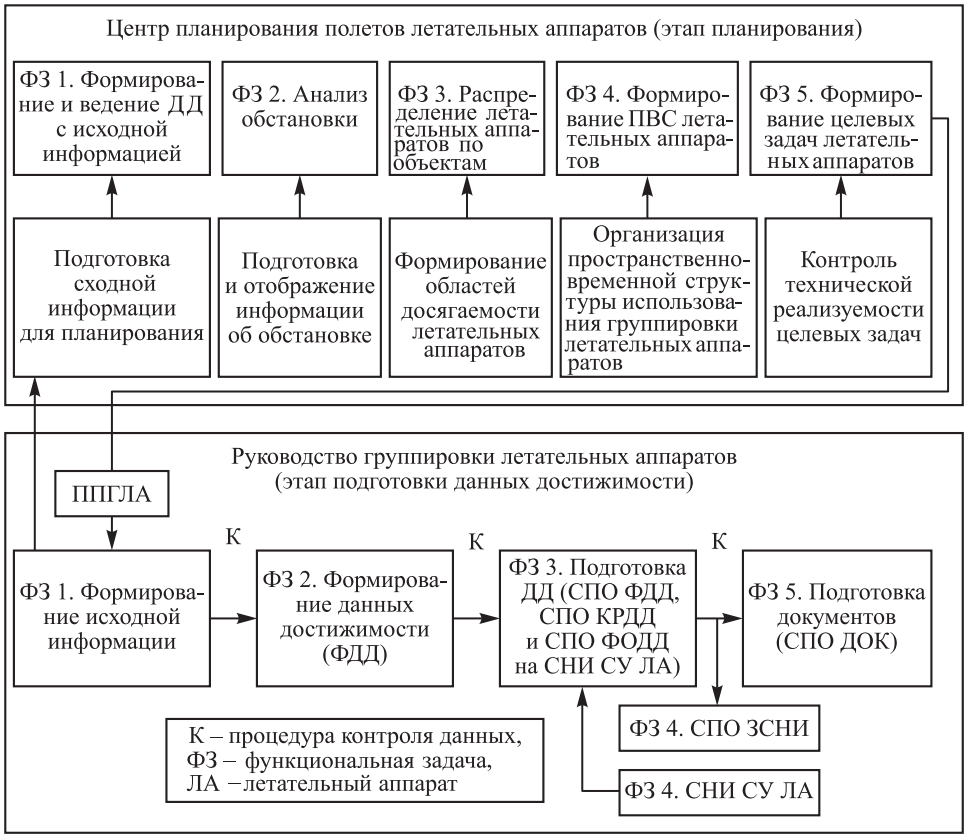

Рис. 1. Схема организации информационно-баллистического обеспечения

Согласно данным (см. рис. 1), процесс подготовки ДД включает два этапа:

- формирование ДД, определяющих план полетов ЛА;
- подготовка ДД, определяющих распределение ЛА по запланированным пунктам прибытия.

Этап подготовки ДД включает СПО, выполняющее определенные функциональные задачи:

- СПО формирования ДД;
- СПО контроля реализуемости ДД;
- СПО записи информации на специальный носитель информации (СНИ) для системы управления (СУ) ЛА.

Для обеспечения достоверности подготовленных ДД как одной из характеристик информационной безопасности необходимо руководствоваться простым принципом [19]: результат выполнения каждой операции должен завершаться контролем его правильности (символ К на рис. 1).

Второй принцип «Оптимальное управление средствами обеспечения защиты информации АСПД». Этот принцип требует решения следующих задач:

- разработки необходимой ПИБ;
- выявления наиболее важной информации, которая требует особой защиты и определяет необходимый уровень защищенности АСПД;
- установления полного, по возможности актуального состава угроз;
- описания актуального состава угроз в структуре семиуровневой базовой модели угроз;
- определения для всех установленных источников угроз их потенциалов по реализации угрозы в соответствии с моделью нарушителя;
- составления профиля защиты и задания по безопасности для АСПД;
- управления рисками АСПД;
- мониторинга причин нарушения свойств ИБ.

Рассмотрим ниже подробно эти задачи.

Задача 1. При разработке ПИБ следует учитывать, что все ее модели основаны на следующих базовых понятиях [1]:

- система определяется как совокупность взаимодействующих субъектов и объектов. Объекты — контейнеры, содержащие информацию; субъекты — выполняющиеся программы, которые воздействуют на объекты различными способами;
- все взаимодействия в системе моделируются установлением отношений определенного типа между объектами и субъектами. Множество типов отношений определяется в виде набора операций, которые могут выполнять субъекты над объектами;
- все операции контролируются монитором взаимодействий и либо запрещаются, либо разрешаются в соответствии с правилами ПИБ;
- ПИБ задается в виде множества правил, определяющих взаимодействие субъектов и объектов. Нарушение этих правил фиксируется средствами защиты, которые пресекают соответствующее взаимодействие;
- множества субъектов и объектов и отношения между ними на данный момент времени определяют состояние системы. Каждое состояние системы является либо безопасным, либо небезопасным в соответствии с принятым критерием безопасности;
- основной элемент модели безопасности — теорема о том, что система, находящаяся в безопасном состоянии, не может перейти в небезопасное состояние без нарушения ПИБ.

Основная цель разработки ПИБ и ее формальной модели [2] состоит, во-первых, в определении условий, которым должно подчиняться поведение системы, во-вторых, в выработке критерия безопасности и, в-третьих, в проведении формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений.

Выбор ПИБ можно осуществить из следующих известных его видов:

- дискреционной ПИБ;
- мандатной ПИБ;
- ПИБ информационных потоков;
- ПИБ ролевого разграничения доступа;
- ПИБ изолированной программной среды;
- ПИБ доменов и типов.

Если по каким-либо причинам ни одна из существующих ПИБ не может удовлетворить требования к ИБ АСПД, то проводится разработка новой специфической ПИБ. Для этого сначала определяют вербальную сущность ПИБ. Например, суть дискреционной ПИБ заключается в дискреционном управлении доступом со следующими свойствами:

- все субъекты и объекты идентифицированы;
- права доступа субъектов к объектам системы определяются на основании внешнего по отношению к системе правила;
- основным элементом дискреционного разграничения доступа является матрица доступов $M[s,o]$ размером $|S|\cdot|O|$, каждый элемент которой определяет доступ субъекта s к объекту o с правом доступа $r \in R$, где R — множество прав доступа.

Доказано, что дискреционная ПИБ имеет существенные недостатки, поэтому для АСПД целесообразно использовать мандатную ПИБ, основанную на мандатном разграничении доступа, определяемом условиями:

- все субъекты и объекты системы однозначно идентифицированы;
- задана решетка уровней конфиденциальности информации;
- каждому объекту системы присвоен уровень конфиденциальности;
- каждому субъекту системы присвоен уровень доступа, определяющий степень доверия к нему и необходимости его присутствия в АСПД.

При формальном построении модели ПИБ необходимо опираться на основные аксиомы теории защиты информации [11, 14]. При анализе ИБ системы в рамках выбранной ПИБ важно уделить внимание

доказательству алгоритмической разрешимости (неразрешимости) проверки безопасности произвольных систем с данной ПИБ. Например, в работе [1] доказано, что при использовании дискреционной модели Харрисона — Руззо — Ульмана (HRU security model) задача проверки безопасности произвольной системы с такой ПИБ является алгоритмически неразрешимой задачей, алгоритмически разрешимой — для мандатной ПИБ. Мандатная ПИБ чаще всего описывается моделью Белла — Лападула (Bell-LaPadula model) [1–3, 11, 12]. В связи с этим для АСПД можно рекомендовать данную модель.

При проектировании СЗИ АСПД необходимо конкретизировать указанные выше элементы ПИБ в виде модели Белла — Лападула и для этих элементов доказать теорему о формальном соответствии системы выбранному критерию безопасности при соблюдении установленных правил и ограничений.

Задача 2. Для выявления наиболее важной информации проводится ранжирование всех циркулирующих в АСПД видов данных по их важности с точки зрения величины ущерба, который может иметь место при нарушении хотя бы одного из основных свойств ИБ.

Задача 3. Для выявления полного актуального состава угроз используется методика, основанная на анализе всех имеющихся в распоряжении проектировщиков СЗИ, описаний реализованных угроз с целью установления возможности реализации данной угрозы в АСПД на данный период времени.

Задача 4. Проводится описание актуального состава угроз в структуре семиуровневой базовой модели угроз, которая включает следующие структурные элементы:

- аннотацию угрозы;
- возможные источники угрозы;
- способ реализации угрозы;
- информационные ресурсы (ИР), подверженные воздействию угрозы;
- используемые уязвимости;
- нарушаемые характеристики безопасности активов;
- возможные последствия реализации угрозы.

Задача 5. Для каждого вида установленных источников угроз проводится оценка его потенциала, определяющего возможность нарушителя реализовать ту или иную угрозу из актуального состава. Уровень вычисленного потенциала нарушителя по реализации угрозы определяет необходимый уровень защиты от этой угрозы.

Задача 6. Модель нарушителя связана с его потенциалом реализовать угрозу той или иной опасности. Эта модель содержит следующие структурные элементы, связанные определенным алгоритмом:

- мотивация нарушителя создать угрозу;
- квалификация нарушителя;
- знание нарушителем объекта нападения;
- доступ нарушителя к защищаемому активу АСПД;
- «оснащенность нарушителя средствами реализации угрозы».

В [6–8] указано, что важным условием корректного проектирования СЗИ любой системы, в том числе и АСПД, является разработка профиля защиты (ПЗ) и задания по безопасности (ЗБ). Общая схема последовательного формирования требований безопасности и спецификаций АСПД при разработке ПЗ и ЗБ представлена на рис. 2. Спецификации ПЗ и ЗБ представлены в табл. 2.

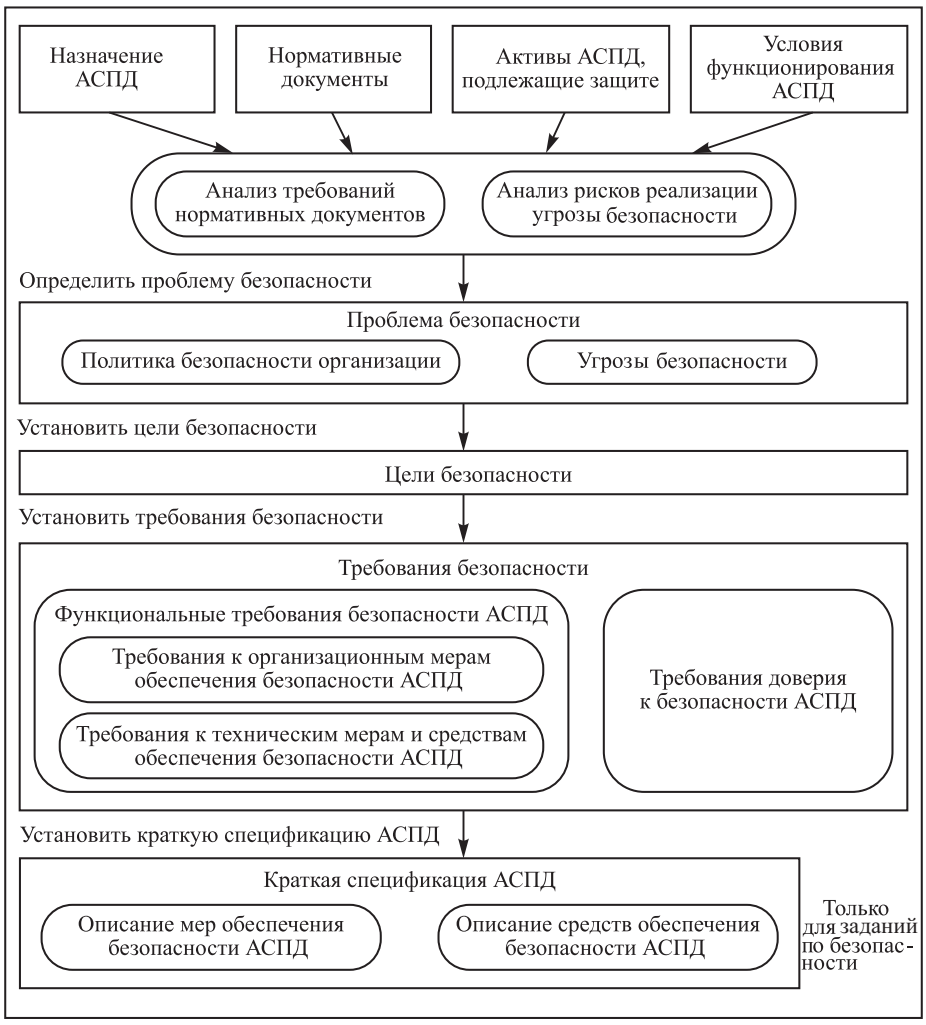

Рис. 2. Схема формирования требований безопасности АСПД в виде ПЗ и ЗБ

Таблица 2

Спецификации профиля защиты и заданий для безопасности в автоматизированных системах подготовки данных

Спецификация	
Профиль защиты	Задания для безопасности
1. Введение 1.1. Идентификация 1.2. Аннотация	1. Введение 1.1. Идентификация 1.2. Аннотация
2. Описание автоматизированных систем подготовки данных	2. Описание автоматизированных систем подготовки данных
3. Утверждения о соответствии автоматизированных систем подготовки данных требованиям безопасности	3. Утверждения о соответствии автоматизированных систем подготовки данных требованиям безопасности
4. Определение проблемы безопасности в автоматизированных системах подготовки данных 4.1. Угрозы безопасности Спецификация профиля защиты для автоматизированных систем подготовки данных 4.2. Политика безопасности организации	4. Определение проблемы безопасности в автоматизированных системах подготовки данных 4.1. Угрозы безопасности Спецификация заданий по безопасности для автоматизированных систем подготовки данных 4.2. Политика безопасности организации
5. Цели обеспечения безопасности автоматизированных систем подготовки данных	5. Цели обеспечения безопасности автоматизированных систем подготовки данных
6. Требования безопасности в автоматизированных системах подготовки данных 6.1. Функциональные требования безопасности автоматизированных систем подготовки данных 6.2. Требования доверия к безопасности автоматизированных систем подготовки данных	6. Требования безопасности в автоматизированных системах подготовки данных 6.1. Функциональные требования безопасности автоматизированных систем подготовки данных 6.2. Требования доверия к безопасности автоматизированных систем подготовки данных
7. Обоснование целей и требований безопасности в автоматизированных системах подготовки данных 7.1. Обоснование целей безопасности в автоматизированных системах подготовки данных 7.2. Обоснование требований безопасности, предъявляемых к системе защиты информации	7. Краткая спецификация системы защиты информации в автоматизированных системах подготовки данных
–	8. Обоснование целей и требований безопасности в автоматизированных системах подготовки данных 8.1. Обоснование целей безопасности в автоматизированных системах подготовки данных 8.2. Обоснование требований безопасности 8.3. Обоснование краткой спецификации системы защиты информации в автоматизированных системах подготовки данных

Во «Введении» должны быть указаны роли участников разработки, согласования, утверждения и применения ПЗ и ЗБ. Требования нормативных документов находят отражение в ПЗ и ЗБ для АСПД в виде политики безопасности организации — владельца системы. В «Определении проблемы безопасности» детально раскрываются угрозы безопасности, которым должна противостоять СЗИ АСПД, в структуре семиуровневой базовой модели угроз и политики безопасности, удовлетворяющей СЗИ АСПД. При формировании данного раздела используют результаты оценки рисков для определения того, каким угрозам безопасности необходимо противостоять применением мер и средств обеспечения безопасности системы.

«Цели обеспечения безопасности автоматизированных систем подготовки данных» включают цели безопасности для АСПД, отражающие направления решения проблемы безопасности. Эти направления связаны с особенностью АСПД: подобная система, с одной стороны, является сложным программным комплексом с основным свойством надежности СПО, с другой — специфической системой контроля с основным свойством «достоверность контроля».

Если в рамках АСПД определены домены безопасности, то в «Определении проблемы безопасности» выделена общая часть, относящаяся ко всей системе в целом, а также части, каждая из которых применима к конкретному домену безопасности, определенному в рамках АСПД.

В «Требованиях безопасности» задают требования для АСПД с учетом необходимого баланса технических и организационных мер обеспечения безопасности системы. Таким образом строится модель процесса защиты информации АСПД, представленная на рис. 3 [15].

Задача 7. Цель управления рисками АСПД — поддержать в процессе эксплуатации степень рисков на допустимом уровне при меняющихся условиях эксплуатации. Общая схема управления рисками приведена на рис. 4.

Для управления рисками создают систему управления информационной безопасностью (СУ ИБ). Если анализ рисков в процессе мониторинга рисков показывает, что риск превосходит допустимый уровень, то проводится обработка рисков с целью их минимизации, в том числе и путем изменения ПИБ.

Задача 8. Мониторинг предполагает выявление причин (источников) нарушения свойств ИБ. Процесс мониторинга может быть затруднен ввиду следующих факторов:

- разнообразия форматов, структуры и источников информации;
- множественности пользовательских интерфейсов;
- наличия в механизмах безопасности разных приложений.

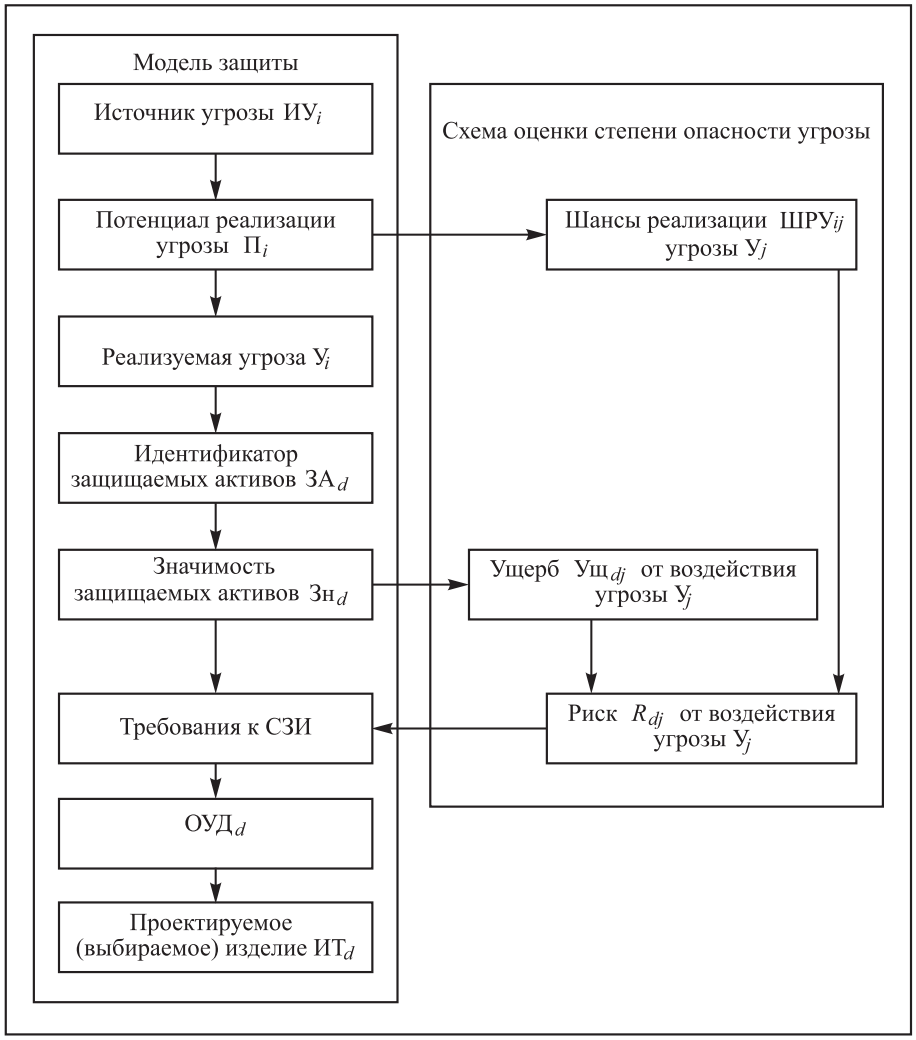

Рис. 3. Модель защиты активов автоматизированных систем подготовки данных при воздействии угрозы

Все это обусловливает последствия в виде увеличения:

- сроков выявления и устранения инцидентов безопасности;
- риска принятия неправильного решения из-за отсутствия своевременного доступа исполнителей к необходимой информации;
- сроков принятия решения;
- риска потери данных, пропуска существенных событий;
- затрат для качественного проведения мониторинга ИБ АСПД.

Общепринятого и универсального метода оценки риска нарушения ИБ произвольной системы не существует. Для управления рисками можно, например, использовать качественную оценку рисков согласно матрице оценки рисков (рис. 5).

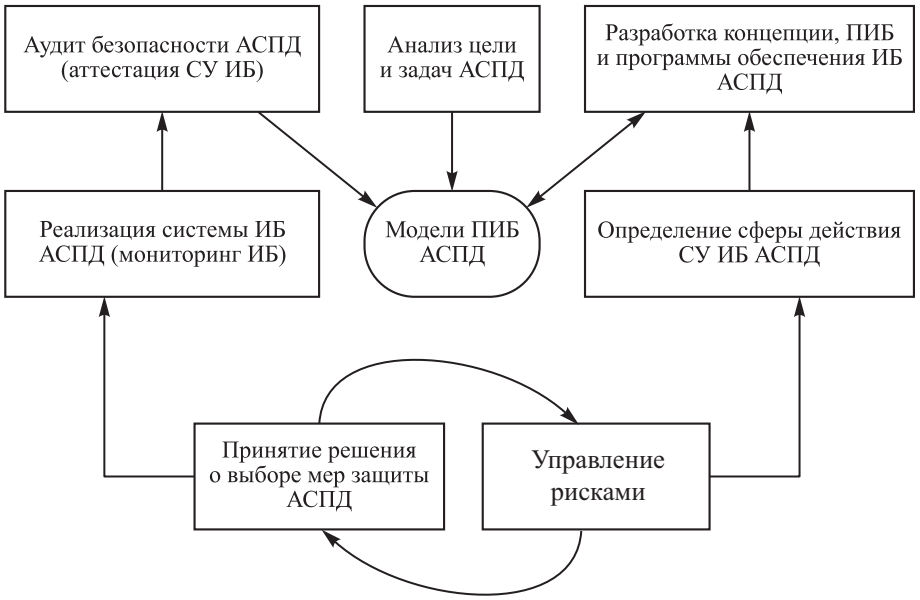

Рис. 4. Общая схема управления рисками

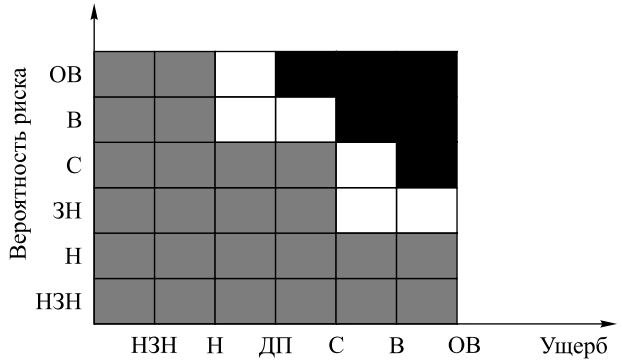

Рис. 5. Матрица оценки рисков:
уровни: НЗН — незначительный; Н — низкий; ДП — допустимый; ЗН — значимый; С — средний; В — высокий; ОВ — очень высокий

Темная зона матрицы определяет недопустимый уровень риска, что требует от разработчика АСПД включения процедуры обработки рисков с обоснованным выбором адекватных мер защиты. Наличие белой зоны диктует принятие определенных мер по защите информации с целью перевода текущего значения риска в серую зону, где уровень риска считается допустимым. Серой зоне соответствует такой уровень риска, который еще можно считать допустимым.

Таким образом, в настоящей статье рассмотрены все основные аспекты проблемы информационной безопасности АСПД от основных принципов обеспечения информационной безопасности до вопросов разработки спецификаций профиля защиты и задания по безопасности.

При проектировании СЗИ АСПД необходимо все рассмотренные вопросы конкретизировать и координировать так, чтобы спроектированная СЗИ явилась целостной подсистемой АСПД.

Заключение. Поскольку проблема информационной безопасности далека от своего решения, она актуальна и в настоящее время. Решение проблемы ИБ, по всей видимости, будет развиваться последовательно — сначала в виде решения отдельных вопросов защиты информации конкретных автоматизированных систем, а затем в виде методов, обобщающих полученные конкретные результаты.

Наиболее остро стоит вопрос практической реализации СЗИ для конкретных систем. При этом СЗИ должна удовлетворять требованиям взаимодействия открытых систем для обеспечения гибкости СЗИ в условиях появления новых типов ЛА. Настоящая статья является попыткой акцентировать внимание проектировщиков СЗИ как подсистемы АСПД на ряд вопросов, которые необходимо решить в процессе ее проектирования.

К первому вопросу относится необходимость соблюдения двух основных принципов системного подхода: установление всех аспектов, относящихся к проблеме защиты информации АСПД, и оптимальное управление средствами обеспечения защиты информации АСПД.

Ко второму вопросу относится необходимость правильной разработки ПИБ в виде определенных формальных правил санкционированного доступа к защищаемой информации АСПД.

Третий вопрос связан с необходимостью разработать для АСПД спецификации ПЗ и ЗБ в соответствии с документом [6–8].

ЛИТЕРАТУРА

[1] Девянин П.Н. *Модели безопасности компьютерных систем. Управление доступом и информационными потоками*. Москва, Горячая линия-Телеком, 2013, 338 с.

[2] Грушо А.А., Тимонина Е.Е. *Теоретические основы защиты информации*. Москва, Яхтсмен, 1996, 188 с.

[3] Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. *Теория информационной безопасности и методология защиты информации*. 2-е изд., испр. и доп. Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, 2018, 100 с.

[4] Кияев В.И., Саитов А.В. *Комплексная информационная безопасность в управлении современным предприятием*. Санкт-Петербург, Санкт-Петербургский государственный экономический университет, 2016, 222 с.

[5] Крылов Г.О., Ларионова С.Л., Никитина В.Л. *Базовые понятия информационной безопасности*. Москва, Русайнс, 2017, 258 с.

[6] *ГОСТ Р ИСО/МЭК 15408-1–2012. Информационная технология* (*ИТ*). *Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель*. Москва, Стандартинформ, 2014, 50 с.

[7] *ГОСТ Р ИСО/МЭК 15408-2–2013. Информационная технология, методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности*. Москва, Стандартинформ, 2014, 155 с.

[8] *ГОСТ Р ИСО/МЭК 15408-3–2013. Информационная технология, методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности*. Москва, Стандартинформ, 2014, 144 с.

[9] Гатчин Ю.А., Климова Е.В. *Введение в комплексную защиту объектов информатизации*. Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, 2011, 112 с.

[10] Шаньгин В.Ф. *Комплексная защита информации в корпоративных системах*. Москва, Форум; ИНФРА-М, 2017, 592 с.

[11] Бондарев В.В. *Введение в информационную безопасность автоматизированных систем*. Москва, Изд-во МГТУ им. Н.Э. Баумана, 2016, 250 с.

[12] Дроботун Е.Б. *Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления*. Санкт-Петербург, Наукоемкие технологии, 2017, 120 с.

[13] Щербаков А.Ю. *Разрушающие программные воздействия*. Москва, Эдель, 1993, 64 с.

[14] Ухлинов Л.М., Сычев М.П., Скиба В.Ю., Казарин О.В. *Обеспечение безопасности информации в центрах управления полетами космических аппаратов*. Москва, Изд-во МГТУ им. Н.Э. Баумана, 2000, 366 с.

[15] Андреев А.Г., Казаков Г.В., Корянов В.В. Модель угроз информационной безопасности автоматизированной системы подготовки данных управления летательными аппаратами и модель защиты. *Известия высших учебных заведений. Машиностроение*, 2018, вып. 6, с. 86–95.
DOI: 10.18698/0536-1044-2018-6-86-95

[16] *ГОСТ Р 51583–2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.* Москва, Стандартинформ, 2015, 20 с.

[17] *ГОСТ Р 51624–2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.* Москва, Стандартинформ, 2001, 30 с.

[18] *Приказ ФСТЭК от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».*
URL: https://fstec.ru/index?id=868:prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения 05.07.2020).

[19] Андреев А.Г., Казаков Г.В., Корянов В.В. Метод оценки показателя достоверности выходных данных, подготавливаемых средствами автоматизированной системы подготовки данных полета летательных аппаратов. *Инженерный журнал: наука и инновации*, 2019, вып. 4.
http://dx.doi.org/10.18698/2308-6033-2019-4-1868

Статья поступила в редакцию 23.03.2020

Ссылку на статью просим оформлять следующим образом:

Андреев А.Г., Захаров В.Н., Казаков Г.В., Корянов В.В. Принципы организации защиты информации в автоматизированной системе подготовки данных полета летательных аппаратов. *Инженерный журнал: наука и инновации*, 2020, вып. 7. http://dx.doi.org/10.18698/2308-6033-2020-7-2000

Андреев Анатолий Георгиевич — канд. техн. наук, старший научный сотрудник ФГБУ «4 ЦНИИ» Минобороны России. e-mail: kgv.64@mail.ru

Захаров Владимир Николаевич — д-р техн. наук, профессор, главный научный сотрудник ФГБУ «4 ЦНИИ» Минобороны России. e-mail: kgv.64@mail.ru

Казаков Геннадий Викторович — канд. техн. наук, доцент, начальник управления ФГБУ «4 ЦНИИ» Минобороны России, почетный работник науки и техники Российской Федерации. e-mail: kgv.64@mail.ru

Корянов Всеволод Владимирович — канд. техн. наук, доцент, первый заместитель заведующего кафедрой «Динамика и управление полетом ракет и космических аппаратов» МГТУ им. Н.Э. Баумана. e-mail: vkoryanov@bmstu.ru

Principles of organization of information protection in automated system for aircraft flight data preparation

© A.G. Andreev[1], V.N. Zakharov[1], G.V. Kazakov[1], V.V. Koryanov[2]

[1]FSBI the 4th Central Research Institute of the Ministry of Defence of the Russian Federation, Korolyov town, Moscow region, 141091, Russia
[2]Bauman Moscow State Technical University, Moscow, 105005, Russia

When designing automated systems for aircraft flight data preparation, many practical problems are solved by introducing either insufficient protection means or their redundancy. Both situations create information security vulnerability. On the basis of a number of publications analysis it is concluded that the basics of information security theory are reduced to the formulation of the main axioms, with the implication that there is currently no complete theory of information security of computer systems. As a result there are many issues, including issues of general nature, requiring some elaboration. The article considers a set of issues related to ensuring information security of the automated system for aircraft flight data preparation. The nature of two basic principles of information protection organization in this system is unraveled. The first principle requires consideration of all aspects related to the problem of ensuring information security of the system, and the second — optimal control of means of information protection of the automated system of aircraft flight data preparation.

Keywords**:** *automated system, information security, approachability data, flight data, aircraft, data preparation, policy of information security*

REFERENCES

[1] Devyanin P.N. *Modeli bezopasnosti kompyuternykh sistem. Upravleniye dostupom i informatsionnymi potokami* [Models of Computer Systems Security. Access and information flow control]. Moscow, Goryachaya liniya-Telekom Publ., 2013, 338 p.

[2] Grusho A.A., Timonina E.E. *Teoreticheskie osnovy zashchity informatsii* [Fundamental theory of information security]. Moscow, Yakhtsmen Publ., 1996, 188 p.

[3] Gatchin Yu.A., Sukhostat V.V., Kurakin A.S., Donetskaya Yu.V. *Teoriya informatsionnoy bezopasnosti i metodologiya zashchity informatsii* [Information security theory and methodology of information protection]. St. Petersburg, University of Information Technology, Mechanics and Optics Publ., 2018, 100 p.

[4] Kiyaev V.I., Saitov A.V. *Kompleksnaya informatsionnaya bezopasnost v upravlenii sovremennym predpriyatiyem* [Comprehensive information security in the management of a modern enterprise]. St. Petersburg, St. Petersburg State Economic University, 2016, 222 p.

[5] Krylov G.O., Larionova S.L., Nikitina V.L. *Bazovye ponyatiya informatsionnoy bezopasnosti* [Basic Concepts of Information Security]. Moscow, RUSAYNS Publ., 2017, 258 p.

[6] *GOST R ISO/IEC 15408-1–2012. Informatsionnaya tekhnologiya (IT). Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologiy. Chast 1. Vvedeniye i obshchaya model* [State Standard R ISO/IEC 15408-1–2012. Information technology. Security techniques. Evaluation criteria for IT security. Part 1. Introduction and general model]. Moscow, Standartinform Publ., 2014.

[7] *GOST R ISO/IEC 15408-2–2013. Informatsionnaya tekhnologiya. metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti infor-*

matsionnykh tekhnologiy. Chast 2. Funktsionalnyye komponenty bezopasnosti [State Standard R ISO/IEC 15408-2–2013. Information technology. Security techniques. Evaluation criteria for IT security. Part 2. Security functional components]. Moscow, Standartinform Publ., 2014.

[8] *GOST R ISO/IEC 15408-3–2013. Informatsionnaya tekhnologiya. metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologiy. Chast 3. Komponenty doveriya k bezopasnosti* [State Standard R ISO/IEC 15408-3–2013. Information technology. Security techniques. Evaluation criteria for IT security. Part 3. Security assurance requirements]. Moscow, Standartinform Publ., 2014.

[9] Gatchin Yu.A., Klimova E.V. *Vvedenie v kompleksnuyu zashchitu obyektov informatizatsii* [Introduction to Comprehensive Protection of Informatization Objects]. St. Petersburg, University of Information Technology, Mechanics and Optics Publ., 2011, 112 p.

[10] Shangin V.F. *Kompleksnaya zashchita informatsii v korporativnykh sistemakh* [Comprehensive information protection in corporate systems]. Moscow, "FORUM"; INFRA-M Publ., 2017, 592 p.

[11] Bondaryev V.V. *Vvedeniye v informatsionnuyu bezopasnost avtomatizirovannykh sistem: uchebnoye posobiye* [Introduction to Information Security of Automated Systems: Tutorial]. Moscow, BMSTU Publ., 2016, 250 p.

[12] Drobotun E.B. *Teoreticheskiye osnovy postroyeniya sistem zashchity ot kompyuternykh atak dlya avtomatizirovannykh sistem upravleniya* [Basic theory of designing computer attack protection systems for automated control systems]. Monograph. St. Petersburg, Naukoyemkie tekhnologii Publ., 2017, 120 p.

[13] Scherbakov A. *Razrushayushchie programmnye vozdeystviya* [Destructive software effects]. Moscow, EDEL Publ., 1993, 64 p.

[14] Ukhlinov L.M., Sychev M.P., Skiba V.Y., Kazarin O.V. *Obespechenie bezopasnosti informatsii v tsentrakh upravleniya poletami kosmicheskikh apparatov* [Ensuring Information Security in Spacecraft Flight Control Centers]. Moscow, BMSTU Publ., 2000, 366 p.

[15] Andreev A.G., Kazakov G.V., Koryanov V.V. *Izvestiya vysshikh uchebnykh zavedeniy. Mashinostroenie — Proceedings of Higher Educational Institutions. Machine Building*, 2018, no. 6, pp. 86–95.
DOI: 10.18698/0536-1044-2018-6-86-95

[16] *GOST P 51583–2014. Zashchita informatsii. Poryadok sozdaniya avtomatizirovannykh sistem v zashchishchennom ispolnenii. Obshchiye polozheniya* [State Standard P 51583–2014. Information protection. Sequence of protected operational system formation. General provisions]. Moscow, Standartinform Publ., 2018.

[17] *GOST P 51624–2000. Zashchita informatsii. Avtomatizirovannyye sistemy v zashchishchennom ispolnenii. Obshchiye trebovaniya* [State Standard P 51624–2000. Protection of information. Protected automated systems. General requirements]. Moscow, Standartinform Publ., 2001, 30 p.

[18] *Prikaz Federalnoy sluzhby po tekhnicheskomu i eksportnomu kontrolyu ot 14 marta 2014 g. № 31* [Order of the Federal Service for Technical and Export Control dated March 14, 2014, no. 31]. "*Ob utverzhdenii trebovaniy k obespecheniyu zashchity informatsii v avtomatizirovannykh sistemakh upravleniya proizvodstvennymi i tekhnologicheskimi protsessami na kriticheski vazhnykh obyektakh, potentsialno opasnykh obyektakh, a takzhe obyektakh, predstavlyayushchikh povyshennuyu opasnost dlya zhizni i zdorovya lyudey i dlya okruzhayushchey prirodnoy sredy*" ["On approval of requirements for ensuring information security in automated control systems for production and technologi-

cal processes at critical facilities, potentially dangerous facilities, as well as facilities that pose an increased risk to life and human health and the environment"]. Available at: https://kkp.rk.gov.ru/uploads/kkp/attachments/d4/1d/8c/d98f00b204e9800998ecf8427e/phpwbcd3k_9.pdf

[19] Andreev A.G., Kazakov G.V., Koryanov V.V. *Inzhenernyy zhurnal: nauka i innovatsii — Engineering Journal: Science and Innovation*, 2019, iss. 4. http://dx.doi.org/10.18698/2308-6033-2019-4-1868

Andreev A.G., Cand. Sc. (Eng.), Senior Research Fellow, 4th Central Research Institute of the Ministry of Defence of the Russian Federation. Author of over 80 research publications in the field of reliability of automated control systems. e-mail: kgv.64@mail.ru

Zakharov V.N., Dr. Sc. (Eng.), Professor, Chief Researcher, 4th Central Research Institute of the Ministry of Defence of the Russian Federation. Author of over 150 research publications in the field of designing control systems. e-mail: kgv.64@mail.ru

Kazakov G.V., Cand. Sc. (Eng.), Assoc. Professor, Head of the Department, 4th Central Research Institute of the Ministry of Defence of the Russian Federation, Honorary Worker of Science and Technology of the Russian Federation. Author of over 80 research publications in the field of reliability of automated control systems. e-mail: kgv.64@mail.ru

Koryanov V.V., Cand. Sc. (Eng.), Assoc. Professor, First Deputy Head of the Department of Dynamics and flight control of rockets and spacecrafts, Bauman Moscow State Technical University. Author of over 40 research publications.
e-mail: vkoryanov@bmstu.ru