УДК 004.056.53 DOI: 10.18698/2308-6033-2021-7-2096

Методический подход к выявлению программных закладок в специальном программном обеспечении систем критических приложений

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

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

Рассмотрен методический подход к выявлению программных закладок в программном обеспечении систем критических приложений, который базируется на анализе предметной области, связанной с функционированием таких систем. Понятие программной закладки является локальным и зависит от системы, в которую ее внедряют. В связи с этим методический подход к выявлению программных закладок исследован на примере автоматизированной системы подготовки данных на полеты летательных аппаратов. В качестве программных закладок проанализировано вредоносное программное обеспечение, которое способно воздействовать на алгоритмы функционирования системы, нарушая штатный режим ее функционирования с нанесением весьма значительного ущерба целям применения системы. Определены действия для выявления вероятного места внедрения закладок, заключающиеся в раскрытии особенности оценки качества каждого из основных элементов системы и сущности программных закладок с учетом особенностей автоматизированной системы подготовки данных, описании системы с учетом ее особенностей, определении наиболее вероятного места внедрения программных закладок и условия их инициализации.

Ключевые слова: *автоматизированная система подготовки данных, данные достижимости, данные полета, летательный аппарат, недекларированные возможности, программная закладка*

Введение. Понятие надежности программного обеспечения (ПО) неотъемлемо связано с воздействием на него разного рода источников как случайных угроз (программные ошибки), так и источников преднамеренных угроз, которые могут быть внедрены в него на этапах разработки и эксплуатации. Среди множества типов преднамеренных угроз особое место занимают программные закладки (ПЗ). Следует отметить, что понятие ПЗ разными авторами трактуется поразному. Так, в [1] этот термин трактуется как ситуация, которая несколько отличается от ранее использованной в литературе [2–5], где словосочетание *программная закладка* связано с процессом разработки исходных текстов программ с созданием ПЗ: логическая бомба, логический люк, троянский конь. Автор [1] утверждает, что особенностью закладок может быть то, что они фактически неотделимы от прикладных или системных программ, если внедрены в них на стадии разработки или путем обратного проектирования, далее рассмотрены только программы с потенциально опасными последствиями

для работы. Это уже любые источники преднамеренных угроз в виде программных вирусов, программных червей, эксплойтов и т. п. Семантика понятия ПЗ — локальная, зависящая от системы, в которую она внедряется. В связи с этим методический подход к выявлению ПЗ рассмотрен на примере автоматизированной системы подготовки данных на пуски летательных аппаратов (АСПД).

В качестве ПЗ рассматривается такое вредоносное ПО, которое способно воздействовать на алгоритмы функционирования АСПД, нарушая штатный режим ее функционирования с нанесением значительного ущерба целям применения системы.

Цель настоящей статьи — разработать методический подход к выявлению ПЗ в специальном программном обеспечении систем критических приложений на базе анализа предметной области, связанной с функционированием таких систем.

Системы, подверженные внедрению программных закладок. Существует достаточно большой класс автоматизированных систем критических приложений (или систем с потенциально опасными последствиями), нарушение штатного безопасного процесса функционирования которых чревато большими негативными или даже катастрофическими последствиями для государства. К таким системам управления (СУ) относятся следующие:

– СУ экологически опасными производствами, атомными электростанциями, транспортной системой, финансовой системой, персональными данными;

– СУ объектами по ликвидации чрезвычайных ситуаций;

– СУ объектами оборонного назначения.

Объектом управления последних двух систем является группировка летательных аппаратов (ГЛА), включающая подразделения летательных аппаратов (ЛА) с различным назначением.

Чем важнее автоматизированная система, тем большее число различных источников угроз может на нее воздействовать, нанося разного уровня ущерб целям ее функционирования. Наиболее значительный ущерб могут нанести системе ПЗ вредоносного ПО [6–9] (атака на ПАО «Газпром», Игналинскую атомную электростанцию и др.). В настоящей статье в качестве примера рассмотрена АСПД, которая относится к классу систем с потенциально опасными последствиями.

Для определения вероятного места внедрения ПЗ необходимо выполнить следующие действия.

Раскрыть особенность оценки качества каждого из основных элементов АСПД. Основной элемент АСПД — специальное (прикладное) программное обеспечение (СПО), поскольку оно реализует алгоритмы функционирования системы в соответствии с ее назначением.

Обычно СПО АСПД принимают в эксплуатацию, если по результатам его тестирования на достаточном объеме репрезентативных входных данных из некоторой допустимой области $X_{\text{доп}}$ определяют показатель его надежности $R_{\text{н}}$:

$$R_{\text{н}} \geq R_{\text{н}}^{\text{тр}}, \qquad (1)$$

где $R_{\text{н}}^{\text{тр}}$ — требуемое значение показателя надежности СПО АСПД.

Такая оценка показателя надежности СПО АСПД справедлива только при учете наличия в СПО источников случайных угроз в виде программных ошибок, допущенных в процессе его разработки.

Возможны проверки СПО на наличие в нем так называемых недекларированных возможностей (НДВ), т. е. диагностика отсутствия таких функций, выполняемых СПО, которые не представлены в документации на него. Если СПО не содержит НДВ и выполнено условие (1), можно утверждать, что СПО отвечает заданному качеству и принимается в эксплуатацию.

Однако для систем критических приложений, к классу которых относится и АСПД, такой подход неприемлем, поскольку можно считать, что имеющаяся ПЗ в СПО также относится к НДВ, но для ее выявления нужны специальные меры.

Следовательно, оценка показателя надежности СПО АСПД только по результатам его тестирования на репрезентативной выборке вариантов входных данных из допустимой области $X_{\text{доп}}$ без проверки наличия ПЗ в ее СПО не является корректной. Таким образом, качество СПО как основного элемента АСПД можно оценить двумя показателями:

1) надежностью СПО в виде вероятности проявления программной ошибки в процессе его эксплуатации;

2) наличием в СПО ПЗ, который уже не имеет вероятностной меры, а определяется только признаковой информацией 1 (да) или 0 (нет).

Более того, нельзя указать степень уверенности — 1 или 0. Задача обнаружения указанного вида ПЗ в литературе по теории безопасности систем критических приложений еще не рассматривалась, поэтому на настоящем этапе можно только сформулировать подход к решению поставленной задачи.

Предметная область исследований. Следующим действием определения вероятного места внедрения ПЗ является описание АСПД с учетом ее особенностей.

Полет ГЛА и отдельных ее подразделений производится согласно плану полетов группировки ЛА (ППГЛА), который разрабатывается автоматизированной системой планирования полетов ГЛА. Данные для СУ ЛА готовятся средствами АСПД, особенность которой состоит в подготовке двух видов данных:

1) данных достижимости (ДД) — массив данных, содержащий координаты пунктов прибытия для каждого ЛА, определяемые из энергетических возможностей (запасов топлива) данного ЛА;

2) данных на полеты ЛА (ДПЛА) — массив данных, которые вводятся в СУ ЛА и входят в состав формируемых ею управляющих сигналов, обеспечивающих заданную точность прилета ЛА в запланированный, согласно ППГЛА, пункт прибытия с учетом ограничений, накладываемых на инерционно-массовые и конструктивные характеристики ЛА, а также на параметры СУ ЛА.

Структура массива ДД представляет собой кортеж вида

$$\text{ДД} = \langle SI_1, D, SI_2 \rangle,$$

где SI_1 — служебная информация начала массива ДД; D — данные, определяющие задачу ЛА согласно ППГЛА с координатами пункта прибытия; SI_2 — служебная информация конца массива ДД.

Структура ДПЛА представляет собой кортеж вида

$$\text{ДДЛА} = \langle SI_3, D, U, SI_4 \rangle,$$

где SI_3 — служебная информация начала массива ДПЛА; U — установки ДПЛА, в соответствии с которыми формируется управляющее воздействие СУ ЛА; SI_4 — служебная информация конца массива ДПЛА.

С учетом указанной особенности общая схема АСПД представлена на рис. 1. Видно, что подготовку ДПЛА и управляемый полет ЛА до пункта прибытия обеспечивают три системы: автоматизированная система планирования полетов ГЛА, АСПД, СУ ЛА.

В АСПД входят следующие элементы:

– база данных (БД);

– управляющий программный комплекс (УПК);

– специальное (прикладное) программное обеспечение формирования ДД (СПО ФДД).

Особенность АСПД состоит в том, что она подготавливает ДД с использованием СПО контроля их реализуемости (СПО КРДД), по которым в наземном цифровом вычислительном комплексе (НЦВК) рассчитывают и проверяют на реализуемость ДПЛА, поступающие далее в СУ ЛА для формирования управляющего сигнала. Основным свойством ДД и ДПЛА является их реализуемость (семантическая правильность).

Данные ДД и ДПЛА — реализуемые, если их использование в СУ ЛА не приведет к срыву выполнения поставленной в ППГЛА задачи по доставке груза в заданный пункт прибытия.

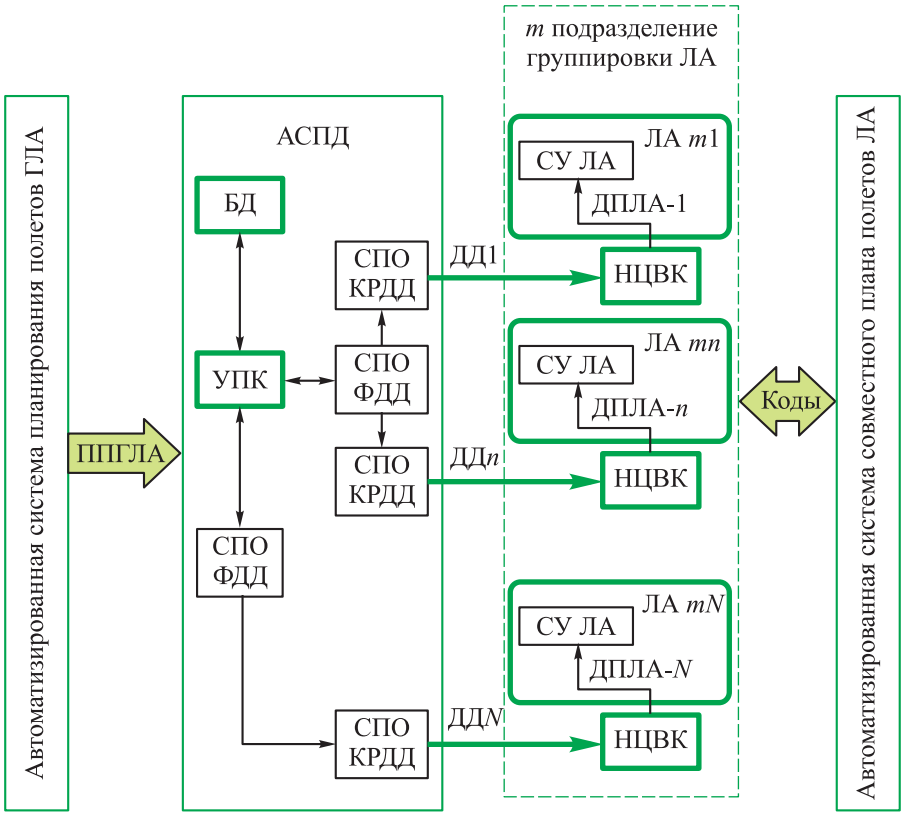

Рис. 1. Схема подготовки данных полета ЛА для *m*-го подразделения ГЛА

От семантической правильности ДД и ДПЛА напрямую зависит выполнение группировкой ЛА поставленной в ППГЛА задачи по доставке грузов в заданные пункты прибытия с заданной точностью и учетом определенных ограничений. Раскроем физическую суть рассматриваемой задачи более подробно.

Суть задачи повышения надежности специального программного обеспечения контроля реализуемости данных достижимости. Для определения вероятного места внедрения ПЗ необходимо раскрыть сущность этой закладки с учетом особенностей АСПД.

Поскольку качество АСПД в значительной мере зависит от степени ее информационной безопасности [10], то при разработке адекватных средств защиты информации АСПД следует учитывать особенности источников преднамеренных угроз. Первичный источник преднамеренной угрозы — злоумышленник, который внедряет либо ПЗ, либо другое вредоносное ПО (программный вирус, троянского коня, программного червя и т. п.) в СПО АСПД. Такая закладка становится (вторичным) источником преднамеренной угрозы. Если злоумышленник обладает высокой квалификацией, то внедренная им ПЗ будет снабжена средствами маскировки, благодаря которым ее будет

невозможно обнаружить простыми антивирусными средствами. Опасность вторичного источника заключается в том, что он всегда реализует угрозу с нанесением максимального ущерба целям применения АСПД, если его не обнаружить и не нейтрализовать. В связи с этим для преднамеренных угроз понятие вероятности проявления угрозы отсутствует, следовательно, о показателе надежности ПО, подверженного воздействиям источника преднамеренной угрозы, также говорить не совсем корректно. Итак, можно наблюдать некое противоречие:

– присутствует довольно обширный класс систем критических приложений, для которых весьма актуальной и важной задачей является защита от источников преднамеренных угроз, внедряемых на этапе разработки СПО;

– не существует общего метода обнаружения и нейтрализации ПЗ.

Для обнаружения ПЗ нецелесообразно увеличивать объем тестирования. Можно протестировать СПО АСПД по допустимой области входных данных и обнаружить все случайные ошибки кодирования, но ПЗ не будет обнаружена. Это связано с тем, что ПЗ инициализируется и проявляется по другому принципу. Она инициализируется при выполнении некоторого множества условий $U = (u_1, u_n, \ldots, u_N)$, известных только злоумышленнику.

Схема инициализации ПЗ представлена на рис. 2. Если условия U не выполнены, то ПЗ не инициализируется (рис. 2, *а*); если условия соблюдены и проведены, то ПЗ перехватывает управление процессом подготовки ДПЛА (рис. 2, *б*) на себя и дальнейшая их подготовка происходит по алгоритмам ПЗ.

Исходя из сущности ПЗ, необходимо определить прогнозное множество условий инициализации ПЗ U. Без определения этого множества невозможно обнаружить внедренную ПЗ. Поэтому требуется выполнить задачу по определению возможных целей злоумышленника. Для ее решения учитывают все возможные разрушающие информационные воздействия (РИВ): искажение (И), уничтожение (У), подмена (П), раскрытие (Р), блокировка (Б).

Определим наиболее опасные РИВ, используя метод анализа иерархий и рассчитав собственный вектор $\boldsymbol{W}_{\text{РИВ}}$ матрицы $\text{М}_{\text{РИВ}}$ парных сравнений указанных РИВ по признаку уровня их опасности.

Наиболее опасный РИВ — подмена ДПЛА, наименее опасный — ПЗ, отсылающая злоумышленнику закрытую информацию. Очевидно, что в момент выполнения ГЛА поставленной задачи раскрытие конфиденциальной информации особого смысла не имеет и его можно не учитывать. Оставшиеся четыре РИВ расположим в убывающем порядке: П → И → У → Б.

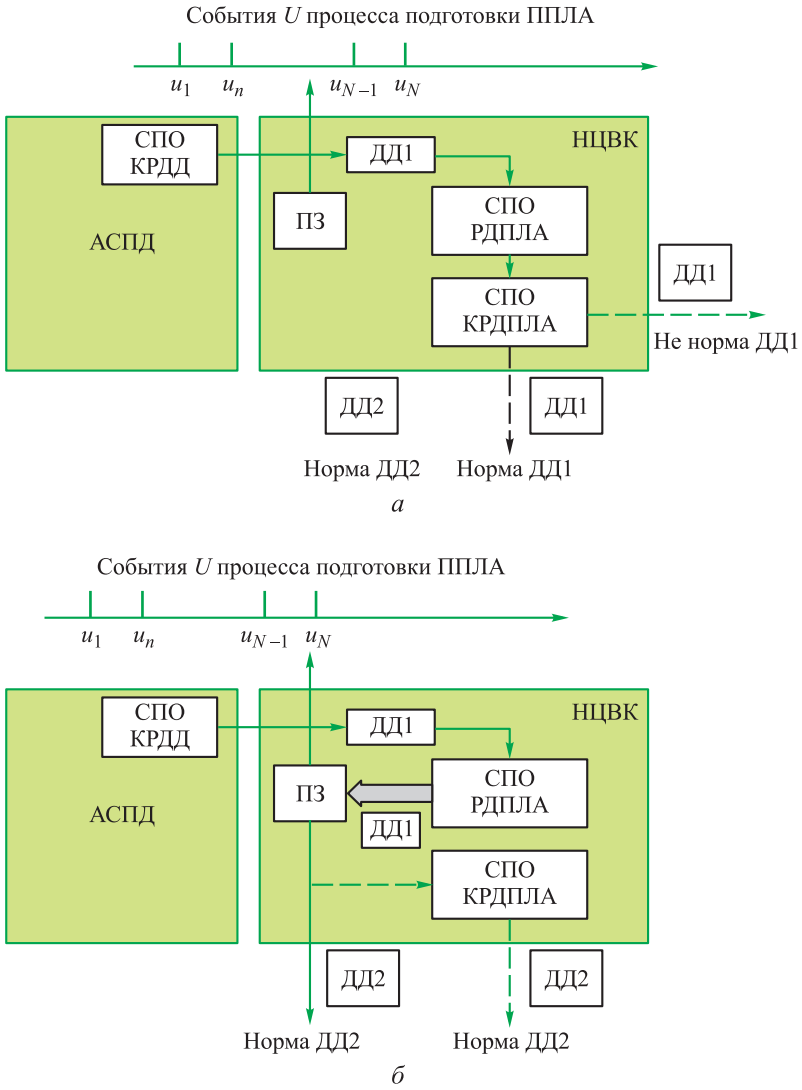

Рис. 2. Действие программной закладки, находящейся в НЦВК:
а — $U \not\subset U_N$; *б* — $U_N \subseteq U$

Определение места внедрения программной закладки в автоматизированную систему подготовки данных. В целях обнаружения вероятного места внедрения ПЗ необходимо определить наиболее вероятное место внедрения и условия инициализации закладки.

Специфика АСПД состоит в том, что она подготавливает данные для управления автоматическим объектом, например ЛА, не позволяющим проводить натурные испытания его СПО, т. е. осуществлять реальные полеты ЛА и фиксировать результаты функционирования СПО КРДД с последующим устранением причин обнаруженных ошибок.

Особенность СУ заключается в том, что реализуемость подготавливаемых ею ДД зависит от реализуемости ДПЛА, подготавливаемых НЦВК ЛА, не входящим в состав АСПД. Тогда для контроля реализуемости ДД требуется иметь модель НЦВК, поскольку именно ДПЛА определяют качество полета ЛА и выполнение им поставленной в ППГЛА задачи.

Для проверки качества СПО КРДД важно создать программный моделирующий комплекс (ПМК), который моделировал бы реальный полет ЛА. Общая структура такой АСПД показана на рис. 3. Рассмотрим процесс подготовки ДД*. Сначала средствами СПО ФДД и СПО КРДД подготавливаются ДД, затем эти данные поступают в ПМК, и в случае нормы ||н|| контроля реализуемости они возвращаются в БД АСПД, а в случае ненормы ||нн|| контроля реализуемости они поступают в группу анализа («Анализ») для выявления и устранения причин ненормы контроля ДД. Если группа «Анализ» не сможет скорректировать ДД так, чтобы они были реализуемыми, то они отсылаются в автоматизированную систему планирования полетов ГЛА, в которой проводится выявление и анализ причин нереализуемости ДД и их корректировка (возможно для всего подразделения ГЛА). В результате будут получены реализуемые ДД, которые опять проходят все стадии: формирования (СПО ФДД), контроля (СПО КРДД) и расчета и контроля ДПЛА (ПМК). Эти ДД помечаются звездочкой ДД*. Точно такая же процедура имеет место, если ненорму контроля ||нн|| выдаст ПМК.

При реальном полете ГЛА скорректированные ДД вновь поступают в СПО КРДД, а затем в НЦВК, где будет признак нормы ||н|| контроля, и они поступят в СУ ЛА.

В целях разработки первого вида средств решения указанной проблемы обратимся к некоторым результатам работы [11], в которой рассмотрены основные вопросы построения адекватной модели контроля реализуемости ДПЛА и показана целесообразность представления данных управления полетом летательных аппаратов двумя видами данных: ДД и ДПЛА.

Должна быть построена модель реализуемости для каждого из этих видов данных с учетом всех необходимых факторов и ограничений реального полета ЛА, контроль которых обеспечит адекватность построенной на их основе модели полета ЛА.

Для определения места внедрения ПЗ удобно использовать специальную формальную схему процесса подготовки ДПЛА (рис. 4).

Схема (см. рис. 4) используется для размещения ПЗ последовательно с различными воздействиями РИВ в разные места схемы с последующим анализом реальности исполнения того или иного варианта ПЗ и ее топологии. Очевидно, что ПЗ с РИВ раскрытие в данном случае не будет использовано.

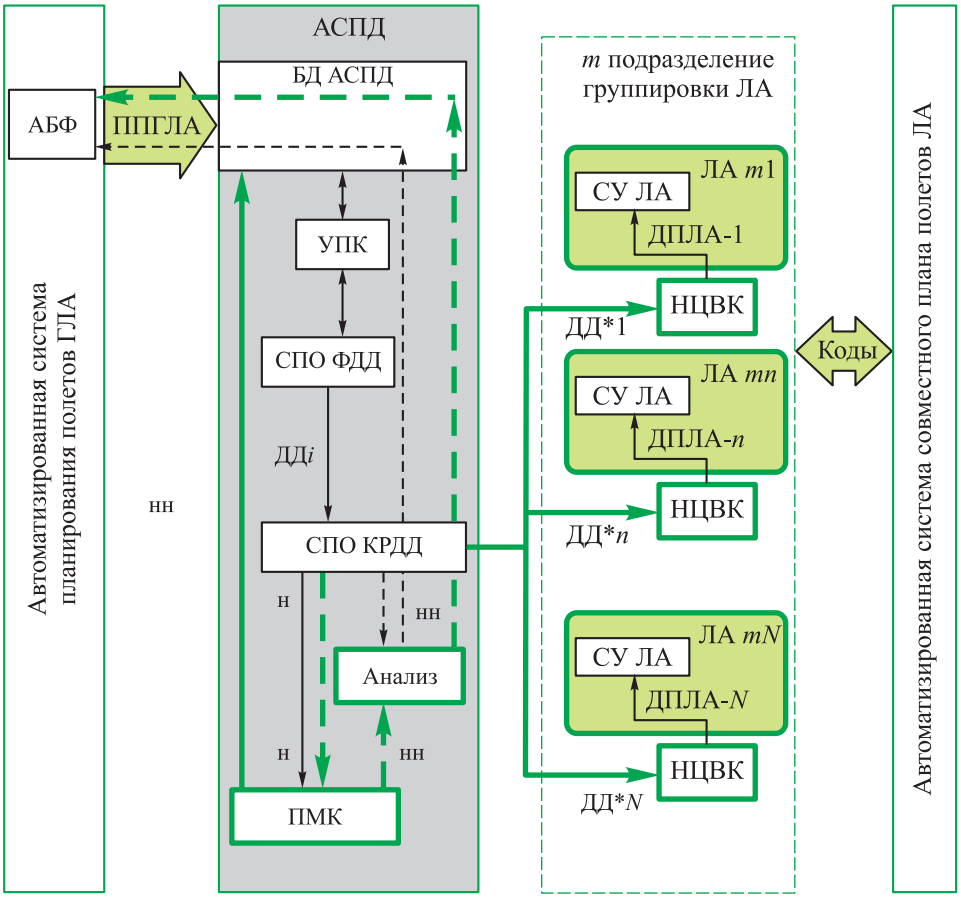

Рис. 3. Схема АСПД с использованием ПМК

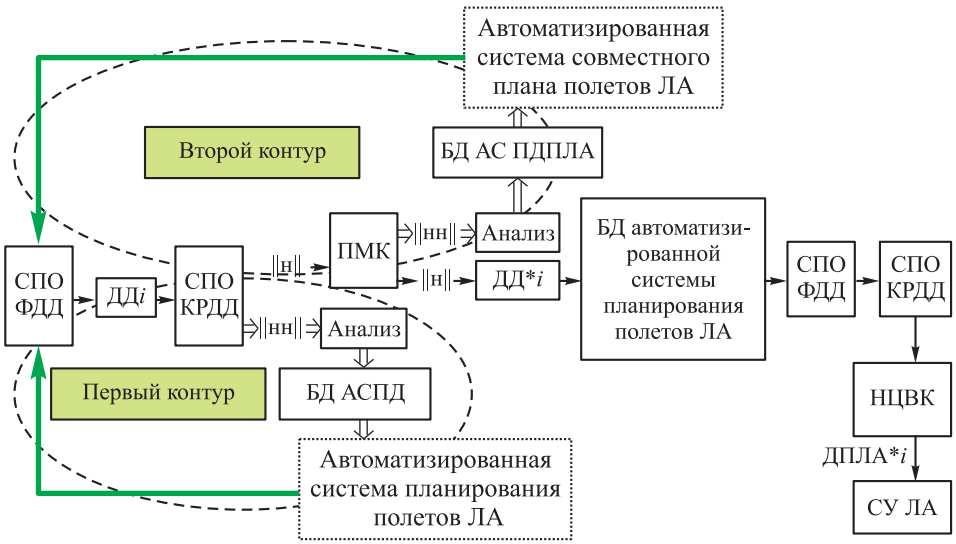

Рис. 4. Формальная схема процесса подготовки ДПЛА

Далее необходимо конкретизировать структуру ПМК и расширить ее включением модели предстартовой подготовки ЛА. Поскольку предстартовая подготовки ЛА всегда используется в реальном полете ЛА, она может содержать непустое U_1 подмножество множества U ($U_1 \subseteq U$). Эта модель представлена на рис. 5.

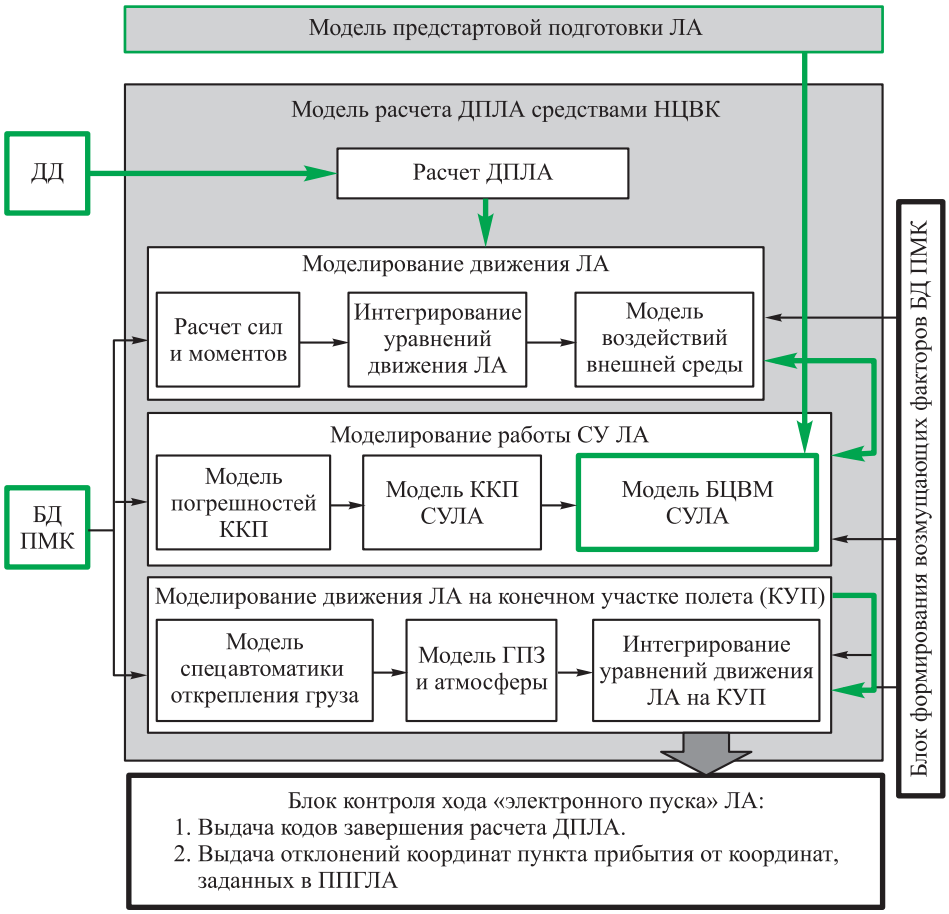

Рис. 5. Общая структура ПМК:
ККП — комплекс командных приборов; БЦВМ — бортовая цифровая вычислительная машина

В ПМК должны быть учтены основные уравнения, характерные для любого типа ЛА, к которым относятся уравнения движения аппарата, выражения, учитывающие гравитационное поле Земли и атмосферу [11, 12].

Внедряя ПЗ в СПО АСПД, злоумышленник учитывает реальную ситуацию, связанную с подготовкой и полетом ЛА. Поэтому, создавая модель ПМК, следует иметь в виду реальные события, которые отражаются в НЦВК. Такой ситуацией, например, является факт

отключения наземного оборудования от ЛА. Следовательно, в состав модели ПМК должен быть включен процесс наземной подготовки ЛА к пуску (см. рис. 5).

Заключение. Сложная задача обнаружения ПЗ, воздействия которой способны изменить траекторию полета ЛА, базируется на описании предметной области функционирования АСПД, в котором необходимо использовать принцип от общего к частному, что позволит не упустить основные цели решаемой задачи для АСПД за счет рассмотрения множества частных вопросов:

– раскрыть особенности оценки качества СПО КРДД;

– описать предметную область АСПД с учетом ее особенностей;

– раскрыть сущности ПЗ с учетом особенностей АСПД;

– определить наиболее вероятное место внедрения и условия инициализации ПЗ.

В дальнейших исследованиях необходимо решить частные вопросы, связанные с более подробным описанием предметной области на уровне модульной структуры СПО КРДД, вплоть до исходных текстов программ, что позволит точно и достоверно выявить возможные места внедрения ПЗ.

ЛИТЕРАТУРА

[1] Казарин О.В. *Безопасность программного обеспечения компьютерных систем*. Москва, МГУЛ, 2003, 212 с.

[2] Гроувер Д., Сатер Р., Фипс Дж., Девис Д., Паркин Г., Уихман Б., Самосуик М., Харт Р., Картрайт Дж., Элсом С. *Защита программного обеспечения*. Москва, Мир, 1992, 120 с.

[3] Наумов А.А., Айдинян А.Р. Надежность программного обеспечения и методы ее повышения. *Инженерный вестник Дона*, 2018, № 2. URL: http://www.ivdon.ru/ru/magazine/archive/N2y2018/4946

[4] Липаев В.В. *Надежность и функциональная безопасность комплексов программ реального времени*. Саратов, Вузовское образование, 2015, 207 с.

[5] Андреев А.Г., Казаков Г.В., Корянов В.В. Метод оценки показателя надежности программного обеспечения автоматизированной системы подготовки данных управления летательными аппаратами. *Инженерный журнал: наука и инновации*, 2018, вып. 6. http://dx.doi.org/10.18698/2308-6033-2018-6-1771

[6] Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак. *Труды СПИИРАН*, 2016, № 2, с. 207–244. DOI: 10.15622/sp.45.13

[7] Булдакова Т.И., Джалолов А.Ш. Выбор технологий Data Mining для систем обнаружения вторжений в корпоративную сеть. *Инженерный журнал: наука и инновации*, 2013, вып. 11. http://dx.doi.org/10.18698/2308-6033-2013-11-987

[8] 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, № 6, с. 86–95.

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

[10] Андреев А.Г., Казаков Г.В. Метод оценки показателя информационной безопасности автоматизированной системы подготовки данных применения ракет. *Труды 4 ЦНИИ Минобороны России*, № 150, т. 1, ч. 3. Королев, 2019, с. 84–88.

[11] Андреев А.Г., Казаков Г.В., Соловьев Ю.С. Построение адекватной модели контроля реализуемости данных управления полетом летательных аппаратов. *Известия ВА РВСН имени Петра Великого*, 2018, № 280, с. 26–38.

[12] Сихарулидзе Ю.Г. *Баллистика и наведение летательных аппаратов*. Москва, Лаборатория знаний, 2020, 410 с.

Статья поступила в редакцию 21.06.2021

Ссылку на эту статью просим оформлять следующим образом:

Андреев А.Г., Казаков Г.В., Корянов В.В. Методический подход к выявлению программных закладок в специальном программном обеспечении систем критических приложений. *Инженерный журнал: наука и инновации*, 2021, вып. 7. http://dx.doi.org/10.18698/2308-6033-2021-7-2096

Андреев Анатолий Георгиевич — канд. техн. наук, старший научный сотрудник ФГБУ «4 ЦНИИ» Минобороны России. Автор более 80 работ в области надежности автоматизированных систем управления. 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. Автор более 80 работ в области надежности автоматизированных систем управления. 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. Автор более 170 публикаций.
e-mail: vkoryanov@bmstu.ru

Methodological approach to identifying software bugs in special software for systems of critical applications

© A.G. Andreev[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, Moscow region, 141091, Russia
[2]Bauman Moscow State Technical University, Moscow, 105005, Russia

The paper focuses on a methodological approach to identifying software in special software for systems of critical applications. The approach relies on the analysis of the subject area associated with the functioning of such systems. The term 'software bugs' is local and depends on the system into which they are embedded. In this regard, the methodological approach to identifying software bugs is illustrated by an automated system for preparing data for aircraft flights. By software bugs, we mean malicious software that can affect the algorithms for the functioning of the system, disrupting the normal mode of its operation and causing significant damage to the goals of the system. To find where software bugs are likely to be embedded, we specified actions which consist in understanding the features of assessing the quality of each of the main elements of the system and the essence of software bugs, with account for the features of the automated data preparation system; describing the system and its specifics; determining the most likely place for embedding software bugs and conditions for their initialization.

Keywords: *automated data preparation system, reachability data, flight data, aircraft, undeclared capabilities, software bug*

REFERENCES

[1] Kazarin O.V. *Bezopasnost programmnogo obespecheniya kompyuternykh sistem* [Computer systems software security]. Monograph. Moscow, BMSTU Mytischi Branch Publ., 2003, 212 p.

[2] Grover D., ed. *The Protection of Computer Software — its Technology and Applications*. Cambridge University Press, 1989. [In Russ.: Grover D., et al. Zaschita programmnogo obespecheniya. Moscow, Mir Publ., 1992, 120 p.].

[3] Naumov A.A., Aidinyan A.R. *Inzhenerny vestnik Dona — Engineering journal of Don,* 2018, no. 2. Available at: http://www.ivdon.ru/ru/magazine/archive/N2y2018/4946

[4] Lipaev V.V. *Nadezhnost i funktsionalnaya bezopasnost kompleksov programm realnogo vremeni* [Reliability and functional safety of real-time software complexes]. Saratov, Vuzovskoe obrazovanie Publ., 2015, 207 p.

[5] Andreev A.G., Kazakov G.V., Koryanov V.V. *Inzhenerny zhurnal: nauka i innovatsii — Engineering Journal: Science and Innovation*, 2018, iss. 6. http://dx.doi.org/10.18698/2308-6033-2018-6-1771

[6] Branitskiy A.A., Kotenko I.V. *Trudy SPIIRAN — SPIIRAS Proceedings*, 2016, no. 2, pp. 207–244. https://doi.org/10.15622/sp.45.13

[7] Buldakova T.I., Dzhalolov A.Sh. *Inzhenerny zhurnal: nauka i innovatsii — Engineering Journal: Science and Innovation*, 2013, iss. 11. http://dx.doi.org/10.18698/2308-6033-2013-11-987

[8] Andreev A.G., Kazakov G.V., Koryanov V.V. *Izvestiya vysshikh uchebnykh zavedeniy. Mashinostroenie — BMSTU Journal of Mechanical Engineering,* 2018, no. 6, pp. 86–95.

[9] Drobotun E.B. *Teoreticheskie osnovy postroeniya sistem zaschity ot kompyuternykh atak dlya avtomatizirovannykh sistem upravleniya* [Theoretical foundations of building protection systems against computer attacks for automated control systems]. Monograph. St. Peterburg, Naukoemkie tekhnologii Publ., 2017, 120 p.

[10] Andreev A.G., Kazakov G.V. *Trudy 4 TsNII Minoborony Rossii (Proceedings of the 4th Central Research Institute of the Ministry of Defence of the Russian Federation)*, no. 150, vol. 1, part 3. Korolyov, 2019, pp. 84–88.

[11] Andreev A.G., Kazakov G.V., Solovev Yu.S. *Izvestiya VA RVSN imeni Petra Velikogo (Proceedings of the Peter the Great Military Academy of Strategic Rocket Troops)*, 2018, no. 280, pp. 26–38.

[12] Sikharulidze Yu.G. *Ballistika i navedenie letatelnykh apparatov* [Aircraft ballistics and guidance]. 4th ed., enl. Moscow, Laboratoriya znaniy Publ., 2020, 410 p.

Andreev A.G. (b. 1941), Cand. Sc. (Eng.), Senior Research Fellow, FSBI "The 4th Central Research Institute of the Ministry of Defence of the Russian Federation"; Author of over 80 works in the field of automated control system reliability.
e-mail: kgv.64@mail.ru

Kazakov G.V. (b. 1964), Cand. Sc. (Eng.), Assoc. Professor, Head of the FSBI "The 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 works in the field of automated control system reliability. e-mail: kgv.64@mail.ru
SPIN-code: 8553-9753

Koryanov V.V. (b. 1982) graduated from Bauman Moscow State Technical University in 2006; Cand. Sc. (Eng.), Assoc. Professor, First Deputy Head of the Department of Dynamics and Flight Control of Rockets and Spacecraft; Author of over 170 works in the field of ballistics modelling and dynamics of spacecraft and descent vehicle motion.
e-mail: vkoryanov@bmstu.ru