ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 72118— 2025

Защита информации

СИСТЕМЫ С КОНСТРУКТИВНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Методология разработки

Издание официальное

Москва
Российский институт стандартизации
2025

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»), Акционерным обществом «Лаборатория Касперского» (АО «Лаборатория Касперского»), Федеральным государственным бюджетным учреждением науки «Институт системного программирования им. В.П. Иванникова Российской академии наук» (ИСП РАН)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 6 июня 2025 г. № 539-ст

4 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Оформление. ФГБУ «Институт стандартизации», 2025

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Сокращения и обозначения 4
5 Общие положения 5
6 Реализация подходов к созданию систем с конструктивной информационной безопасностью 9
7 Содержание основных работ при создании систем с конструктивной информационной безопасностью 12
8 Документирование конструктивных подходов к обеспечению информационной безопасности 18
9 Применение шаблонов проектирования и разработки при создании систем с конструктивной информационной безопасностью 19
Приложение А (рекомендуемое) Примеры типовых шаблонов проектирования программного обеспечения, обладающего свойствами конструктивной информационной безопасности 21

Введение

Состояние современной индустрии разработки компьютеризированных систем, в том числе автоматизированных систем, информационных систем, информационно-управляющих систем, программно-аппаратных комплексов, прикладного программного обеспечения (ПО), программных платформ и компонентов (далее — системы), характеризуется недостаточным учетом вопросов обеспечения безопасности информации, информационных технологий и информационной инфраструктуры на ранних этапах жизненного цикла систем. Как результат соответствующие требования не имеют должного приоритета и часто определяются только после проектирования функциональной составляющей системы.

Вместе с тем данный пробел будет восполнен, если требования по обеспечению безопасности информации будут определены и сформулированы на этапе замысла системы, а реализованы на уровне конструктивных решений при проектировании и создании системы, то есть такие требования будут учитываться и прорабатываться в ходе всего жизненного цикла. Это позволит сократить количество потенциальных уязвимостей в архитектуре, коде и конфигурации систем, а также оптимизировать применение средств защиты информации. Таким образом, информационная безопасность, реализуемая на уровне конструктивных решений (конструктивная информационная безопасность), вероятно, позволит уменьшить избыточную функциональную и архитектурную сложность, а также эксплуатационные затраты, направленные на обеспечение защищенности соответствующих систем, в частности, за счет снижения вероятности появления уязвимостей, в том числе в программном обеспечении. При этом нужно отметить, что именно с факторами избыточной сложности связано существенное число ошибок в реализации системами информационных технологий, телекоммуникационных технологий и технологий управления, что подтверждает актуальность стандартизации конструктивной информационной безопасности.

Вместе с тем для обеспечения штатной работы систем (выполнения ими своих целевых функций) реализация требований безопасности информации должна быть согласована (синхронизирована) с реализацией основного функционала соответствующих систем на всех этапах их жизненного цикла. Целью настоящего стандарта является определение и описание содержания работ, необходимых для такой синхронизации при создании систем с конструктивной информационной безопасностью.

Процесс создания систем, в ходе которого обеспечивается учет опыта блокирования и исправления известных (типовых) уязвимостей и ошибок, а также минимизация числа потенциальных (новых, неизвестных) уязвимостей и ошибок, упрощается за счет формирования и использования шаблонов проектирования и разработки. Обеспечение конструктивной информационной безопасности может опираться на использование таких шаблонов, описание которых, а также принципов их формирования и применения содержится в настоящем стандарте.

С учетом изложенного конструктивная информационная безопасность может быть реализована в создаваемых системах и/или системах, для которых запланирована глубокая модернизация с полной заменой оборудования, где использование наложенных (внешних и (или) встраиваемых) средств защиты затруднено и (или) невозможно. В качестве примера можно привести системы, включающие малоресурсные устройства (в том числе многие устройства «Интернета вещей/Промышленного интернета вещей» — IoT/IIoT), применяемые для промышленной автоматизации, информатизации транспортных средств и других областей жизнедеятельности. Такие устройства должны разрабатываться как системы с конструктивной информационной безопасностью. Таким образом, данный подход может применяться для создания доверенных систем, в которых существует возможность подтверждения доверия.

Примечание — Малоресурсное устройство — это устройство (программно-аппаратный комплекс) с малыми объемами оперативной и долговременной памяти, невысокой (относительно низкой) производительностью и предназначенное (оптимизированное) для выполнения конкретной задачи (программы), например управления технологическим процессом (транспортным объектом, станком, механизмом и т. д.), сбора и передачи данных и т. д. На таком устройстве затруднены или невозможны установка и работа любого другого ПО, за исключением ПО, предназначенного для выполнения основной целевой функции (функции назначения) данного устройства.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

СИСТЕМЫ С КОНСТРУКТИВНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Методология разработки

Information protection. Systems secure by design.
Development methodology

Дата введения — 2025—12—01

1 Область применения

Настоящий стандарт распространяется на создаваемые системы, реализующие информационную технологию, а также осуществляющие с помощью информационной технологии контроль и управление различными процессами (информационными, телекоммуникационными, технологическими, производственными), и устанавливает требования и рекомендации для методологии разработки таких систем, обеспечивающие реализацию конструктивных подходов к информационной безопасности. Также данный стандарт может быть применен для обеспечения информационной безопасности систем, для которых запланирована глубокая модернизация с полной заменой оборудования, где использование наложенных (внешних и (или) встраиваемых) средств защиты затруднено и (или) невозможно.

Положения настоящего стандарта предназначены для заказчиков и разработчиков систем, реализующих информационную технологию. Положения стандарта содержат методологию разработки системы с конструктивной информационной безопасностью (далее — СКИБ) и дополняют положения комплексов стандартов «Информационная технология. Системная и программная инженерия» и «Защита информации. Разработка безопасного программного обеспечения». Также настоящий стандарт предназначен для организаций, проводящих оценку соответствия систем с конструктивной информационной безопасностью его положениям.

Примечание — Настоящий стандарт может использоваться для создания автоматизированных систем в защищенном исполнении. Тем не менее не во всех автоматизированных системах в защищенном исполнении (АСЗИ) реализована конструктивная информационная безопасность.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ ISO/IEC TS 19249 Информационные технологии. Методы и средства обеспечения безопасности. Каталог принципов построения архитектуры и проектирования безопасных продуктов, систем и приложений

ГОСТ Р 51583 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения

ГОСТ Р 53114 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

ГОСТ Р 56939 Защита информации. Разработка безопасного программного обеспечения. Общие требования

ГОСТ Р 57193 Системная и программная инженерия. Процессы жизненного цикла систем

Издание официальное

ГОСТ Р 71304 Системная и программная инженерия. Гарантии обеспечения качества систем и программных средств. Общие положения

ГОСТ Р ИСО/МЭК 12207 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 53114, ГОСТ Р 56939, ГОСТ Р 57193, а также следующие термины с соответствующими определениями:

3.1

система: Комбинация взаимодействующих элементов, организованных для достижения одной или нескольких поставленных целей.

[ГОСТ Р 57193—2016, пункт 4.1.44]

Примечание — По тексту настоящего стандарта сеть является видом системы. Также в тексте настоящего стандарта понятия «система» и «сеть» могут использоваться совместно для большей наглядности.

3.2

системный элемент: Представитель совокупности элементов, образующих систему.

Примечание — Системный элемент является отдельной частью системы, которая может быть создана для полного выполнения заданных требований. Элемент системы также может представлять собой систему.

[Адаптировано из ГОСТ Р 57193—2016, пункт 4.1.45]

3.3

информационная система: Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

[ГОСТ Р 51583—2014, пункт 3.4]

3.4

автоматизированная система: Система, состоящая из комплекса средств автоматизации, реализующего информационную технологию выполнения установленных функций, и персонала, обеспечивающего его функционирование.

[ГОСТ Р 59853—2021, статья 2]

3.5 **цели безопасности:** Изложенное намерение обеспечить определенные характеристики (свойства) безопасности системы, выполнение которого проверяется в соответствии с набором согласованных критериев.

Примечание — Характеристики (свойства) системы и критерии проверки должны быть описаны таким образом, чтобы обеспечить возможность проверки факта выполнения изложенного намерения, то есть достижения целей безопасности.

3.6 **предположения безопасности:** Ограничения и допущения, принимаемые в контексте определения целей безопасности и дополняющие цели безопасности.

Примечание — Предположения безопасности, как правило, связаны с особенностями среды функционирования системы и эксплуатационными требованиями (могут относиться к специфике физического доступа к элементам системы), возможностями и расположением потенциального нарушителя. Доказательство соответствия критериям, описывающим цели безопасности, может опираться на условия, соответствующие предположениям безопасности.

3.7 **политика безопасности системы:** Упорядоченный и обоснованный набор правил, процедур, практических приемов или руководящих принципов в области безопасности системы, который используется при проектировании, разработке и обосновании ее свойств безопасности, а также при ее эксплуатации впоследствии.

Примечания

1 Политика безопасности описывает реализацию целей безопасности с учетом предположений безопасности.

2 Положения политики безопасности лежат в основе нормативного обеспечения безопасности системы.

3.8 **доверенная система:** Система, для которой доказано (обосновано) соответствие целям безопасности при условии выполнения предположений безопасности.

Примечание — Доверенным может быть также элемент системы.

Пример — Хранилище данных является доверенным, если оно обеспечивает конфиденциальность, целостность данных и доступность данных по авторизованному запросу.

3.9 **доверенная среда:** Среда функционирования системы, в которой обеспечено выполнение предположений безопасности и соблюдение политики безопасности системы.

3.10 **конструктивный подход (к обеспечению информационной безопасности):** Подход, при использовании которого системе в процессе ее создания с момента замысла придаются характеристики (свойства), которые должны обеспечивать соответствие целям безопасности, включая проверку такого соответствия.

Примечания

1 Примерами таких характеристик являются модульность, иерархичность, распределенность, устойчивость к сбоям и угрозам за счет резервирования элементов системы и т. п., которые могут выполняться не только для систем с конструктивной информационной безопасностью.

2 Конструктивный подход применяется на протяжении жизненного цикла соответствующей системы, начиная с замысла, формирования концепции и проектирования, и может использоваться для создания доверенных систем.

3.11 **конструктивная информационная безопасность:** Информационная безопасность системы, достигнутая применением конструктивных подходов.

Примечания

1 Конструктивная информационная безопасность не является новым и (или) отдельным видом информационной безопасности, а является результатом применения конструктивного подхода к обеспечению информационной безопасности.

2 Процесс обеспечения конструктивной информационной безопасности включает в себя организацию внутренней структуры системы и ее элементов, ее аппаратной и программной архитектуры, а также организацию процессов проектирования и разработки. Это позволяет обеспечить информационную безопасность системы непосредственно в конструкции наряду с применением встроенных механизмов и наложенных средств обеспечения безопасности (при необходимости). Создаваемые с использованием таких способов системы называются системами с конструктивной информационной безопасностью.

3 Автоматизированные системы в защищенном исполнении (в соответствии с ГОСТ Р 51583) могут быть системами с конструктивной безопасностью. Обратное не всегда верно, например в случае внедрения средства защиты информации (СЗИ) после создания защищаемой системы, а также тогда, когда невозможность использования СЗИ компенсируется за счет организационных мер. Совместное применение настоящего стандарта и ГОСТ Р 51583 позволит снизить сложность и стоимость создаваемых АСЗИ за счет встраивания механизмов обеспечения безопасности информации и отказа от использования соответствующих наложенных (внешних) СЗИ.

3.12 **принцип проектирования и разработки безопасной системы:** Принцип проектирования и разработки программного и/или аппаратного обеспечения системы, использование которого придает системе характеристики (свойства), обеспечивающие соответствие целям безопасности.

Примечание — Как правило, принципы проектирования и разработки носят полуформальный, зачастую — эвристический характер (включая принцип наименьших привилегий, принцип эшелонирования защиты и т. д.). Применение принципов проектирования и разработки может быть обосновано положениями нормативных документов, соответствие которым необходимо обеспечить для создаваемой СКИБ.

3.13 **модель безопасности системы:** Структурированное формальное или полуформальное представление правил, процедур, практических приемов или руководящих принципов в области безопасности системы, которое используется при проектировании, реализации и обосновании свойств этой системы, способствующих обеспечению соответствия целям безопасности.

3.14 **механизм обеспечения безопасности:** Взаимоувязанная совокупность способов, методов, правил и процедур, используемых для реализации требований к безопасности системы.

3.15 **шаблон проектирования (и разработки) безопасной системы:** Апробированная схема решения типовой задачи проектирования и разработки программного и/или аппаратного обеспечения системы, применение которой позволяет системе достигнуть целей безопасности с учетом предположений безопасности и придать ей соответствующие свойства.

Примечание — Использование шаблонов проектирования и разработки позволяет решать типовые задачи разработки программного обеспечения, такие как работа в условиях ограниченной производительности компьютерного оборудования (на малоресурсном устройстве), обеспечение доступности, минимизация определенных рисков (предположений безопасности) при выполнении заданных целей безопасности. Некоторые шаблоны проектирования и разработки могут быть реализованы как на программном, так и на аппаратном уровне. Применение шаблонов проектирования позволяет снизить суммарные затраты на создание и эксплуатацию системы.

3.16

безопасное программное обеспечение: Программное обеспечение, разработанное в ходе реализации совокупности процессов (мер), направленных на предотвращение появления и устранение недостатков программы.

[ГОСТ Р 56939—2024, пункт 3.1]

3.17

верификация: Подтверждение, посредством представления объективных свидетельств того, что установленные требования были выполнены.

[ГОСТ Р ИСО 9000—2015, пункт 3.8.12]

3.18 **валидация целей безопасности:** Процедура, которая позволяет убедиться, что реализованные механизмы безопасности в той или иной мере обеспечивают достижение целей безопасности и согласованы с функциональными требованиями и требованиями безопасности к системе.

Примечания

1 В соответствии с ГОСТ Р 57193 требование — утверждение, которое переводит или выражает какую-то потребность и связанные с ней ограничения и условия.

2 Валидацией целей безопасности процедурой может быть, например, тестирование защитных механизмов системы.

3 В валидацию целей безопасности может входить проверка того, что цели безопасности согласованы с функциональными требованиями.

4 Сокращения и обозначения

В настоящем стандарте применены следующие сокращения:

АС — автоматизированная система;

АСЗИ — автоматизированная система в защищенном исполнении;

ВФС — виртуальная файловая система;

ЖЦ — жизненный цикл;

ЗИ — защита информации;

ИБ — информационная безопасность;

КИБ — конструктивная информационная безопасность;

НСД — несанкционированный доступ;

ОС — операционная система;

ПБ — предположения безопасности;

ПО — программное обеспечение;

СЗИ — средство защиты информации;

СКИБ — система с конструктивной информационной безопасностью;

ТЗ — техническое задание;

ЦБ — цели безопасности;

ЭП — электронная подпись;

IoT — интернет вещей (Internet of Things);

IIoT — промышленный интернет вещей (Industrial Internet of Things);

POSIX — набор стандартов, описывающих интерфейсы между операционной системой и прикладной программой (Portable Operating System Interface);

TLS — протокол защиты транспортного уровня (Transport Layer Security).

5 Общие положения

5.1 Методология разработки СКИБ предназначена для реализации мероприятий по защите информации в ходе следующих процессов жизненного цикла систем (в соответствии с ГОСТ Р 57193):

- процесса планирования проекта;
- процесса анализа бизнеса или назначения;
- процесса определения потребностей и требований заинтересованной стороны;
- процесса определения системных требований;
- процесса определения архитектуры;
- процесса определения проекта;
- процесса системного анализа;
- процесса реализации;
- процесса комплексирования;
- процесса гарантии качества;
- процесса верификации;
- процесса валидации.

5.2 Методология разработки СКИБ описывает, как именно в процессах ЖЦ системы реализуются конструктивные подходы к ИБ, детализирует содержание основных работ при создании СКИБ и описывает требования и рекомендации по документированию конструктивных подходов при создании СКИБ. В рамках методологии предлагается к рассмотрению и применению ряд шаблонов проектирования и разработки систем и элементов систем с КИБ. Использование этих шаблонов способствует созданию СКИБ.

5.3 Меры по разработке СКИБ, представленные в рамках методологии, выражены в форме требования, рекомендации или допустимого действия, предназначенных для поддержки достижения результатов реализации мер.

Примечание — Для этой цели в настоящем стандарте используют вспомогательные глаголы «должен», «следует» и «может», чтобы подчеркнуть различие между разными формами требований к реализации мер. Глаголы «должен» и «следует» использованы для выражения условия, требуемого для соответствия, «рекомендуется» и «целесообразно» — для выражения рекомендации среди других возможностей, «может» — для того, чтобы отразить направление допустимых действий в пределах ограничений настоящего стандарта.

Организации, разрабатывающие СКИБ на основании положений настоящего стандарта, ответственны за выбор модели ЖЦ для проекта и своевременное планирование процессов, подходов и работ из настоящего стандарта в своей модели ЖЦ.

5.4 В качестве систем, которые могут быть реализованы как СКИБ, рассматриваются программные и программно-аппаратные средства управления и телекоммуникации, программные и программно-аппаратные комплексы, операционные системы, встраиваемое ПО, серверное ПО, прикладное ПО, программные платформы и их элементы, а также любые информационные, информационно-управ-

ляющие и автоматизированные системы, в отношении которых законодательством или полномочным заинтересованным лицом установлены требования по защите информации, но где использование наложенных (внешних и (или) встраиваемых) средств защиты затруднено и (или) невозможно, например системы, включающие малоресурсные устройства (устройства «Интернета вещей/Промышленного интернета вещей»), применяемые для промышленной автоматизации, информатизации транспортных средств и других областей жизнедеятельности.

Примечания

1 По тексту понятия «система с конструктивной информационной безопасностью» и «система, безопасная конструктивно» являются взаимозаменяемыми.

2 Вычислительные сети и системы, представляющие информационную инфраструктуру организаций, в том числе промышленных предприятий, коммерческих организаций и других объектов хозяйственной деятельности, могут рассматриваться как СКИБ, если для их создания применяются конструктивные подходы, адаптированные с учетом требований к ЖЦ таких систем, особенностей отрасли хозяйственной деятельности, организации процессов проектирования, реализации, ввода в эксплуатацию.

5.5 Если система является ПО любого вида или содержит ПО в качестве элемента, то для его разработки совместно с настоящеим стандартом может быть использован ГОСТ Р 56939.

Примечание — ГОСТ Р 56939 и настоящий стандарт согласованы для параллельного использования в отдельном проекте или отдельной организации.

5.6 Область применения СКИБ включает объекты критической информационной инфраструктуры (системы промышленной автоматизации, энергетики, транспортной инфраструктуры), инфраструктуры телекоммуникации, системы автоматизации и информатизации зданий и сооружений, приборы и бытовые устройства, но не ограничивается ими.

5.7 Целью создания и применения СКИБ является обеспечение информационной безопасности и доверия к системе за счет реализации конструктивных подходов (включая решения по ИБ, заложенные в архитектуру соответствующей системы, но не ограничиваясь ими).

Примечание — Примером решений по ИБ, заложенных в архитектуру, являются принципы построения архитектуры и проектирования, которые могут использоваться при разработке безопасных продуктов, систем и приложений, описанные ГОСТ ISO/IEC TS 19249.

Выбор конструктивных подходов рекомендуется проводить так, чтобы упростить обоснование соответствия ЦБ для системы. Такое обоснование может опираться на предотвращение или снижение последствий от реализации угроз безопасности информации, связанных с воздействием вредоносных программ, осуществлением НСД, а также с эксплуатацией уязвимостей, в результате которых возможны сбои и изменения алгоритмов функционирования системы. Упрощение обоснования может быть связано с уменьшением поверхности атаки, со снижением количества связей между элементами системы (тем самым уменьшается возможность сценариев развития атаки), с выбором технологий реализации, устойчивых к определенным видам атак, актуальных для системы, и т. п.

5.8 Методы, применяемые при реализации КИБ, могут обеспечивать соответствие ЦБ (при условии соблюдения ПБ) соответствующей системы (СКИБ или системы, элементом которой является СКИБ) путем задания, реализации и контроля выполнения следующих требований:

- требований по ЗИ, начиная с этапа замысла, концепции, проектирования архитектуры сети, системы и проектирования архитектуры соответствующего ПО;
- требований по обеспечению безопасности взаимодействия системы с внешними системами и информационной инфраструктурой;
- требований по устойчивому выполнению системой целевых (минимального набора заранее определенных) функций, в том числе в нестабильных внешних условиях или под атакой;
- требований к процессам жизненного цикла системы (в соответствии с ГОСТ Р 57193), в том числе требований по безопасной разработке программного обеспечения (в соответствии с ГОСТ Р 56939);
- требований по обеспечению соответствия функционирования системы положениям законодательства и нормативных документов государственных и отраслевых регуляторов (при наличии таких требований).

5.9 Система является безопасной конструктивно, если решения, заложенные в ее архитектуру и реализацию, упрощают обеспечение соответствия данной системы определенным для нее ЦБ (при условии соблюдения ПБ), включая возможность обоснования такого соответствия, в сравнении со случаем, когда такие решения не применяются.

Примечания

1 Обоснование может проводиться, к примеру, на основе комплексного учета трудозатрат на внедрение механизмов безопасности, на основе объема программы и методики испытаний, на основе количества тестов, реализуемых в процессе введения в эксплуатацию, или другими методами. Определение или ограничение методов демонстрации соответствия не является задачей настоящего национального стандарта. Методы оценки зависят от вида и характеристик системы, а объективность методов оценки является предметом рассмотрения при утверждении методики оценки соответствия настоящему национальному стандарту.

2 Наиболее очевидным эффект от применения конструктивных методов может быть для систем и сетей инфраструктуры крупных хозяйственных объектов, таких как промышленные предприятия.

Пример — Взаимная изоляция сетевых сегментов, заложенная при проектировании сетевой инфраструктуры, помогает снизить объем работ по тестированию на проникновение в вычислительных сетях.

5.10 Характерные черты процесса разработки СКИБ:

- мероприятия по защите информации и обеспечению ИБ являются неотъемлемой частью мероприятий, выполняемых на протяжении ЖЦ системы, и согласованы между собой на всех этапах ЖЦ системы;
- ЦБ для системы и (или) ее элементов определяются частично или полностью задачами обработки информации и (или) управления процессами, которые формулируются исходя из целевого назначения данной системы, требованиями, предъявляемыми к обрабатываемой информации и процессам, контролируемым (реализуемым) при помощи системы, угрозами безопасности информации (при наличии модели угроз ЦБ не должны ей противоречить) и процессам, контролируемым (реализуемым) при помощи системы;
- ПБ для системы и (или) ее элементов определяются частично или полностью программным и аппаратным составом системы, конфигурацией, условиями функционирования и эксплуатации (в том числе — сетевого взаимодействия), планируемыми (предполагаемыми) требованиями и интересами оператора или владельца системы, человеческим фактором, физическим размещением, другими внешними по отношению к системе факторами;
- состав требований по ЗИ для системы определяется ЦБ и ПБ;
- состав требований по ЗИ для системы при необходимости следует дополнить обязательными требованиями по ЗИ, выдвигаемыми государственными и отраслевыми регуляторами;
- при создании системы как системы с КИБ конструктивные подходы к обеспечению информационной безопасности этой системы и ее элементов реализуются начиная с ранних этапов жизненного цикла этой системы (замысла, концепции, проектирования архитектуры системы, проектирования архитектуры программных средств);
- при создании системы как системы с КИБ применяемые конструктивные подходы к информационной безопасности рекомендуется обосновать относительно ЦБ, ПБ и требований по ЗИ; к примеру, применение моделей безопасности системы, описывающих контроль доступа, может обосновываться необходимостью разделения прав при многопользовательском доступе к системе;
- реализация КИБ не должна вносить искажения в нормальное (штатное) функционирование системы (нарушать функционирование системы), составным элементом которой является СКИБ (или в составе которой планируется применение СКИБ), однако может накладывать дополнительные ограничения на работу данной системы.

5.11 При проектировании систем с использованием конструктивного подхода (подходов) достигаются ключевые характеристики СКИБ:

- вычислимость безопасного состояния — возможность провести валидацию ЦБ для системы на основе достоверной информации о наблюдаемых действиях и событиях в этой системе и (или) в среде ее функционирования. Выводы о достоверности информации основываются на предположениях безопасности (которые, в свою очередь, могут опираться на обоснованные характеристики других систем).

Пример — Примером источника достоверной информации могут быть средства мониторинга, внешние по отношению к СКИБ;

- подотчетность — возможность отслеживания и учета действий и событий в системе и (или) в среде ее функционирования, влияющих на состояние безопасности;
- безопасные умолчания — запрет по умолчанию на выполнение действий, влияющих на состояние безопасности; выполнение таких действий — только при наличии явного (формального) разрешения или указания, описанного моделью безопасности системы или политикой безопасности;

- минимальные возможности компрометации — минимизация функций и привилегий, ассоциированных с каждым элементом системы, до необходимого (оптимального) множества этих функций и привилегий, а также оптимизация количества элементов системы;

- согласованность (валидируемость, проверяемость, корреляция) ЦБ и ПБ — возможность оценки корректности требований безопасности, функциональных спецификаций и т. п. относительно ЦБ (валидируемость), а также корректности работы системы в соответствии с требованиями безопасности (верифицируемость);

- невозможность подделки и несанкционированной модификации элементов системы, влияющих на состояние безопасности.

5.12 При разработке СКИБ рекомендуется руководствоваться следующими положениями:

- действия (мероприятия) по созданию СКИБ должны быть реализованы в ходе процессов ЖЦ системы;

- используемые при создании СКИБ шаблоны проектирования целесообразно выбирать исходя из задач, решаемых этой СКИБ и (или) системой (сетью), для использования в которой создается СКИБ, ЦБ и ПБ, и учитывать особенности проектирования элементов этой системы, частью (элементом) которой будет СКИБ;

- используемые при создании СКИБ шаблоны проектирования могут обеспечивать возможность формирования различных вариантов ее построения для выбора оптимального варианта, обеспечивающего максимальную устойчивость создаваемой СКИБ к воздействию вредоносных программ, осуществлению НСД и эксплуатации уязвимостей, а также возможность по наращиванию функционала (модернизации, обновления) СКИБ в зависимости от условий применения и требований безопасности информации;

- СКИБ кроме основных функций может обеспечивать комплексное решение задач по ЗИ от НСД, несанкционированных и непреднамеренных воздействий на информацию в составе других систем и сетей применительно к конкретным условиям ее применения. Состав решаемых задач по ЗИ определяется задачами обработки информации, составом и конфигурацией системы, осуществляющей обработку информации, условиями функционирования, требованиями, предъявляемыми к обрабатываемой информации, угрозами безопасности информации;

- СКИБ следует создавать с учетом требований безопасности информации при сетевом взаимодействии;

- входящие в состав СКИБ программные модули, реализующие функции ЗИ и контроль работы этих функций (в том числе аудит событий ИБ), не должны препятствовать реализации функциональных требований и требований по надежности СКИБ;

- элементы СКИБ должны быть совместимы между собой (корректно работать совместно) и не должны ухудшать надежность и защищенность создаваемой СКИБ;

- создаваемая СКИБ должна быть совместимой с взаимодействующими с ней внешними системами.

5.13 СКИБ рекомендуется создавать в соответствии с базовым документом, на основании которого выполняются работы по ее разработке, а также осуществляется оценка и приемка СКИБ. Примером такого базового документа на СКИБ является ТЗ. Базовый документ может составлять часть документации разработчика в соответствии с ГОСТ Р 56939.

Примечание — Требования к реализации конструктивного подхода при создании СКИБ могут содержаться в отдельном разделе концепции по ее созданию, а также могут быть вынесены в отдельный документ (задание по безопасности, положение по безопасности и т. д.), ссылка на который должна содержаться в концепции создания ПО или в ТЗ.

5.14 В работах (мероприятиях) по созданию СКИБ участвуют:

- заказчик СКИБ — в части задания требований ТЗ, включения в документацию на СКИБ обоснованных требований безопасности информации и контроля их выполнения при экспертизе документации, в ходе проведения испытаний и приемки СКИБ;

- разработчик СКИБ — в части создания СКИБ и обеспечения соответствия разрабатываемой СКИБ требованиям ТЗ, нормативных правовых актов, методических документов и национальных стандартов в области ЗИ, а также гарантии качества;

- организация, проводящая оценку СКИБ на соответствие настоящему стандарту.

Примечание — Гарантия качества (по ГОСТ Р 71304) — основания для уверенности в текущем или будущем соответствии заявленному качеству.

5.15 Испытания СКИБ должны включать в себя испытания на соответствие требованиям безопасности информации и могут осуществляться в соответствии с положениями нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти и государственных стандартов в области ЗИ. Перечень соответствующих документов должен быть зафиксирован в базовом документе на СКИБ.

5.16 Работы по разработке и эксплуатации СКИБ с реализацией криптографической ЗИ необходимо проводить в соответствии с законодательством Российской Федерации.

6 Реализация подходов к созданию систем с конструктивной информационной безопасностью

6.1 Реализация конструктивных подходов в рамках методологии разработки СКИБ должна заключаться:

а) в анализе с точки зрения безопасности информации предметной области (области применения, отрасли промышленности и т.д.), для которой создается СКИБ, в определении границ и внешних взаимодействий СКИБ, группировании системных элементов в соответствии с их функциональным назначением и с требованиями безопасности, описании взаимодействий системных элементов между собой и с внешними системами.

Примечание — Для описания и анализа будущего поведения СКИБ в предметной области, определения границ и внешних взаимодействий СКИБ можно использовать диаграммы развертывания (англ. deployment diagram);

б) определении ЦБ и соответствующих требований обеспечения безопасности информации, подлежащих реализации при создании СКИБ, с учетом интересов всех участников ЖЦ СКИБ, в том числе требований к содержанию и порядку выполнения работ, связанных с созданием СКИБ и формированием (поддержанием) среды обеспечения оперативного устранения выявленных пользователями недостатков и уязвимостей СКИБ;

в) проектировании различных вариантов архитектуры СКИБ и выборе оптимального варианта архитектуры СКИБ путем моделирования свойств СКИБ и механизмов обеспечения безопасности СКИБ, в том числе с использованием следующих методов:

1) создания и анализа диаграмм взаимосвязей между элементами СКИБ, анализа возможных потоков данных и управления между элементами СКИБ и внешними системами.

Примечание — Примером удачного инструмента моделирования для анализа взаимосвязей элементов системы на этом этапе являются диаграммы потоков данных (англ. data flow diagram), также для анализа могут быть использованы диаграммы последовательностей (англ. sequence diagram);

2) определения и анализа алгоритмов взаимодействия и протоколов, обеспечивающих передачу данных, контроль и управление элементами системы;

3) описания и анализа представлений и моделей системы, применимых при проектировании отдельных механизмов обеспечения безопасности, в частности механизмов контроля доступа к системе, ее элементам и ресурсам.

Примечание — Для описания представлений и моделей системы с целью проектирования и анализа механизмов обеспечения безопасности удобно использовать диаграммы состояний (англ. state diagram);

4) обеспечения возможности использования шаблонов проектирования и разработки, соответствующих ЦБ системы, при формировании вариантов архитектуры;

5) выстраивания архитектуры с учетом требований и характеристик проекта, в том числе для соответствия определенным для данного проекта ЦБ при условии соблюдения предположений безопасности за счет применения соответствующих технологий и технических решений;

г) определении (выборе) шаблонов проектирования (перечень примеров которых приведен в приложении А), подлежащих применению при разработке элементов СКИБ и реализации алгоритмов взаимодействия между ними и протоколов, обеспечивающих передачу данных, контроль и управление (при наличии возможности). Допускается самостоятельная разработка таких шаблонов и их повторное использование при условии подтверждения, что использование разработанного шаблона позволяет реализовать КИБ какой-либо системы в порядке, установленном настоящим стандартом, при этом вновь разработанные шаблоны включаются в базовый документ на СКИБ и подлежат проверке на предмет способствования в достижении ЦБ при оценке соответствия СКИБ настоящему стандарту;

д) применении методов организации жизненного цикла разработки системы (в соответствии с ГОСТ Р 57193) с целью обеспечения выполнения функциональных и нефункциональных требований к системе (также в соответствии с ГОСТ Р 57193 и включая требования безопасности), в том числе к реализации участниками процессов ЖЦ систем требований к содержанию и порядку выполнения работ, связанных с созданием безопасного (защищенного) программного обеспечения (в соответствии с ГОСТ Р 56939) и формированием (поддержанием) среды обеспечения оперативного устранения выявленных ошибок и уязвимостей программного обеспечения СКИБ;

е) применении следующих общих принципов проектирования и разработки элементов СКИБ и системы в целом (следование принципам является рекомендуемым, обязательность и приоритет принципов определяются разработчиком исходя из ЦБ и ПБ разрабатываемых систем):

1) принцип разумной простоты (economy of mechanism): СКИБ и ее элементы, включая механизмы обеспечения безопасности, рекомендуется создавать возможно более простыми (в том числе иметь минимально возможный размер программного кода), чтобы уменьшить вероятность возникновения уязвимостей и упростить проверки безопасности;

2) принцип безопасных умолчаний (fail-safe defaults): доступ к информации, информационное и (или) управляющее взаимодействие в отсутствие разрешения на эту операцию должны быть запрещены;

3) принцип полноты перекрытия (complete mediation): реализация механизма обеспечения безопасности должна иметь сквозной характер (по возможности охватывать все взаимосвязанные элементы СКИБ);

4) принцип минимизации поверхности атаки: рекомендуется минимизировать количество интерфейсов, к которым потенциальный злоумышленник может получить доступ, уменьшить сложность этих интерфейсов и защитить их использование для своевременного обнаружения потенциальных злоупотреблений или попыток атаки;

5) принцип централизованной проверки параметров: необходимо гарантировать, что все параметры критических функций проверяются с использованием общего набора функций проверки, которые были тщательно проанализированы на точность и полноту;

6) принцип разделения привилегий (separation of privilege): механизм обеспечения безопасности должен позволять выполнять доступ к информации или выполнение иной операции на основе двух и более независимых факторов авторизации, где это возможно; различные виды или уровни доступа должны требовать различной авторизации на основе установленных факторов;

7) принцип наименьших привилегий (least privilege): если с элементом СКИБ, ее пользователем или процессом ассоциированы какие-либо права и привилегии, они должны быть сведены к минимально необходимым для выполнения установленных для элемента функций;

8) принцип минимизации зависимостей (least common mechanism): количество элементов СКИБ, которые связаны с другими элементами или используются несколькими пользователями или процессами с различными привилегиями, рекомендуется уменьшить, насколько это возможно;

9) принцип эшелонированной защиты (defense-in-depth): безопасность рекомендуется обеспечивать посредством многоуровневой (комплексной) защиты системы с использованием различных мер с целью предотвращения или сдерживания угроз безопасности информации на разных этапах реализации системы;

ж) проведении испытаний элементов СКИБ и СКИБ в целом на соответствие требованиям безопасности информации, включая соответствие ЦБ при условии соблюдения ПБ; проведении работ по регистрации, анализу и классификации инцидентов ИБ и уязвимостей в ходе эксплуатации СКИБ, а также их устранению.

6.2 Общие основы, совокупность приемов и содержание процессов создания системы определяются ГОСТ Р 57193, а общая структура процессов ЖЦ программного обеспечения и программных продуктов (каждый из которых сам по себе является системой) — ГОСТ Р ИСО/МЭК 12207 и ГОСТ Р 56939. Состав основных работ создания СКИБ должен включать:

- определение ЦБ и ПБ;
- определение и последующее уточнение требований, предъявляемых к СКИБ на основе ЦБ и ПБ;
- проектирование архитектуры СКИБ;
- определение технологий реализации СКИБ и ее элементов;
- реализацию элементов СКИБ и проведение испытаний элементов СКИБ и СКИБ в целом на соответствие установленным требованиям, а также ЦБ;

- сопровождение СКИБ в ходе ее эксплуатации в интересах обеспечения гарантии качества и безопасности.

В состав мер по управлению работами при создании СКИБ рекомендуется включать управление конфигурацией, в соответствии с описанием процесса управления конфигурацией в ГОСТ Р 57193.

При этом последовательность вышеуказанных работ в методологии разработки СКИБ соответствует порядку их перечисления выше, если иное не предусмотрено отраслевыми стандартами на ЖЦ создания СКИБ. В последнем случае порядок выполнения работ может быть адаптирован для соответствия отраслевым стандартам.

Примечание — Под отраслевыми стандартами подразумеваются национальные и международные стандарты, принятые в отдельной отрасли экономики производства.

Примеры

1 Автомобилестроение (национальный стандарт): ГОСТ Р ИСО 26262-2 Дорожные транспортные средства. Функциональная безопасность. Часть 2. Менеджмент функциональной безопасности.

2 Промышленное производство (международный стандарт): IEC 62443-4-1:2018. Security for industrial automation and control systems — Part 4-1: Secure product development lifecycle requirements

6.3 Выполнение работы по определению ЦБ и ПБ рекомендуется проводить в ходе процесса планирования проекта и процесса анализа сферы применения (бизнеса) или назначения системы согласно ГОСТ Р 57193, с использованием методов анализа конфликта интересов, аналогий и системного анализа угроз безопасности информации. К примеру, в случае анализа конфликта интересов для системы определяется круг заинтересованных лиц, проводится опрос с целью выяснения их интересов (в соответствии с ГОСТ Р 57193) относительно системы, и затем интересы подвергаются анализу с целью выявления объективных целей, объединяющих эти интересы. При использовании метода аналогий ЦБ могут формулироваться в сравнении с системами похожего назначения или применяющимися в той же предметной области. Системный анализ угроз безопасности информации выявляет актуальные ЦБ для противостояния этим угрозам. Эти и другие методы могут применяться в комплексе мероприятий анализа бизнеса или назначения системы (в соответствии с ГОСТ Р 57193). Для уточнения ЦБ целесообразно проводить анализ требований безопасности, предъявляемых к системе, для применения в которой создается СКИБ, в контексте функциональных требований к этой системе, а также защищенности информационной системы/сети, назначения, функций и условий ее функционирования. В ходе последующих процессов ЖЦ СКИБ требования безопасности информации, предъявляемые к СКИБ, подлежат уточнению по результатам реализации соответствующих процессов ЖЦ СКИБ.

6.4 Выполнение работы по определению требований, предъявляемых к СКИБ на основе ЦБ и ПБ, и технологий реализации СКИБ и ее элементов рекомендуется проводить в ходе процесса определения системных требований и продолжать в ходе процесса определения проекта по созданию СКИБ и процесса системного анализа согласно ГОСТ Р 57193. Определение и уточнение требований целесообразно проводить с использованием методов системного анализа, в том числе на основе анализа результатов формирования архитектуры СКИБ и оценки применимости современных информационных технологий в интересах ее практической реализации. При применении методов системного анализа рекомендуется особое внимание уделять анализу прослеживаемости между характеристиками проекта системы и архитектурными компонентами, определенными взаимодействиями элементов системы, результатами анализа ЦБ и ПБ, методами и методиками верификации и требованиями к системным элементам. Двунаправленная прослеживамость (в соответствии с ГОСТ Р 57193) обеспечивается на протяжении всего жизненного цикла разработки системы.

6.5 Выполнение работы по формированию архитектуры СКИБ следует проводить в ходе процесса определения архитектуры СКИБ, с использованием различных методов, включая (но не ограничиваясь) методы логического и имитационного моделирования, применения архитектурных представлений и шаблонов, методов итерационной или иной организации ЖЦ разработки, нормативных подходов и принципов ИБ. Требования, проистекающие из нормативного регулирования, как правило, ограничивают эталонную архитектуру для обеспечения контроля аспектов поведения системы и обрабатываемой ею информации. В качестве примеров можно привести требование подключения к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы объектов критической информационной инфраструктуры и требования к обработке биометрических персональных данных в единой контролируемой системе. Принципы ИБ,такие как принцип минимизации зависимостей, принцип наименьших привилегий и разделения привилегий, применяются при анализе альтернатив в формировании архитектуры к архитектурным элементам СКИБ.

6.6 Реализацию элементов СКИБ следует осуществлять в ходе процессов определения проекта, системного анализа, реализации, комплексирования, которые, в свою очередь, должны соответствовать ГОСТ Р 57193.

6.7 По результатам выполнения работ по реализации элементов СКИБ следует провести испытания элементов СКИБ и СКИБ в целом на соответствие требованиям безопасности информации; для этого целесообразно реализовать процессы гарантии качества, верификации требований и валидации ЦБ. Изначальные требования к процессам гарантии, верификации и валидации определяются ГОСТ Р 57193 и профильными отраслевыми стандартами.

Примечание — Состав и документирование испытаний СКИБ рекомендуется осуществлять согласно ГОСТ Р 51583.

6.8 Результаты выполнения работ по созданию СКИБ рекомендуется задокументировать путем разработки пояснительных записок, схем, моделей, описаний, алгоритмов и аспектов функционирования СКИБ и т. п. в соответствии с требованиями стандартов Единой системы программной документации и Единой системы конструкторской документации.

6.9 В части результатов работ по созданию СКИБ документированию подлежат:

- ЦБ и ПБ;
- описание архитектуры СКИБ, взаимосвязей с внешними информационными системами и сетями, интерфейсов доступа и способов доступа к СКИБ;
- модель угроз безопасности информации и типового нарушителя с указанием вида нарушителя, его категории, целей и возможных действий (обусловленных его мотивами, интересами, потребностями, т. е. анализ проводится относительно тех же факторов, что и для заинтересованных сторон);
- описание потенциальных векторов, сценариев атак, тактик и техник воздействия вредоносных программ и осуществления НСД;
- требования безопасности информации, предъявляемые к СКИБ, методы и средства обеспечения безопасности информации;
- описание механизмов, обеспечивающих надежную реализацию функций СКИБ в условиях воздействия вредоносных программ, НСД и эксплуатации уязвимостей СКИБ;
- ограничения, предъявляемые к СКИБ;
- рекомендации по реализации требований безопасности, предъявляемых при проведении работ по обновлению системного и прикладного ПО СКИБ;
- программа, методики и протоколы проведения испытаний реализации КИБ.

6.10 Содержание основных работ при создании СКИБ приведено в разделе 7. Содержание соответствующих работ может уточняться в соответствии с требованиями нормативных правовых актов уполномоченных федеральных органов исполнительной власти и национальных стандартов в области ЗИ, а также в соответствии с дополнительными требованиями, предъявляемыми заказчиками ПО, заказчиками (владельцами) информационных систем/сетей, государственными и отраслевыми регуляторами.

7 Содержание основных работ при создании систем с конструктивной информационной безопасностью

7.1 Определение целей и предположений безопасности

7.1.1 Определение ЦБ и ПБ осуществляется в процессе планирования проекта (с учетом результатов анализа бизнеса или требований назначения, выполненного в соответствии с ГОСТ Р 57193).

7.1.2 В качестве основы для определения ЦБ рекомендуется рассматривать мотивы заинтересованных сторон: факторы, описывающие любые виды заинтересованности в сохранении или, напротив, в нарушении безопасности системы. В качестве заинтересованных сторон рассматривается круг субъектов, не ограниченный прямой или косвенной связью с системой. Потенциальный нарушитель (нарушители) входит в круг заинтересованных сторон, его (или их) мотивы целесообразно принимать во внимание и учитывать так, чтобы его интересы не могли быть удовлетворены.

Примечание — В соответствии с ГОСТ Р 57193 заинтересованная сторона — индивидуум или организация, имеющие право, долю, требование или интерес в системе или в обладании ее характеристиками, удовлетворяющими их потребности и ожидания.

Пример — Конечные пользователи, организации конечного пользователя, поддерживающие стороны, разработчики, производители, обучающие стороны, сопровождающие и утилизирующие организации, приобретающие стороны, организации поставщика, органы регуляторов. Некоторые заинтересованные стороны могут иметь противоположные интересы в системе.

7.1.3 Рекомендуется описательная (не предписывающая действие) формулировка ЦБ.

Пример — Формулировка «данные пользователя, внесенные в систему, ни при каких условиях не становятся известны неавторизованным лицам» предпочтительнее формулировки «доступ к данным пользователя должен быть ограничен механизмом авторизации».

7.1.4 Предположения безопасности представляют собой ограничения и допущения, принимаемые в контексте определения ЦБ. Как правило, эти ограничения и допущения связаны с особенностями эксплуатации, средой функционирования системы и требованиями к этой среде, они могут относиться к специфическому порядку физического доступа к системе или элементу системы, предположениям относительно возможностей актуального нарушителя (включая возможности его локального или удаленного доступа к системе и т. п.).

7.1.5 Предположения безопасности могут быть связаны с мотивами заинтересованных сторон (к примеру, является ли внутренний нарушитель одним из видов предполагаемых нарушителей) или действовать как объективные факторы внешней среды.

7.1.6 Некоторые ПБ могут требовать реализации дополнительных организационных мер обеспечения безопасности или технических мер защиты (физический контроль доступа к системе, помещение ее в закрытый корпус, механическая блокировка аппаратных интерфейсов), что в дальнейшем может выражаться в дополнительных эксплуатационных требованиях к СКИБ.

7.1.7 В анализ факторов взаимодействия и мотивов заинтересованных сторон для определения ЦБ рекомендуется включить поиск ответов на следующие вопросы (перечень может быть расширен):

- какие мотивы каких заинтересованных сторон целесообразно учесть при формулировании ЦБ; в частности, при выяснении этого требуется определить проблемные вопросы (субъективные опасения и поводы для беспокойства) в отношении информационной безопасности (для заинтересованных сторон, доступных к опросу/интервьюированию);
- кто является типовым нарушителем и каковы его мотивы, возможности и ограничения;
- какие мотивы относятся непосредственно к обеспечению безопасности и защите системы от атак (к примеру: «необходимо защитить данные в системе, так как они составляют коммерческую тайну», «необходимо защитить систему от атак отказа в обслуживании, поскольку такие атаки часто выполняются на системы схожего назначения»), а какие — косвенно (в том числе требования законодательства, возможность получить маркетинговое преимущество перед конкурентами, репутационные соображения и т. д.);
- есть ли законодательная необходимость в защите создаваемой СКИБ, положения каких нормативных документов следует учитывать в обязательном порядке;
- провоцируют ли мотивы заинтересованных сторон ситуацию конфликта интересов и как эта ситуация разрешается при определении ЦБ (в частности, требуется ли введение дополнительных предположений безопасности о действиях заинтересованных сторон или иных ограничений);
- какие ПБ изначально действуют в отношении системы и контекста ее использования;
- учитывает ли сформулированный перечень ЦБ и ПБ все известные мотивы заинтересованных сторон.

7.1.8 Совокупность перечисленных факторов (субъективных опасений, мотивов, объективных требований законодательства, условий, составляющих контекст использования системы и т. д.) рекомендуется оценивать, детализировать и оценивать повторно на протяжении всего процесса разработки СКИБ; при необходимости ЦБ и (или) ПБ могут быть скорректированы.

7.1.9 Результатом анализа, оценки, детализации и повторной оценки перечисленных факторов является документированный набор ЦБ и ПБ СКИБ.

7.2 Определение требований, предъявляемых к СКИБ на основе целей и предположений безопасности

7.2.1 Определение требований, предъявляемых к СКИБ на основе ЦБ и ПБ, рекомендуется осуществлять в процессе определения системных требований в соответствии с ГОСТ Р 57193. Далее производится уточнение требований в процессе определения проекта, также в соответствии с ГОСТ Р 57193. Таким образом, первичный набор требований целесообразно описать до создания архитектуры систе-

мы и продолжать уточнять после создания архитектуры, так, чтобы наиболее полно реализовать конструктивные решения, заложенные в том числе в архитектуру СКИБ.

7.2.2 Определение требований, предъявляемых к СКИБ на основе ЦБ и ПБ, рекомендуется осуществлять путем проведения анализа назначения, функций, условий функционирования, защищенности создаваемой СКИБ и/или системы, для использования в составе которой создается СКИБ, характера обрабатываемой информации, угроз безопасности информации и требований безопасности информации, предъявляемых к информационной системе/сети, применительно к назначению создаваемой СКИБ.

7.2.3 По результатам анализа и уточнения требований рекомендуется определить:

- перечень пользователей СКИБ;
- перечень внешних сторон, заинтересованных в получении доступа к ресурсам СКИБ и самой СКИБ, их мотивы и возможности, внешние системы, которые они могут использовать.

Примечание — Заинтересованная сторона (см. ГОСТ Р 57193) — индивидуум или организация, имеющие право, долю, требование или интерес в системе или в обладании ее характеристиками, удовлетворяющими их потребности и ожидания. В том числе это могут быть внешние по отношению к системе индивидуумы или организации, которые могут быть заинтересованы в получении доступа к системе;

- границы СКИБ с точки зрения взаимодействий с внешними сторонами и интерфейсов с внешними системами.

Примечание — Границы системы с точки зрения интерфейсов с другими системами и взаимодействий с внешними сторонами представляют собой т. н. поверхность атаки (см. примечание к 9.1.6), которую рекомендуется минимизировать при решении задачи проектирования СКИБ;

- условия получения заинтересованными сторонами доступа к ресурсам СКИБ и самой СКИБ, включая условия непредусмотренного взаимодействия с внешними системами;
- угрозы безопасности информации, связанные с возможными действиями сторон, заинтересованных в получении доступа к ресурсам СКИБ и самой СКИБ;
- характеристики каждого элемента СКИБ, связанные с доверием к этому элементу (описанному с точки зрения ЦБ для этого элемента) и его ролью в выполнении ЦБ для СКИБ в целом.

Примечание — Выявление доверенных элементов является одной из задач процесса определения архитектуры СКИБ;

- характеристики взаимодействий между элементами СКИБ;
- ограничения, предъявляемые к СКИБ, ее элементам и процессам взаимодействия между элементами, связанные с назначением СКИБ, ПБ и угрозами безопасности информации, влияющими на ее функционирование;
- требования безопасности информации, предъявляемые к СКИБ.

7.3 Проектирование архитектуры СКИБ

7.3.1 Создание (разработка) архитектуры СКИБ осуществляется в процессе определения архитектуры СКИБ в соответствии с ГОСТ Р 57193. Согласно упомянутому стандарту проектирование архитектуры СКИБ рекомендуется проводить путем формирования нескольких ее альтернативных вариантов с последующим выбором предпочтительного варианта при условии реализации ЦБ при соблюдении ПБ.

7.3.2 При создании и выборе варианта архитектуры СКИБ рекомендуется опираться на ЦБ и ПБ, их взаимосвязи и взаимозависимости, формировать основу для защиты системы в целом, ее информационных ресурсов и компонентов, а также обеспечения устойчивого функционирования и отсутствия влияния на внешние системы и информационную инфраструктуру в случае компрометации.

Также на архитектуру СКИБ могут оказывать влияние требования безопасности как результат формализации и детализации ЦБ и ПБ, однако после формирования архитектуры СКИБ требования безопасности сами могут быть скорректированы.

7.3.3 Архитектуру СКИБ рекомендуется проектировать в соответствии со следующими основными принципами:

- типизации структурных элементов системы за счет использования шаблонов проектирования;
- системной организации структурных элементов создаваемой СКИБ в интересах снижения ее общей сложности;

- многократного (повторного) использования ранее созданных и апробированных элементов СКИБ, для которых подтверждена их КИБ;
- вложенности (иерархичности) элементов СКИБ;
- минимизации количества функциональных связей между элементами СКИБ;
- минимизации потоков данных, передаваемых между элементами СКИБ;
- возможности проведения испытаний отдельных элементов СКИБ;
- масштабируемости процесса разработки СКИБ.

Примечание — Минимизация количества функциональных связей между элементами СКИБ и потоков данных, передаваемых между элементами СКИБ, достигается при анализе альтернатив в процессе определения архитектуры СКИБ.

7.3.4 В интересах проектирования архитектуры СКИБ рекомендуется разрабатывать ее архитектурную модель применительно к назначению и задачам, подлежащим решению системой или сетью, а также к условиям ее функционирования.

7.3.5 При разработке архитектурной модели СКИБ рекомендуется проводить:

- логическое разделение модели на элементы нескольких уровней, в которых элементы нижних уровней иерархии обеспечивают реализацию функций элементов верхних уровней (вертикальная декомпозиция);
- логическое разделение модели или ее элемента на системные элементы, равноправные согласно иерархии (горизонтальная декомпозиция);
- группирование и типизацию элементов модели, а также связей между ними;
- уточнение требований безопасности информации, предъявляемых к СКИБ, с учетом результатов группирования и типизации элементов модели;
- уменьшение (с учетом требований безопасности информации) количества связей между элементами модели, а также количества точек (интерфейсов) доступа заинтересованных сторон к ресурсам СКИБ до минимально необходимого без потери функциональности СКИБ.

7.3.6 По результатам разработки архитектурной модели СКИБ должны быть определены:

- точки входа в СКИБ со стороны внешних систем;
- описание назначения, содержания и формата внешних данных с учетом доверия к источнику данных (в форме предположений безопасности);
- состав элементов СКИБ, необходимых для решения возложенных на нее задач, в том числе элементов, прямо или косвенно связанных с обеспечением соответствия ЦБ СКИБ, и взаимосвязи между элементами.

Примечание — Определение элементов СКИБ и взаимосвязей между ними на этом этапе осуществляется на уровне деталей, необходимых для выражения архитектурного намерения, и может быть уточнено в процессе определения проекта согласно ГОСТ Р 57193;

- описание назначения, содержания и формата данных, которыми обмениваются структурные элементы СКИБ, описание протоколов взаимодействия;
- состав угроз безопасности информации (применительно к структурным элементам СКИБ), характеристики структурных элементов СКИБ, описание назначения, содержания и формата передаваемых между элементами данных, влияющих на реализацию угроз безопасности информации;
- приемлемые уровни риска, включая риски, связанные с возможной утечкой, утратой целостности или потерей информации, с отказом системы или отдельных функций этой системы, с нештатным (недокументированным) изменением функционирования системы, в том числе производственные риски, риски для окружающей среды, жизни и здоровья людей, любые иные риски, а также допустимые затраты в интересах компенсации этих рисков со стороны СКИБ и ее элементов (риски и затраты оцениваются по шкалам, принятым в области применения системы или сформированным при участии лиц, заинтересованных в корректной работе системы);
- методы и меры обеспечения безопасности информации, подлежащие реализации для достижения требуемого уровня защищенности СКИБ или информационной системы/сети, в интересах которой создается СКИБ.

Примечание — Указанные методы и средства, подлежащие реализации, распределяются по элементам СКИБ так, чтобы обеспечить сквозной характер обеспечения безопасности информации, планируемый уровень отказоустойчивости этих средств и создаваемой системы в целом и другие необходимые проектные характеристики СКИБ;

- шаблоны проектирования (применительно к задачам, подлежащим решению СКИБ) с учетом векторов возможных воздействий на СКИБ, взаимосвязей между элементами СКИБ, которые прямо или косвенно влияют на безопасность элементов СКИБ, требований безопасности информации;
- альтернативные варианты архитектуры СКИБ.

Примечание — Планирование и выделение ресурсов, необходимых для подготовки материалов, указанных в 7.3.6, обеспечивает организация — разработчик СКИБ.

7.3.7 Формирование и оценка вариантов архитектуры СКИБ проводятся с учетом общих принципов проектирования и разработки, перечисленных в 6.1.

7.3.8 В общем случае в определении архитектуры используются различные модели и архитектурные представления. Впоследствии применяются те модели и архитектурные представления, которые лучше всех отражают интересы заинтересованных сторон.

Примечание — Из моделей для ИБ наиболее распространены модели управления доступом, в том числе формальные, однако анализ архитектуры не ограничивается только этим видом моделей. Подходящие модели и архитектурные представления могут подбираться, приспосабливаться или разрабатываться на протяжении процессов проектирования архитектуры и определения проекта и приводить к конкретным проектным решениям, подлежащим дальнейшей реализации в соответствии с ГОСТ Р 57193.

7.3.9 Варианты архитектуры целесообразно продолжать анализировать и адаптировать в процессе определения проекта согласно ГОСТ Р 57193, в том числе при формировании и уточнении системных требований, связанных с обеспечением соответствия ЦБ. Формирование итогового варианта архитектуры может носить итеративный характер, вплоть до определения согласованного с этим вариантом множества требований, предъявляемых к СКИБ на основе ЦБ и ПБ.

Примечание — При определении и анализе вариантов архитектуры рекомендуется обращаться к принципам построения архитектуры безопасных продуктов, систем и приложений, определенным ГОСТ ISO/IEC TS 19249. Для построения архитектуры СКИБ особенно актуальными являются принципы разделения на домены, многоуровневой архитектуры, инкапсуляции и резервирования. При этом на этапе определения проекта следует проследить, чтобы архитектурные принципы получили адекватное техническое воплощение.

7.3.10 Формирование итогового варианта архитектуры СКИБ, определение основных принципов развития (обновления) СКИБ рекомендуется осуществлять путем оценки соответствия вариантов архитектуры СКИБ, ее ЦБ и ПБ, с учетом периодической актуализации угроз безопасности информации и связанных с ними требований безопасности информации, а также с учетом обеспечения прослеживаемости требований при развитии (обновлении) СКИБ.

7.4 Определение технологий реализации СКИБ и ее элементов

7.4.1 Определение технологий реализации СКИБ и ее элементов следует осуществлять в процессе определения проекта и в процессе реализации проекта в соответствии с ГОСТ Р 57193.

7.4.2 Определение технологий реализации СКИБ и ее элементов следует осуществлять с учетом результатов формирования архитектуры СКИБ и определения требований, предъявляемых к СКИБ на основе ЦБ и ПБ, а также с учетом задач, подлежащих решению СКИБ или системой, для использования в составе которой создается СКИБ.

7.4.3 Технологии реализации СКИБ и ее элементов включают, но не ограничиваются следующим перечнем:

- технологии реализации аппаратных компонентов СКИБ;
- технологии реализации загрузки;
- технологии реализации встроенного ПО;
- технологии реализации системного ПО;
- технологии реализации системных и сетевых сервисов;
- технологии реализации удаленного доступа;
- технологии реализации прикладного ПО.

7.4.4 Требования к технологиям реализации следует предъявлять разработчикам и поставщикам элементов и составных частей СКИБ и в дальнейшем следует учитывать при выборе элементов и составных частей СКИБ и в работе с поставщиками.

Примечание — Элементы СКИБ в соответствии с данным определением системы также представляют собой систему, в то время как составные части СКИБ не обязательно являются системой.

7.4.5 В ходе определения технологий реализации СКИБ и ее элементов рекомендуется проводить:

- уточнение взаимосвязей между элементами СКИБ и внешними системами, их влияния на обеспечение безопасности СКИБ;
- определение технологий реализации элементов СКИБ;
- определение технологий реализации взаимодействия элементов СКИБ, включая алгоритмы и протоколы взаимодействия, необходимые характеристики взаимодействия с учетом требований, предъявляемых к СКИБ на основе ЦБ и ПБ;
- определение и реализацию мер и механизмов обеспечения безопасности информации в ходе процесса создания СКИБ;
- уточнение требований безопасности информации применительно к каждому элементу СКИБ;
- определение требований к обеспечению реализации процесса создания СКИБ и ее элементов, в том числе требований безопасной разработки ПО в соответствии с ГОСТ Р 56939;
- уточнение основных принципов развития (модернизации) СКИБ с учетом требований безопасности информации, а также требований, предъявляемых самой СКИБ и/или к системе, в интересах которой создается СКИБ;
- выбор технологий, протоколов и алгоритмов сетевого взаимодействия в интересах практической реализации безопасного доступа к СКИБ и предоставляемым ею интерфейсам;
- выбор языка программирования, методов программирования, средств разработки программ и среды исполнения в интересах практической реализации ПО элементов СКИБ.

При определении технологий реализации СКИБ и ее элементов рекомендуется учитывать принципы полноты перекрытия и эшелонирования защиты.

7.4.6 В ходе определения технологий реализации СКИБ и ее элементов рекомендуется учитывать фактор текущего или потенциального устаревания технологий для обеспечения возможности дальнейшей поддержки СКИБ, гарантии ее качества и безопасности с течением времени.

7.5 Реализация элементов СКИБ, СКИБ в целом и проведение испытаний

7.5.1 Реализацию элементов СКИБ, СКИБ в целом и проведение испытаний рекомендуется выполнять в процессе реализации, осуществляемом в соответствии с ГОСТ Р 57193.

7.5.2 Реализацию элементов СКИБ и СКИБ в целом следует осуществлять с учетом требований к технологиям реализации СКИБ (см. 7.4).

7.5.3 Реализация элементов СКИБ и СКИБ в целом должна приводить к созданию таких систем, которые удовлетворяют требованиям, предъявляемым к СКИБ на основе ЦБ и ПБ (включая распределенные и производные требования), разработанной архитектуре и проектным решениям, реализующим модели и архитектурные представления ИБ в системе.

7.5.4 В процессе реализации рекомендуется определять ограничения реализации, которые влияют на требования, архитектуру или проект, в том числе такие ограничения реализации, которые могут привести к неполной или неадекватной реализации моделей и архитектурных представлений СКИБ, к возникновению уязвимостей и к повышенному в сравнении с предположениями безопасности негативному влиянию человеческого фактора на соответствие ЦБ.

7.5.5 В процессе реализации рекомендуется обеспечивать взаимодействие СКИБ и ее элементов с поддерживающими внешними системами и сервисами, в том числе определять интерфейсы взаимодействия с обеспечивающими системами или сервисами ИБ (к примеру, сервис внешнего мониторинга или облачная инфраструктура обновлений ПО). На этом этапе должны быть доступны обеспечивающие системы или сервисы, необходимые для реализации и проведения испытаний СКИБ.

7.5.6 При реализации элементов СКИБ и СКИБ в целом следует доказывать (обосновывать), что элемент или СКИБ в целом реализованы в соответствии с требованиями, предъявляемыми к СКИБ на основе ЦБ и ПБ, разработанной архитектурой и проектными решениями, реализующими модели и архитектурные представления ИБ в системе. Также следует документировать соответствующие объективные доказательства.

7.5.7 При реализации элементов СКИБ и СКИБ в целом следует доказывать (обосновывать), что процессы реализации осуществляются с учетом требований к технологиям реализации СКИБ. Также следует документировать соответствующие объективные доказательства.

При реализации элементов СКИБ реализацию или адаптацию ПО этих элементов и СКИБ в целом рекомендуется выполнять согласно ГОСТ Р 56939. Также следует документировать объективные доказательства того, что ПО разработано в соответствии с ГОСТ Р 56939.

7.5.8 По результатам реализации элементов СКИБ и СКИБ в целом рекомендуется проводить их испытания на соответствие требованиям безопасности информации. Виды испытаний и общие требования к их проведению могут определяться нормативными правовыми актами федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, и национальными стандартами по ИБ и ЗИ.

Примечания

1 Объективное подтверждение соответствия системного элемента требованиям и характеристикам качества целесообразно получать в процессе верификации. Для объективного подтверждения того, что элемент готов к использованию в заданной эксплуатационной среде согласно требованиям заинтересованных сторон, применяется процесс валидации, в том числе валидации ЦБ.

2 Состав и документирование испытаний СКИБ рекомендуется осуществлять согласно ГОСТ Р 51583.

7.6 Сопровождение СКИБ в ходе ее эксплуатации в интересах обеспечения гарантии качества и безопасности

7.6.1 Сопровождение СКИБ в ходе ее эксплуатации в интересах обеспечения гарантии качества и безопасности осуществляется в процессе сопровождения в соответствии с ГОСТ Р 57193.

7.6.2 При выполнении работ по сопровождению СКИБ в ходе ее эксплуатации могут осуществляться следующие мероприятия:

- регистрация, анализ и классификация инцидентов информационной безопасности;
- регистрация, анализ и классификация уязвимостей СКИБ, в том числе уязвимостей ПО СКИБ (далее — уязвимости);
- информирование заинтересованных сторон, участвующих в обеспечении безопасности СКИБ, о статусе инцидентов информационной безопасности и уязвимостей;
- организация технического устранения (исправления) уязвимостей и отслеживание инцидентов до их разрешения;
- анализ тенденций в инцидентах информационной безопасности и уязвимостях в ПО для выявления систематических ошибок в применяемых конструктивных подходах.

7.6.3 По результатам выполнения указанных мероприятий рекомендуется проводить работы по обновлению ПО СКИБ и мероприятия по компенсации (блокированию) уязвимостей, которые невозможно или затруднительно исправить путем выпуска обновлений.

8 Документирование конструктивных подходов к обеспечению информационной безопасности

8.1 Реализацию конструктивных подходов к обеспечению ИБ следует документировать в «Спецификации конструктивных подходов к информационной безопасности» (далее — спецификация).

8.2 Спецификация является документом, который оформляется по результатам проектирования соответствующей системы с КИБ и содержит описание проделанной работы по обеспечению защиты (безопасности информации) данной системы.

8.3 Спецификацию рекомендуется включать в комплект документов для оценки соответствия системы с КИБ требованиям по защите информации и использовать для формирования программы и методик проведения такой оценки. При этом разработчик системы и прочие заинтересованные стороны вправе не разрабатывать спецификацию в виде отдельного документа сверх перечня документированных результатов, необходимых для оценки соответствия системы, а использовать свой перечень документируемых результатов, при условии, что таковой демонстрирует полноту рассмотрения реализации конструктивных подходов к обеспечению ИБ.

8.4 В спецификацию целесообразно включать разделы следующего содержания (но не ограничиваться ими):

- общие положения: краткое описание СКИБ (ее целевое назначение, основные функции, используемые технологии и т. д.), применяемых подходов к обеспечению конструктивной безопасности, обоснование их выбора, перечень использованных при проектировании системы нормативных документов и стандартов в области безопасности информации;
- требования по защите информации, предъявляемые к системе, с указанием ЦБ и ПБ.

Примечание — Включение требований по ЗИ, предъявляемых к системе, с указанием ЦБ и ПБ рекомендуется для обеспечения и демонстрации прослеживаемости этих требований до детализированного описания мер по их реализации;

- детализированное описание мер по реализации каждого требования по защите информации, которые были проведены в ходе проектирования соответствующей системы с указанием ее конструктивных компонентов (элементов), особенностей их архитектуры (конструкции), позволяющих сделать вывод о том, что выполнение данного требования предусмотрено конструкцией системы;
- перечень элементов системы и связей между ними с обоснованием корректности проведенной декомпозиции системы относительно ее ЦБ и ПБ;
- обобщение проделанных работ по реализации конструктивных подходов к обеспечению ИБ при проектировании системы (выводы).

При отсутствии спецификации перечисленную выше информацию рекомендуется включать в другие документы на СКИБ.

9 Применение шаблонов проектирования и разработки при создании систем с конструктивной информационной безопасностью

9.1 Назначение шаблонов проектирования систем с конструктивной информационной безопасностью

9.1.1 Шаблон проектирования и разработки — это многократно используемая схема решения типовой задачи проектирования и разработки программного и/или аппаратного обеспечения системы, ее элементов и системы в целом, применяемая в общих или ограниченных условиях.

9.1.2 Шаблоны проектирования решают типовые задачи разработки систем, в частности разработки программного обеспечения, такие как ограничения производительности компьютерного оборудования, обеспечение высокой доступности, минимизация определенных рисков, выполнение заданных ЦБ.

9.1.3 Шаблоны проектирования могут применяться как на уровне системы в целом, так и на уровне ее отдельных компонентов.

9.1.4 Некоторые шаблоны проектирования и разработки могут быть реализованы как на программном, так и на аппаратном уровне.

9.1.5 Применение шаблонов проектирования в области создания СКИБ направлено:

- на минимизацию кодовой базы, реализующей политики безопасности;
- упрощение (снижение сложности) общей архитектуры системы и внутренней структуры ее отдельных элементов, в особенности реализующих политики безопасности;
- использование политик безопасности с доказанными свойствами на основе моделей безопасности;
- повторное использование кодовой базы, реализующей политики безопасности;
- минимизацию количества функциональных связей между элементами системы;
- минимизацию потоков данных, передаваемых между элементами системы.

9.1.6 Выполнение мероприятий, перечисленных в 9.1.5, поможет в обеспечении:

- устойчивости функционирования системы в условиях воздействия вредоносных программ, осуществления НСД и эксплуатации уязвимостей;
- снижения поверхности атаки, определяемой как совокупность интерфейсов и реализующих их элементов системы, посредством непосредственного или косвенного использования которых могут реализовываться угрозы безопасному функционированию системы.

Примечание — Поверхность атаки может быть описана как множество подпрограмм (функций, модулей) программного обеспечения, обрабатывающих данные из интерфейсов, напрямую или косвенно подверженных потенциальному риску атаки. Она характеризуется набором интерфейсов/служб, которые могут быть использованы недоверенными и потенциально опасными субъектами для запуска атаки. Сведение к минимуму этого набора важно для снижения вероятности успешного запуска атаки. Поверхность атаки напрямую влияет на защищенность системы, так как при наличии достаточной компетенции у нарушителя позволяет произвести успешную атаку на систему.

9.2 Принципы создания и описания шаблонов проектирования систем с конструктивной информационной безопасностью

9.2.1 Шаблоны проектирования СКИБ рекомендуется создавать на основе общих принципов проектирования и разработки элементов СКИБ и системы в целом, указанных в 6.1, и требований безопасности, предъявляемых к информационным системам (сетям), в отношении которых законодательством или заказчиком установлены требования по ЗИ.

9.2.2 Для шаблона проектирования СКИБ рекомендуется указать следующие базовые атрибуты:

- наименование шаблона;
- назначение шаблона;
- типовые ЦБ, достигаемые при использовании данного шаблона;
- предположения безопасности;
- описание решения;
- требования к технологии разработки элементов системы;
- ограничения на применение шаблона;
- допустимые модификации шаблона.

9.2.3 Наименование шаблона должно характеризовать соответствующую проблему проектирования СКИБ (коррелировать с ней).

9.2.4 Назначение шаблона представляет собой краткую характеристику шаблона, а также описание того, когда рекомендуется применять шаблон и перечень условий его применения.

9.2.5 Типовые ЦБ включают характеристику критериев, выполнение которых достигается в системе, построенной с корректным применением предлагаемого шаблона.

Пример — Конфиденциальность данных при их передаче в сетях общего пользования, устойчивость элемента системы к кибератакам и т. п.

9.2.6 ПБ включают описание условий, необходимых для того, чтобы шаблон мог быть применен. Опционально указываются предположения и условия, при выполнении которых шаблон не может быть применен.

9.2.7 Описание решения, предлагаемого шаблоном, должно включать перечень элементов системы, реализующей шаблон, взаимосвязей между ними (абстрактное описание задачи архитектурного проектирования и того, как она может быть решена с помощью некоторого обобщенного сочетания элементов).

9.2.8 Требования к технологии разработки элементов системы описывают условия и ограничения на техническую реализацию элементов СКИБ, выполнение которых необходимо, чтобы шаблон мог быть применен.

9.2.9 Ограничения на применение шаблона описывают ограничения внешней среды, условий и контекста применения системы, при наличии которых шаблон не может быть применен или должен быть модифицирован.

9.2.10 Допустимые модификации шаблона описывают варианты реализации шаблона (перечень вариантов может быть неисчерпывающим).

9.2.11 Описание шаблона может включать поясняющие примеры использования шаблона.

9.2.12 Некоторые шаблоны могут основываться на других шаблонах проектирования, конкретизируя их ЦБ и ПБ, уточняя состав и назначение элементов системы, требования к технологии разработки и ограничения.

9.2.13 Перечень шаблонов проектирования, использованных для создания СКИБ, рекомендуется привести в документации на СКИБ (спецификации), при этом описание шаблонов может быть вынесено в отдельный документ.

9.2.14 Перечень примеров шаблонов проектирования и разработки при создании СКИБ приведен в приложении А. Этот перечень не является исчерпывающим и может являться основой для формирования других шаблонов проектирования и разработки.

Приложение А
(рекомендуемое)

Примеры типовых шаблонов проектирования программного обеспечения, обладающего свойствами конструктивной информационной безопасности

А.1 Шаблон «Монитор»

А.1.1 Назначение шаблона

Шаблон, предназначенный для организации мониторинга событий в системе, может быть использован самостоятельно для создания пассивного механизма отслеживания потоков данных, потоков управления и выполняемых в системе операций, или в составе активного механизма применения правил и политик безопасности к этим потокам и операциям.

А.1.2 Типовые ЦБ

Типовые ЦБ при применении шаблона включают:

- мониторинг и регистрацию событий в системе, важных для безопасности;
- отслеживание передачи данных в системе и анализ данных на соответствие политике безопасности по обмену данными в системе и между системой и внешним окружением;
- отслеживание системных вызовов, передачи управления и управляющих запросов в системе.

А.1.3 Предположения безопасности

ПБ включают:

- учитываемость данных/событий (accountability);
- известный и прозрачный формат данных и протокол обмена данными.

Предположения и условия, при которых шаблон не может быть применен:

- данные, которые требуется отслеживать при помощи монитора, подвергаются шифрованию, и нет возможности расшифровать их на уровне монитора (модуля анализа монитора).

А.1.4 Описание решения

Элементы системы, реализующей шаблон:

- модуль сбора данных (датчик);
- модуль анализа (детектор);
- модуль реакции;
- база данных/база знаний, используемая и пополняемая алгоритмами анализа, которые реализуются детектором.

Взаимодействие элементов монитора представлено на рисунке А.1.1.

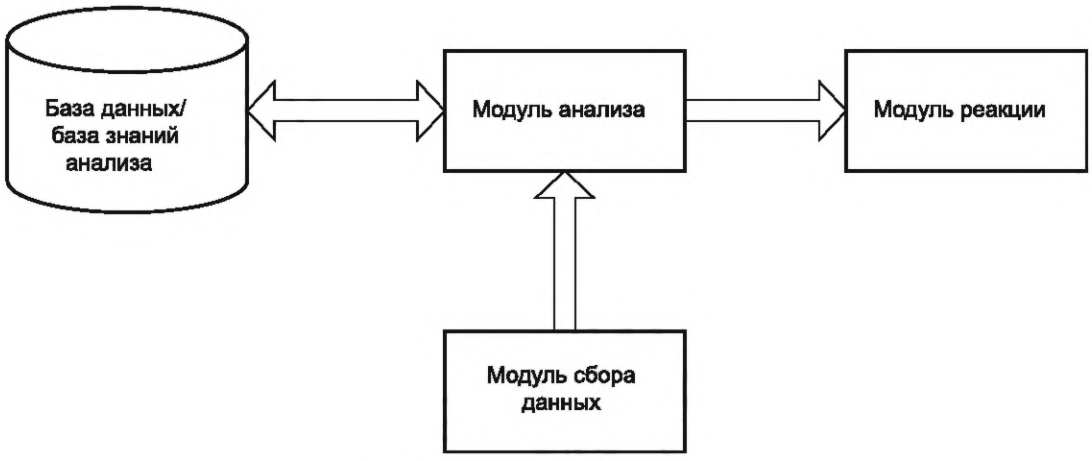

Рисунок А.1.1 — Шаблон «Монитор»

Шаблон используется самостоятельно либо как основа для других шаблонов, в том числе из числа перечисленных в настоящем стандарте. Он также может входить в состав элементов систем, построенных на основе других шаблонов, не определяя при этом их основные свойства.

А.1.5 Требования к технологии разработки элементов системы

- технология сбора данных, реализованная модулем сбора данных, должна исключать вмешательство в процессы работы системы, она должна быть реализована прозрачным для этих процессов образом, так, чтобы минимизировать влияние на временные характеристики работы системы, показатели ее производительности, надежности и безопасности;

- модуль анализа, в зависимости от потребностей мониторинга, может реализовать анализ в режиме времени выполнения или отложенный анализ на основе данных, поступающих от датчика;

- алгоритмы анализа должны минимизировать количество ошибок первого рода и ложных срабатываний, но пороговые значения и показатели производительности анализа устанавливаются индивидуально в зависимости от потребностей и назначения мониторинга.

А.1.6 Ограничения на применение шаблона

Применение шаблона может быть ограничено в системах с требованиями к выполнению в реальном времени, а также в системах с повышенными требованиями к функциональной безопасности и надежности в тех случаях, когда датчик реализует технологию перехвата потоков данных и/или потоков управления с последующей ретрансляцией этих потоков, что потенциально может повлиять на выполнение упомянутых требований.

А.1.7 Допустимые модификации шаблона

Допустимо использовать не один, а несколько датчиков или систему модулей сбора данных, поставляющих данные в модуль анализа (см. рисунок А.1.2).

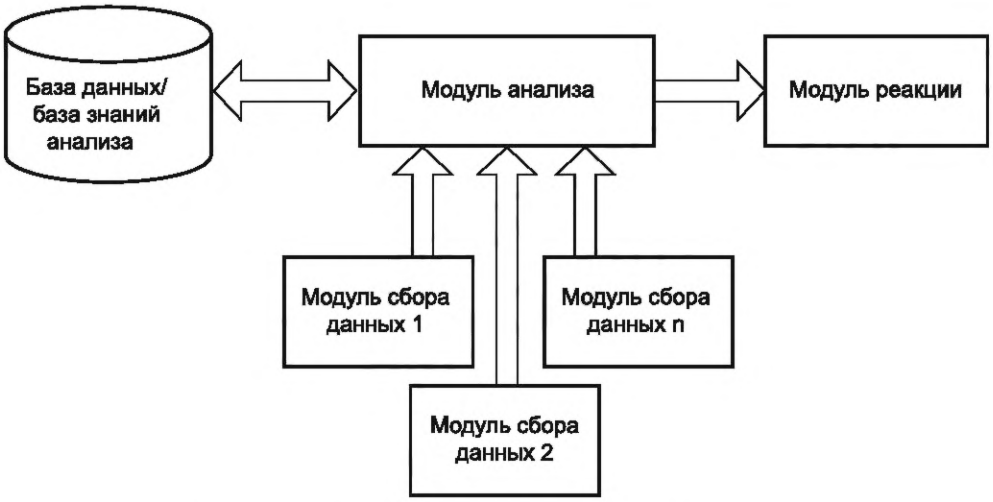

Рисунок А.1.2 — Модификация шаблона «Монитор»,
включающая несколько модулей сбора данных

Допустимо использовать несколько модулей анализа, реализующих одни и те же алгоритмы, для оптимизации и балансирования нагрузки на модуль анализа (см. рисунок А.1.3).

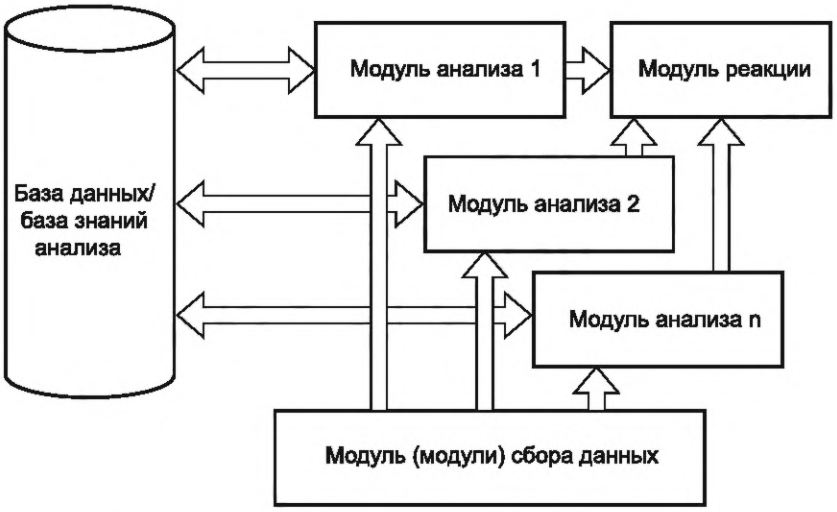

Рисунок А.1.3 — Модификация шаблона «Монитор»,
включающая несколько модулей анализа для оптимизации и балансирования нагрузки

Допустимо использовать несколько модулей анализа, реализующих несколько различных алгоритмов анализа, для получения более полных результатов анализа (см. рисунок А.1.4).

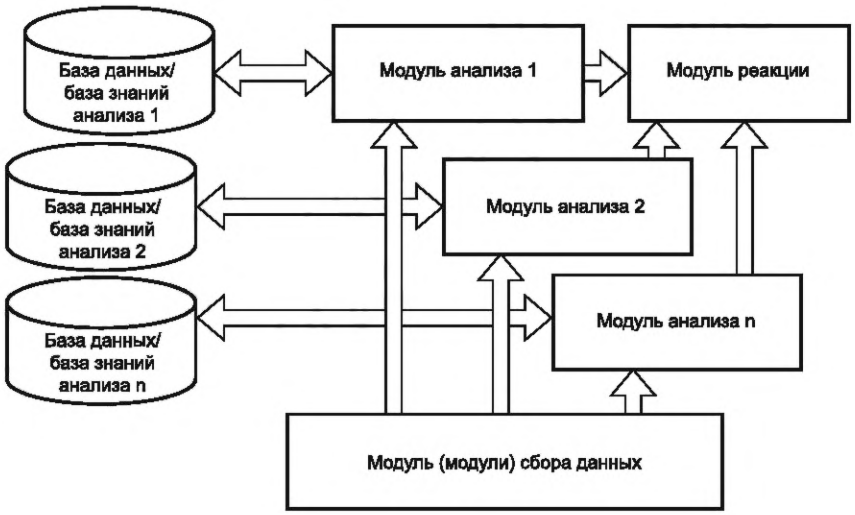

Рисунок А.1.4 — Модификация шаблона «Монитор», включающая несколько модулей анализа
для получения более полных результатов анализа

Допустимо организовывать модули анализа в иерархию, нижние уровни которой служат датчиками для верхних, для получения более точных результатов анализа (см. рисунок А.1.5).

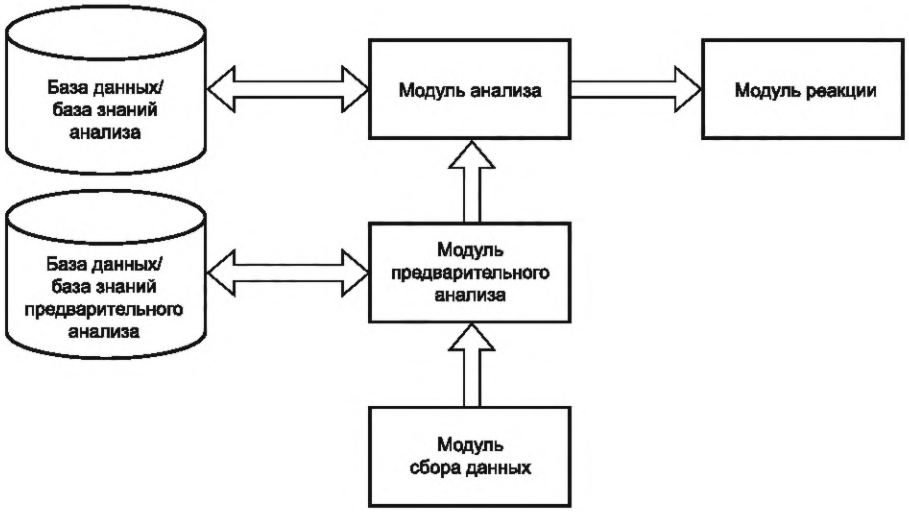

Рисунок А.1.5 — Модификация шаблона «Монитор» с иерархией модулей анализа

Допустимо использовать не один, а несколько модулей реакции, реализующей связь с внешними системами через одни и те же или различные типы каналов связи (см. рисунок А.1.6).

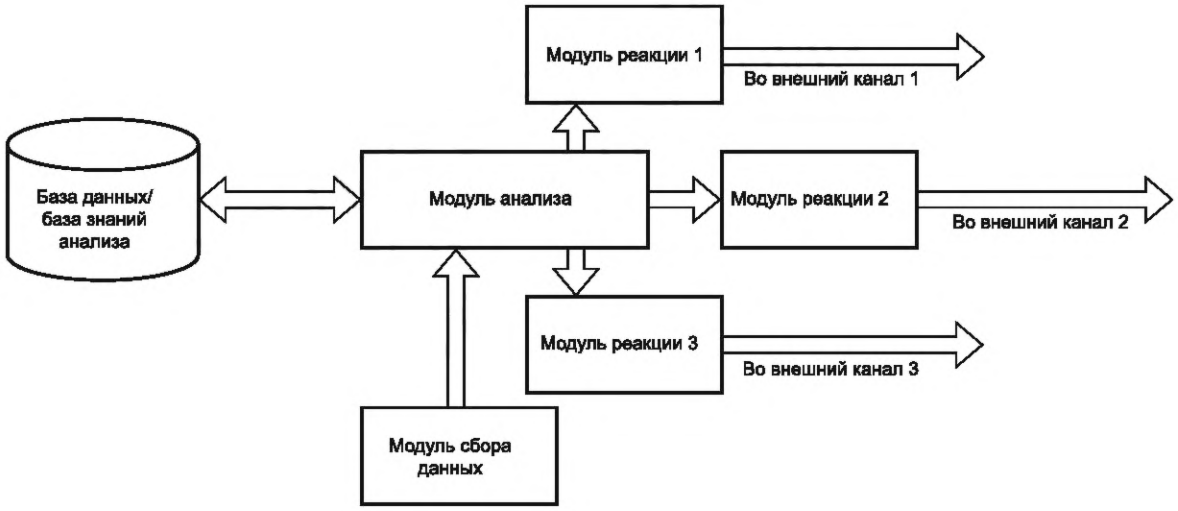

Рисунок А.1.6 — Модификация шаблона «Монитор», реализующая связь с внешними системами через различные модули реакции

Допустимо реализовывать обратную связь от внешних систем, подключенных через модуль реакции, для переконфигурирования монитора с целью обеспечения его устойчивой работы, а также для корректировки параметров сбора данных и подстройки алгоритмов анализа. Для управления и конфигурирования модулями шаблона вводится дополнительный отдельный модуль — агент управления и конфигурации, действующий внутри шаблона (см. рисунок А.1.7).

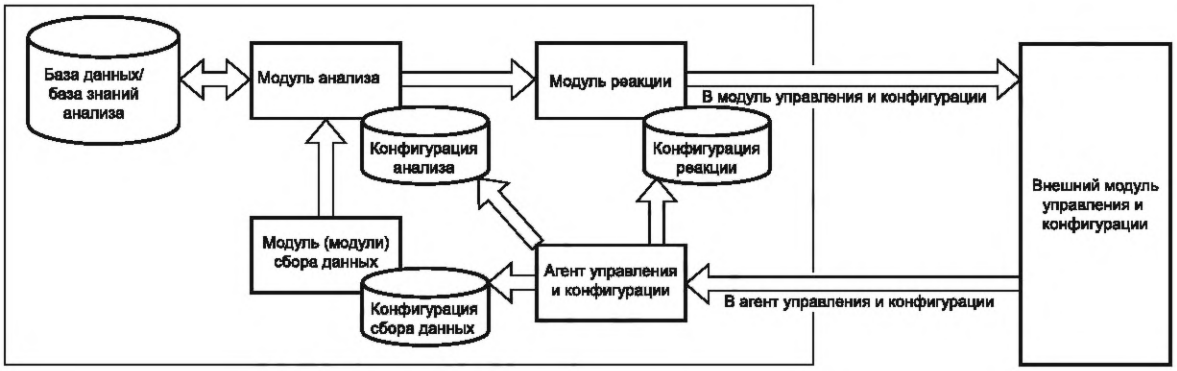

Рисунок А.1.7 — Модификация шаблона «Монитор» с обратной связью
от внешней системы для управления и конфигурирования модулями шаблона

Допустимость модификаций, не входящих в указанный перечень, должна быть обоснована при проектировании архитектуры и формировании требований, предъявляемых к системе на основе целей и предположений безопасности для этой системы.

А.2 Шаблон «Раздельное принятие и применение решений о безопасности»

А.2.1 Назначение шаблона

Шаблон «Раздельное принятие и применение решений о безопасности» предназначен для реализации активного механизма контроля доступа и фильтрации потоков данных/потоков управления на основе заданных правил и политик безопасности. Шаблон предполагает разделение механизмов принятия решения о возможности доступа или разрешении потока и применении этого решения к потокам данных, потокам управления и выполняемым в системе операциям. Это в конечном счете позволяет улучшить гибкость работы механизма контроля доступа и/или фильтрации потоков данных/потоков управления в системе и оптимизировать доказательство корректности его работы.

А.2.2 Типовые ЦБ

Типовые ЦБ при применении шаблона включают:

- обеспечение конфиденциальности и/или целостности данных или активов путем реализации контроля доступа к этим данным и активам;
- обеспечение контроля выполнения операций в системе в соответствии с заданными правилами и политиками безопасности;
- обеспечение контроля и фильтрации сообщений (таких, как пакеты данных, команды управления, системные вызовы, служебные сигналы протоколов взаимодействия), передаваемых между субъектами в системе (субъектами могут быть процессы в ОС, вычислительные системы в компьютерной сети, виртуальные машины в среде виртуализации и пр.), в соответствии с заданными правилами и политиками безопасности.

А.2.3 Предположения безопасности

ПБ включают:

- известный и прозрачный формат данных и протокол доступа к данным или активам (выполнения операций в системе, обмена сообщениями);
- отсутствие скрытых каналов передачи данных/скрытых каналов управления, использование которых позволяет обходить механизм контроля, реализуемый шаблоном «монитор безопасности».

Предположение (условие), при котором шаблон не может быть применен: данные и операции, которые требуется отслеживать и контролировать при помощи шаблона, подвергаются шифрованию, и нет возможности расшифровать их на уровне модуля анализа и принятия решений.

А.2.4 Описание решения

Элементы системы, реализующей шаблон:

- модуль анализа и принятия решений (decision point);
- модуль применения решения (enforcement point);
- правила и политики принятия решений;
- (опционально) база данных/база знаний, используемая и пополняемая алгоритмами принятия решений, которые реализуются модулем анализа и принятия решения (information point);
- (опционально) модуль управления правилами и политиками, в соответствии с которыми принимается решение о разрешении или блокировке потока данных или потока управления (операции) (authorization point).

Взаимодействие элементов монитора представлено на рисунке А.2.1.

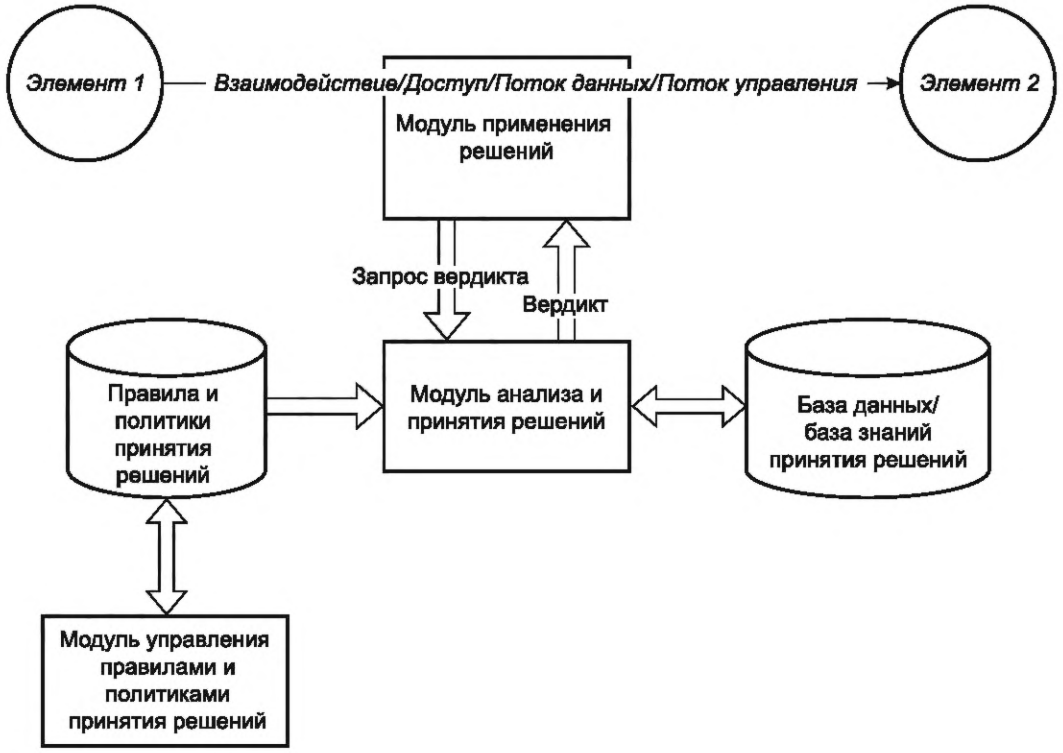

Рисунок А.2.1 — Шаблон «Раздельное принятие и применение решений о безопасности»

А.2.5 Требования к технологии разработки элементов системы

Модуль анализа и принятия решений должен реализовать анализ событий по факту их регистрации (runtime, проспективный анализ) или отложенный анализ на основе доступной информации о выполнении доступа к данным и активам, об обмене сообщениями, о выполняемых операциях в системе.

Модуль применения решений должен реализовать концепцию монитора безопасности пересылок, обеспечивая полное перекрытие потоков контролируемых данных, каналов выполнения операций и способов выполнения доступа к данным и активам. Невыполнение этого требования приводит к возникновению способов обхода контроля доступа к данным и контроля выполнения операций.

Технология применения решений, ограничивающая доступ, передачу команд управления для выполнения операций и передачу данных, должна быть реализована прозрачным для этих процессов образом так, чтобы минимизировать влияние на временные характеристики работы системы, показатели ее производительности, надежности и безопасности.

А.2.6 Ограничения на применение шаблона

Применение шаблона может быть ограничено в системах с требованиями к выполнению в реальном времени, а также в системах с повышенными требованиями к функциональной безопасности и надежности вследствие необходимости перехвата потоков данных и/или потоков управления и возможной блокировки этих потоков, что потенциально может повлиять на выполнение упомянутых требований.

А.2.7 Допустимые модификации шаблона

Допустимо использовать для реализации модуля принятия решений шаблон «Монитор», в котором:

- алгоритмы анализа предназначены для вычисления вердикта о разрешении или запрете доступа к данным или активам, разрешении или запрете выполнения операции или разрешении или запрете передачи данных;
- модуль реакции, который передает вычисленный вердикт модулю применения решения или совпадает с модулем применения решения (см. рисунок А.2.2).

Допустимо использовать модификации, описанные для шаблона «Монитор», при условии выполнения требований к модулю принятия решений и указанных выше ограничений для настоящего шаблона.

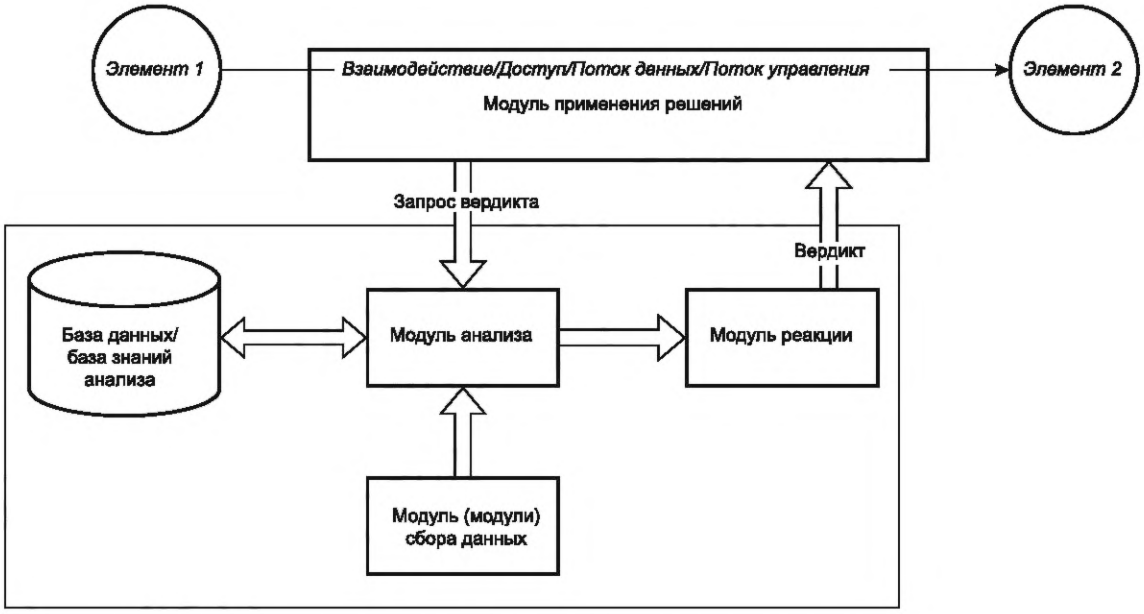

Рисунок А.2.2 — Модификация шаблона «Раздельное принятие и применение решений о безопасности» на основе шаблона «Монитор»

Допустимость модификаций, не входящих в указанный перечень, должна быть обоснована при проектировании архитектуры и формировании требований, предъявляемых к системе на основе целей и предположений безопасности для этой системы.

А.3 Шаблон «Иерархия доверия»

А.3.1 Назначение шаблона

Шаблон предназначен для организации иерархии доверия элементов в системе таким образом, что доверие множеству элементов на каждом уровне иерархии, кроме первого, основывается на последовательности доказательств целостности и аутентичности элементов предыдущего уровня, а также способности элемента (элементов) предыдущего уровня засвидетельствовать целостность и аутентичность элементов следующего уровня.

А.3.2 Типовые ЦБ

Типовые ЦБ при применении шаблона включают:

- обеспечение целостности программного обеспечения системы;
- обеспечение аутентичности программного обеспечения системы;
- обеспечение должного поведения программного обеспечения системы в соответствии со спецификациями этого поведения.

А.3.3 Предположения безопасности

ПБ включают:

- возможность обеспечения доверия одному (корневому) элементу организационными или техническими методами, реализация которых лежит вне реализации шаблона и системы, в архитектуре которой он применен. Целью организационных и технических мер обеспечения первичного доверия может быть обеспечение физической безопасности, обеспечение секретности некоторой ключевой информации и т. д.

Предположения и условия, при которых шаблон не может быть применен:

- неэффективность организационных и технических методов обеспечения доверия корневому элементу иерархии доверия.

Примечание — Под неэффективностью организационных и технических методов обеспечения доверия понимается фактическая компрометация или очевидная возможность компрометации информационной безопасности элемента (согласно сформулированным для него целям безопасности), несмотря на реализацию всех этих методов.

А.3.4 Описание решения

Элементы системы, реализующей шаблон:

- корень доверия, элемент, доверие которому обеспечивается организационными или техническими методами, реализация которых лежит вне реализации шаблона и системы, в архитектуре которой он применен; доверие должно выражаться в определенных характеристиках элемента;

- элемент или множество элементов, доверие которым обеспечивается через зависимость их явно выраженных характеристик целостности и/или аутентичности, от характеристик корня доверия;
- элемент или множество элементов, доверие которым обеспечивается через зависимость их явно выраженных характеристик целостности и/или аутентичности, от характеристик элемента (элементов) предыдущих уровней.

Взаимодействие элементов шаблона «Иерархия доверия» представлено на рисунке А.3.1.

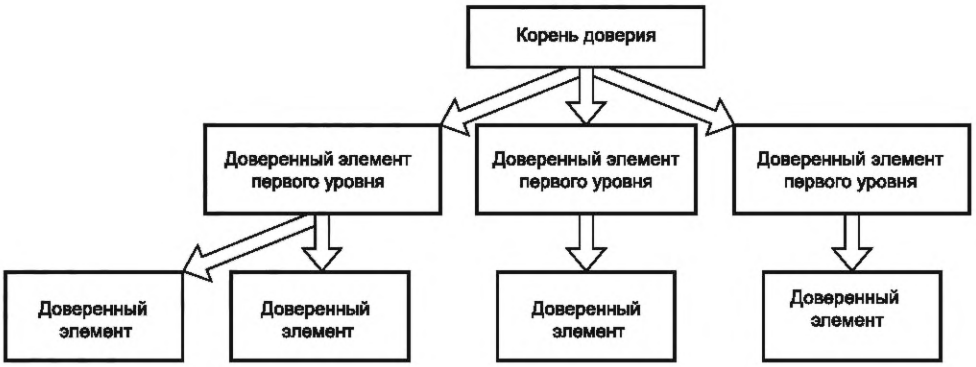

Рисунок А.3.1 — Шаблон «Иерархия доверия»

Примечание — Характеристики элемента, которые могут засвидетельствовать доверие к этому элементу, обычно представляют собой криптографические примитивы, такие как контрольная сумма или электронная подпись. Кроме этого, доверие может обеспечиваться гарантиями невозможности внесения несанкционированных изменений в состав программного обеспечения (ПО) элементов, составляющих часть иерархии доверия. Такие гарантии должны быть обеспечены в том числе архитектурой системы и процессами реализации СКИБ.

А.3.5 Требования к технологии разработки элементов системы

Требования к технологии разработки элементов системы не предъявляются.

А.3.6 Ограничения на применение шаблона

Ограничения на применение шаблона отсутствуют.

А.3.7 Допустимые модификации шаблона

Допустимо при принятии решения о доверии для отдельных элементов иерархии доверия основываться также на дополнительных условиях, не связанных исключительно с характеристиками корня доверия.

Допустимость прочих модификаций должна быть обоснована при проектировании архитектуры и формировании требований, предъявляемых к системе на основе целей и предположений безопасности для этой системы.

А.4 Шаблон «Безопасная загрузка»

А.4.1 Назначение шаблона

Шаблон предназначен для организации загрузки устройства с использованием только программного обеспечения, которому доверяет изготовитель аппаратной платформы (оборудования) системы.

А.4.2 Типовые ЦБ

Типовые ЦБ при применении шаблона включают:

- обеспечение целостности базового программного обеспечения;
- обеспечение аутентичности базового программного обеспечения.

А.4.3 Предположения безопасности

ПБ включают:

- доверие аппаратной платформе (оборудованию) системы в смысле отсутствия аппаратных и программных закладок;
- сохранение целостности и аутентичности загрузчика первой стадии загрузки и ключевой информации, хранимых в памяти только для чтения.

Предположения и условия, при которых шаблон не может быть применен:

- неэффективность организационных и технических методов обеспечения доверия оборудованию системы.

А.4.4 Описание решения

Шаблон реализуется на основе шаблона «иерархия доверия». При этом корень доверия представляет собой загрузчик первой стадии загрузки и криптографический ключ (ключи или сертификаты, содержащие ключевую информацию), хранимые на уровне аппаратной платформы и используемые для проверки целостности и аутентичности как встроенного программного обеспечения, так и ключевой информации, хранимой загрузчиком следующей стадии.

На каждом этапе загрузки операционной системы, начиная от момента подачи питания до полной загрузки и передачи управления пользователю, загрузчик на текущей стадии загрузки проверяет целостность и аутентичность программного кода, используемого на следующей стадии, путем проверки его ЭП. Таким образом может гарантироваться, что на каждой стадии загрузки устройства будет происходить проверка аутентичности и целостности программного кода. Будут загружаться только компоненты, подписанные заранее известными сертификатами, хранящимися в доверенном хранилище. У злоумышленника не будет возможности подменить код ни на одной стадии загрузки.

Элементы системы, реализующей шаблон:

- загрузчик первой стадии и корневой сертификат, хранимые в памяти, доступной только для чтения;
- загрузчик второй стадии и сертификат(ы) загрузчика второй стадии;
- загрузчик третьей стадии и сертификат(ы) загрузчика третьей стадии;
- ядро операционной системы и сертификат(ы) уровня ОС;
- элементы, отнесенные к приложениям пространства пользователя.

Взаимодействие элементов системы, реализующей шаблон при проверке электронных подписей, показано на рисунке А.4.1.

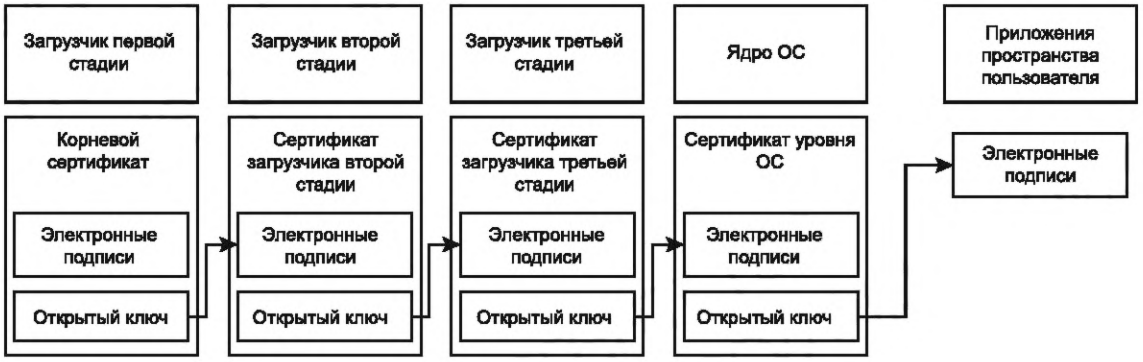

Рисунок А.4.1 — Шаблон «Безопасная загрузка»

А.4.5 Требования к технологии разработки элементов системы

Необходимо организовать хранение на уровне аппаратной платформы загрузчика первой стадии загрузки и криптографического ключа (ключей или сертификатов, содержащих ключевую информацию).

Необходима гарантия со стороны аппаратной платформы целостности и аутентичности загрузчика первой стадии и криптографического ключа (ключей или сертификатов, содержащих ключевую информацию);

Необходима реализация криптографических алгоритмов проверки аутентичности и целостности цифровых образов исполняемого кода с использованием хранимых или сгенерированных в процессе работы ключей.

А.4.6 Ограничения на применение шаблона

Ограничения на применение шаблона отсутствуют.

А.4.7 Допустимые модификации шаблона

Допустимо изменение количества стадий доверенной загрузки.

Допустимость прочих модификаций должна быть обоснована при проектировании архитектуры и формировании требований, предъявляемых к системе на основе целей и предположений безопасности для этой системы.

А.5 Шаблон «Выделенный обработчик для очистки данных»

А.5.1 Назначение шаблона

Шаблон предназначен для проверки целостности и безопасности потока данных, поступающих на вход системы, которая позволяет снизить поверхность атаки на сложные элементы системы за счет вынесения функции проверки в специальный изолированный компонент.

А.5.2 Типовые ЦБ

Типовые ЦБ при применении шаблона включают:

- защиту элементов системы от некорректных, плохо сформированных входных данных, способных нанести ущерб при злонамеренной эксплуатации уязвимостей в этих элементах.

Примечание — Под некорректными, плохо сформированными (англ.malformed) данными понимаются входные данные, специальным образом подготовленные злоумышленником таким образом, чтобы при наличии в системе уязвимости реализовать угрозу безопасности, например вызвать отказ системы, выполнить программный код, обойти механизм аутентификации и получить несанкционированный доступ и т. п;

- очистку данных от конфиденциальной информации перед передачей их внешнему недоверенному агенту, в том числе перед размещением в сетях общего доступа.

А.5.3 Предположения безопасности

ПБ включают известный формат данных и известный протокол обмена данными.

Предположения и условия, при которых шаблон не может быть применен: данные, которые требуется контролировать, подвергаются шифрованию, и нет возможности расшифровать их на уровне компонента, реализующего проверку и обработку данных.

А.5.4 Описание решения

Крупные и сложные элементы системы (такие, как базы данных, микросервисы и т. д.) обладают обширной поверхностью атаки, в связи с чем усложняется задача обеспечения безопасности и проведения проверок для установления доверия. Для уменьшения поверхности атаки рекомендуется заранее проводить проверку входных данных на их безопасность относительно этих элементов, в том числе требуется проводить необходимую очистку этих данных от лексических и синтаксических конструкций, представляющих опасность в отношении потенциальных уязвимостей в элементах системы. Подобные проверку и очистку рекомендуется вынести в отдельный, небольшой, изолированный компонент, отвечающий следующим требованиям:

- реализация монитора безопасности пересылок (режим работы «в разрыв» — перехват всего входящего потока данных без возможности обхода компонента);
- получение на вход, проверку, очистку и передачу на выход потока данных с приемлемым уровнем задержки и потери;
- применение правил проверки и очистки данных на основе обновляемого набора правил.

Элементы системы, реализующей шаблон:

- источник данных;
- получатель данных;
- компонент, реализующий проверку и обработку данных перед передачей получателю.

Взаимодействие элементов шаблона представлено на рисунке А.5.1.

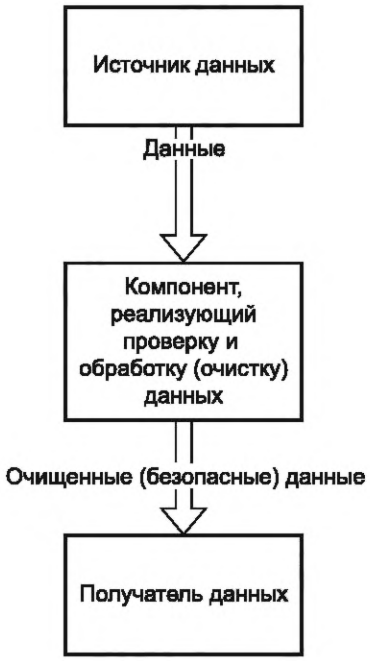

Рисунок А.5.1 — Шаблон «Выделенный обработчик для очистки данных»

А.5.5 Требования к технологии разработки элементов системы

Необходимо исключить каналы передачи данных между источником и получателем данных, которые могут быть использованы для передачи необработанных данных. Гарантии отсутствия скрытых каналов или невозможности использования таких каналов элементами системы, реализующими шаблон, могут быть предоставлены на низком уровне относительно реализации шаблона.

Необходимо обеспечить аутентичность и целостность канала передачи данных между компонентом, реализующим очистку данных, и получателем данных для исключения подделки данных и атаки «человек посередине». Гарантии аутентичности и целостности канала передачи данных могут быть предоставлены на низком уровне относительно реализации шаблона.

Необходимо реализовать подходы к обеспечению корректности производимой обработки (очистки) данных, в первую очередь методические и кооперационные подходы, обеспечивающие безопасность и корректность работы программного кода компонента, реализующего проверку и обработку (очистку) данных.

А.5.6 Ограничения на применение шаблона

Применение шаблона может быть ограничено в системах с требованиями к выполнению в реальном времени, а также в системах с повышенными требованиями к функциональной безопасности и надежности вследствие необходимости обработки данных и возможного изменения данных, что потенциально может повлиять на выполнение упомянутых требований.

А.5.7 Допустимые модификации шаблона

Допустимо применять шаблон не только для обработки (очистки) данных, но также с целью нормализации или изменения формата данных для обеспечения их корректной интерпретации получателем.

Допустимо применять шаблон с целью мониторинга безопасности данных без их обработки (очистки), только для проверки данных, как показано на рисунке А.5.2.



Рисунок А.5.2 — Шаблон «Выделенный обработчик для проверки данных»

Допустимость модификаций, не входящих в указанный перечень, должна быть обоснована при проектировании архитектуры и формировании требований, предъявляемых к системе на основе целей и предположений безопасности для этой системы.

А.6 Шаблон «Выделенный механизм поддержания состояния безопасности»

А.6.1 Назначение шаблона

Шаблон предназначен для одновременного контроля состояния безопасности системы и состояний, связанных с требуемой логикой исполнения системой некоторой функции, с принудительным переводом системы в гарантированно безопасное состояние при необходимости.

А.6.2 Типовые ЦБ

Типовые ЦБ при применении шаблона включают сохранение гарантированно безопасного состояния системы (состояния по умолчанию) при выполнении функции системы.

Пример поддержания гарантированно безопасного состояния при выполнении функции системы: при выполнении функции обновления ПО системы применение шаблона должно гарантировать безопасность (целостность и аутентичность) образов обновления либо отказ в выполнении обновления. Гарантированно безопасным состоянием в этом случае является отказ (невыполнение) обновления и сохранение текущего состояния системы в противовес некорректному или зловредному обновлению.

Другим примером поддержания гарантированно безопасного состояния является отключение небезопасных функций работы с файлами, полученными из внешних источников, до явного указания пользователем факта доверия каждому из этих файлов. Если ПО, в которое загружен недоверенный файл сложного формата (документ,

таблица, изображение), инициирует потенциально вредоносные действия (запуск скрипта, исполняемого файла, обращение к ресурсам), то эти действия будут заблокированы.

А.6.3 Предположения безопасности

ПБ включают:

- отслеживаемость параметров выполнения функции системы со стороны выделенного механизма безопасности;
- возможность полного (исчерпывающего) определения перехода системы в небезопасное состояние по этим параметрам.

Предположения и условия, при которых шаблон не может быть применен: невозможность останова выполнения функции системы внешним механизмом или вмешательства в выполнение функции для обеспечения гарантированно безопасного состояния.

А.6.4 Описание решения

Шаблон описывает способ защиты, аналогичный реализации противоаварийной защиты промышленных установок при помощи отдельно стоящих приборных систем безопасности. Обязательным условием построения такой системы является вывод контролируемого установкой процесса в результате ее срабатывания в безопасное состояние «по умолчанию». Как правило, устройства, составляющие противоаварийную защиту, создают такие управляющие воздействия, которые должны остановить нежелательное развитие событий с точки зрения функциональной безопасности. Схожим образом, выделенный элемент системы должен обеспечивать поддержание состояния информационной безопасности согласно значениям контролируемых параметров функции системы и при необходимости останавливать выполнение функции системы либо не давать сигнал на ее выполнение/продолжение.

Элементы системы, реализующей шаблон:

- источник данных или событий для выполнения функции системы;
- элемент системы, реализующий контроль состояния безопасности;
- элемент системы, реализующий функцию;
- правила и политики, которым соответствует безопасное выполнение функции;
- журнал контроля состояния безопасности.

Взаимодействие элементов шаблона представлено на рисунке А.6.1.

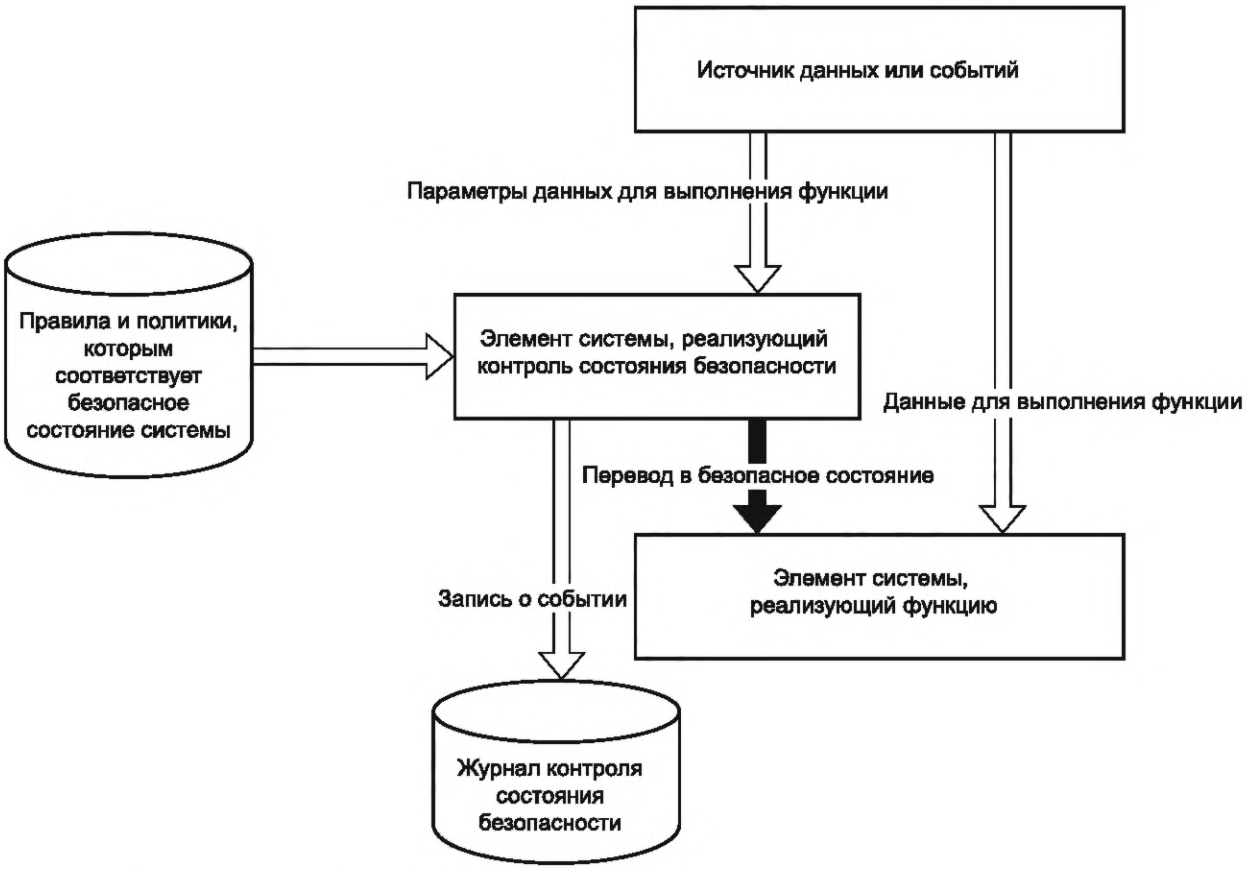

Рисунок А.6.1 — Шаблон «Выделенный механизм поддержания состояния безопасности»

Допускается вариант реализации шаблона, в котором перевод в безопасное состояние системы заменяется на разрешение выполнения функции системы. В этом случае элемент системы, реализующий функцию, остается в состоянии «по умолчанию» до получения такого разрешения.

Пример конкретного применения шаблона к функции обновления системы показан на рисунке А.6.2. Элементы системы, реализующей шаблон:

- источник образов (бинарных образов, данных, исходных текстов, скриптов обновления) для обновления системы;
- элемент системы, реализующий контроль целостности обновлений;
- элемент системы, реализующий обновление ПО;
- правила и политики, которым соответствует безопасное обновление;
- журнал обновлений.

При выполнении обновления элемент системы, реализующий контроль целостности, применяет к полученным данным правила проверки целостности и аутентичности полученных образов для обновления. При успешной проверке элемент, выполняющий обновление, получает сигнал на выполнение, в противном случае (в том числе в случае сбоя при проверке) система остается в безопасном состоянии.

Выделение компонента, осуществляющего проверку, позволяет снизить возможность компрометации функции системы через атаку отказа в обслуживании на функцию проверки безопасности.

Взаимодействие элементов шаблона представлено на рисунке А.6.2.

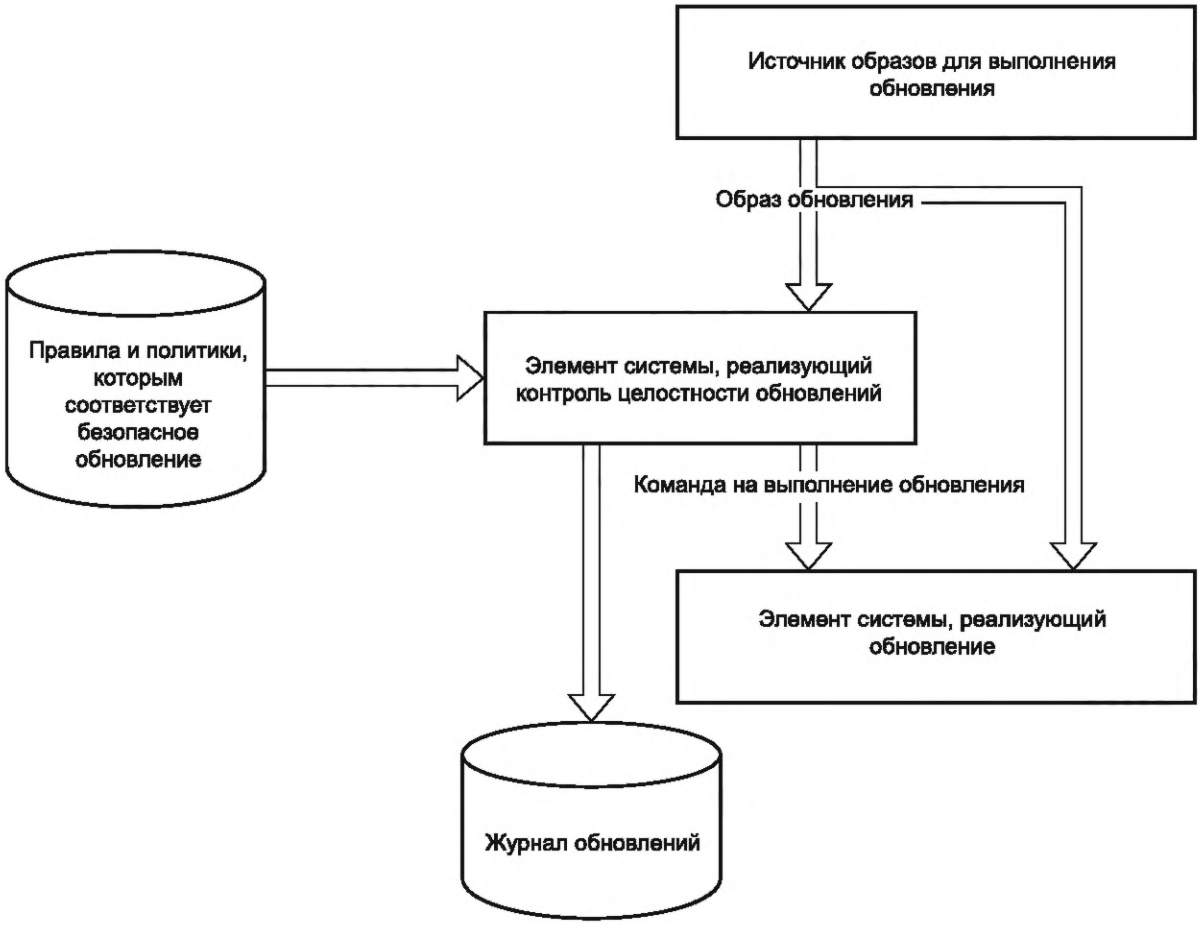

Рисунок А.6.2 — Шаблон «Выделенный механизм поддержания состояния безопасности при обновлении ПО»

А.6.5 Требования к технологии разработки элементов системы

Необходимо обеспечить аутентичность, целостность и доступность канала, используемого для перевода в безопасное состояние, для исключения подделки данных и атаки «человек посередине». Гарантии аутентичности, целостности и доступности канала передачи данных могут быть предоставлены на низком уровне относительно реализации шаблона.

Необходимо реализовать подходы к обеспечению корректности контроля состояния безопасности, в первую очередь методические и кооперационные подходы, обеспечивающие безопасность и корректность работы программного кода компонента, реализующего контроль состояния безопасности.

А.6.6 Ограничения на применение шаблона

Применение шаблона может быть ограничено в системах с требованиями к выполнению в реальном времени, а также в системах с повышенными требованиями к функциональной безопасности и надежности вследствие необходимости обработки данных и возможного изменения данных, что потенциально может повлиять на выполнение упомянутых требований.

А.6.7 Допустимые модификации шаблона

Допустимо реализовать несколько элементов системы, реализующих контроль состояния безопасности по различным параметрам, обеспечив запрет выполнения функции системы по каждому каналу перевода в безопасное состояние и усилив тем самым контроль.

Допустимо реализовать несколько элементов системы, реализующих контроль состояния безопасности по различным параметрам, обеспечив выполнение функции системы по одновременному разрешению от двух или более компонентов (реализация принципа разделения обязанностей).

Допустимость модификаций, не входящих в указанный перечень, должна быть обоснована при проектировании архитектуры и формировании требований, предъявляемых к системе на основе целей и предположений безопасности для этой системы.

А.7 Шаблон «Разделение потоков данных на уровне драйвера ресурсов»

А.7.1 Назначение шаблона

Шаблон предназначен для разделения потоков данных для ограничения доступа к ресурсам на уровне драйвера ресурсов с целью обеспечения конфиденциальности, целостности и взаимного невлияния потоков данных. Примером применения шаблона является уменьшение поверхности атаки на ВФС за счет разделения одной ВФС на несколько: например, отдельно для работы с внешней сетью и отдельно для работы с внутренней сетью и блочным устройством.

А.7.2 Типовые ЦБ

Типовые ЦБ при применении шаблона включают:

- конфиденциальность данных, обрабатываемых в системе;
- целостность данных, обрабатываемых в системе;
- обеспечение режима доступа к специальным ресурсам (к примеру, единоразовый доступ к криптографическим ключам в процессе загрузки системы, однонаправленный доступ к конфигурационным данным и т. п.).

А.7.3 Предположения безопасности

ПБ включают:

- корректность работы драйверов и системного ПО, лежащего в основе реализации драйверов разделяемых ресурсов;
- отсутствие или ничтожность скрытых каналов доступа и управления разделяемыми ресурсами на уровне нижележащих драйверов, системного ПО, кода прошивок устройств и оборудования.

Предположения и условия, при которых шаблон не может быть применен: наличие альтернативного канала доступа к ресурсу, который позволяет обходить установленные на основе реализации шаблона ограничения доступа.

А.7.4 Описание решения

Элементы системы, реализующей шаблон:

- субъекты доступа к ресурсам;
- драйверы доступа к ресурсам различных типов, количество элементов определяется числом ресурсов каждого типа, требующих различных политики и/или режима доступа;
- пул ресурсов каждого типа согласно количеству элементов-драйверов ресурсов для обеспечения разделения ресурсов, пул ресурсов определяется согласно возможностям адресации ресурсов (диапазон адресов в памяти, выделенный канал связи, адресуемый как целое, и т. п.).

Взаимодействие элементов шаблона представлено на рисунке А.7.1.

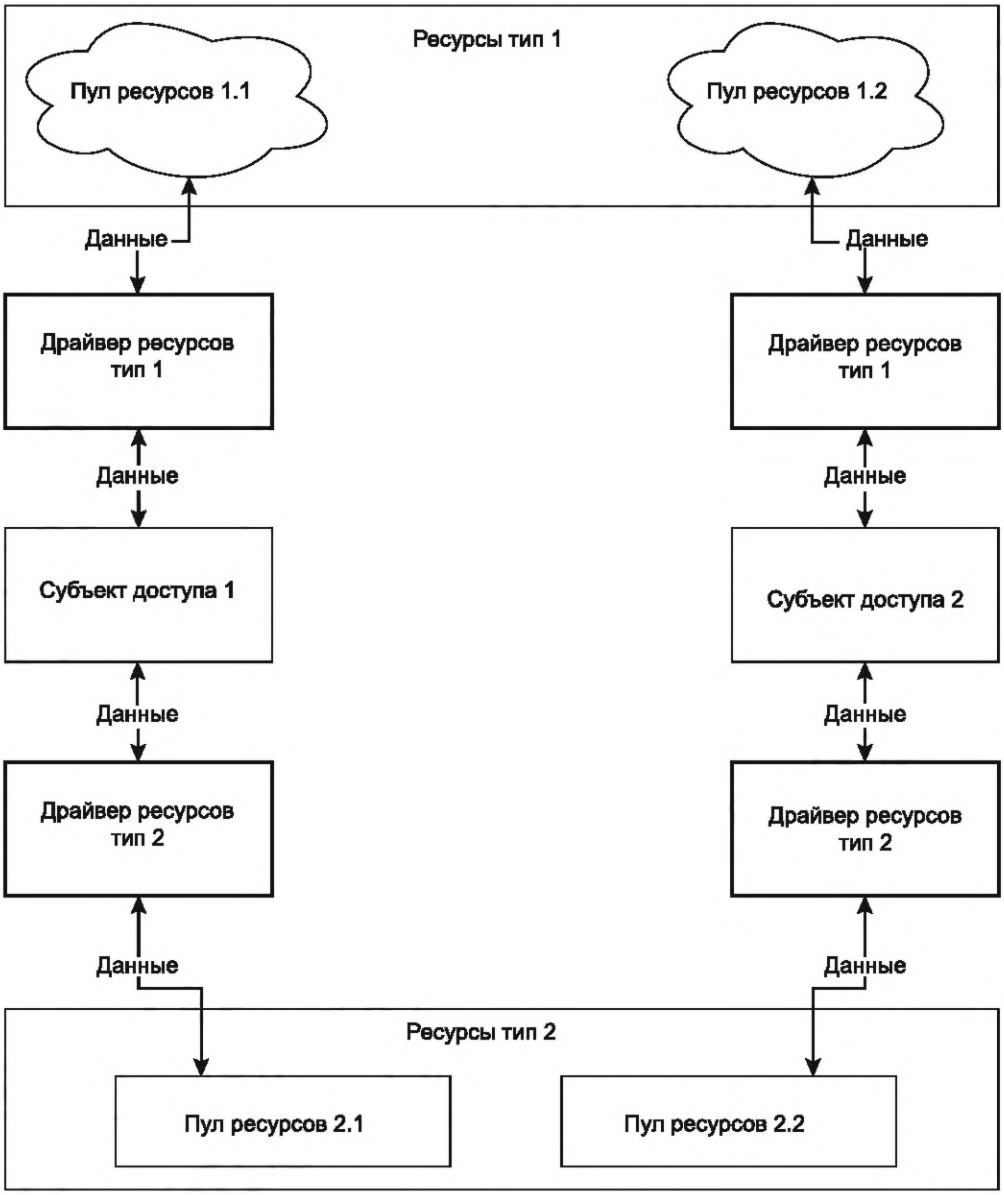

Рисунок А.7.1 — Шаблон «Разделение потоков данных на уровне драйвера ресурсов»

В качестве поясняющего примера рассмотрим ВФС, работающие с сетью и с блочными устройствами, которые должны быть разделены и помещены в разные домены безопасности.

Субъекты и/или процессы, обрабатывающие данные из сетей, приходящие на разные контроллеры или адаптеры, должны использовать разные ВФС.

Компрометация сетевой ВФС не должна приводить к компрометации субъектов и процессов, с которыми она взаимодействует.

Рассмотрим угрозы безопасности на примере приложения с одной ВФС, которая обеспечивает сразу несколько типов взаимодействия:

- недоверенный компонент обменивается данными с публичной и локальной сетью;
- полученная из публичной и локальной сети информация записывается в хранилище данных на жестком диске;
- доверенный компонент обменивается высокоцелостными данными с жестким диском;
- недоверенный компонент обменивается данными с жестким диском и уведомляет об этом доверенный компонент.

Для выполнения первого требования нужно реализовать подход разделения одной ВФС на несколько, а точнее, на четыре (ВФС для работы с публичной сетью для обоих субъектов или процессов, ВФС для работы с локальной сетью для обоих субъектов или процессов).

Чтение и запись данных из хранилища данных осуществляют два компонента: «Доверенный компонент» и «Недоверенный компонент». Для каждого из них требуется отдельная ВФС.

Второе требование достигается автоматически при выполнении первого требования, поскольку разделение сети на несколько подсетей в данном примере не рассматривается.

Далее, для выполнения третьего требования должны быть реализованы независимые хранилища информации. Для этого:

- к драйверу блочного устройства необходимо подключить драйвер раздела;
- в драйвере раздела прописать два выделенных диапазона адресуемых блоков, один для субъекта «Доверенный компонент», второй для «Недоверенный компонент»;
- обеспечить взаимодействие субъекта или процесса только с предопределенным для него выделенным диапазоном адресуемых блоков посредством задания ограничения (политики безопасности) для драйвера раздела.

Для выполнения последнего требования необходимо убедиться, что доверенные компоненты, взаимодействующие с файловым хранилищем, не обращаются напрямую к сетевому драйверу, взаимодействующему с публичной сетью.

Пример показан на рисунке А.7.2.

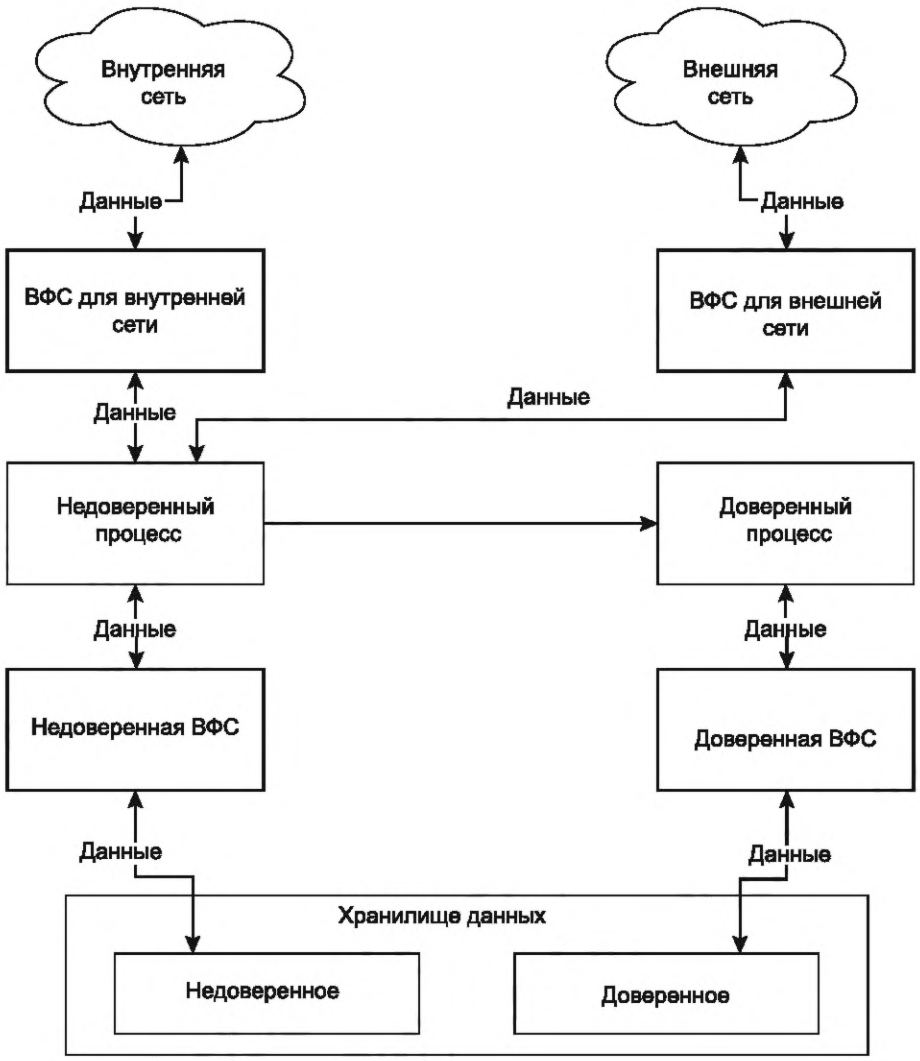

Рисунок А.7.2 — Пример использования шаблона «Разделение потоков данных на уровне драйвера ресурсов»

А.7.5 Требования к технологии разработки элементов системы

Необходимо реализовать разделение на разных уровнях драйверов: драйвер ВФС или драйвер раздела, чем ниже уровень, на котором проводится разделение, тем проще осуществить доказательство невлияния потоков данных.

Необходимо реализовать разделение пула ресурсов для привязки к ним раздельных драйверов доступа, что должно быть обеспечено технической возможностью адресации ресурсов определенного типа и невозможностью драйвера адресовать ресурсы того же типа вне заданного для него пула адресов.

Необходимо реализовать подходы к обеспечению корректности работы драйверов ресурсов и драйверов ниже этого уровня (если они доступны для контроля), в первую очередь методические и кооперационные подходы, обеспечивающие безопасность и корректность работы драйверов.

А.7.6 Ограничения на применение шаблона

Ограничения на применение шаблона определяются ограничениями на производительность и требованиями доступности ресурсов, доступ к которым реализуется с использованием шаблона

А.7.7 Допустимые модификации шаблона

Допустимые модификации шаблона определяются через количество типов ресурсов и политики разграничения доступа к этим ресурсам.

Допустимость модификаций, не входящих в указанный перечень, должна быть обоснована при проектировании архитектуры и формировании требований, предъявляемых к системе на основе целей и предположений безопасности для этой системы.

А.8 Шаблон «Терминатор TLS»

А.8.1 Назначение шаблона

Шаблон предназначен для безопасной передачи данных между системой и удаленным сервером по протоколу TLS с использованием изолированного доверенного компонента.

А.8.2 Типовые ЦБ

Типовые ЦБ при применении шаблона включают:

- обеспечение конфиденциальности, целостности и аутентичности данных при взаимодействии с удаленным сервером;
- защиту ключевой информации (закрытых ключей шифрования, сертификатов закрытого ключа) от раскрытия.

ЦБ могут уточняться в зависимости от области применения шаблона, к примеру, целью может быть обеспечение целостности и аутентичности данных бинарных образов программных модулей при выполнении процедуры обновления системы.

А.8.3 Предположения безопасности

ПБ включают:

- отсутствие известных уязвимостей в криптографических алгоритмах, используемых в криптонаборах TLS;
- отсутствие известных уязвимостей в алгоритмах и технических средствах генерации криптографических ключей и сертификатов;
- проведение должных испытаний программного обеспечения, реализующего алгоритмы и протокол TLS, и иные мероприятия по обеспечению соответствия его поведения спецификациям.

Предположения и условия, при которых шаблон не может быть применен:

- неэффективность организационных и технических методов обеспечения доверия к реализации протокола TLS в изолированном компоненте;
- неэффективность организационных и технических методов обеспечения доверия к взаимодействию защищаемого ресурса и изолированного компонента, реализующего TLS;
- наличие множественных уязвимостей в реализации протокола TLS и в реализации протоколов, на основе которых он работает.

А.8.4 Описание решения

Шаблон основан на реализации другого шаблона проектирования «Разделение потоков данных на уровне драйвера ресурсов» и реализует раздельный доступ к сетевому интерфейсу и к двум разделам файлового хранилища. Один из разделов файлового хранилища предназначен для ключей и других секретов шифрования, второй — для прочих данных, обмен которыми происходит по TLS. Это позволяет реализовать следующие требования:

- изоляция и раздельное хранение доверенных данных (сертификатов и ключей шифрования) и недоверенных (данные, полученные по сети);
- гарантированное подключение компонента, реализующего транспортную логику, только к тому серверу, с которым производилась аутентификация;
- минимизация возможностей компрометации ключей и секретов шифрования посредством эксплуатации уязвимостей.

Элементы системы, реализующей шаблон:

- элемент, реализующий обмен данными с внешней сетью (к примеру, реализующий ВФС для внешней сети);
- элемент, реализующий обмен данными с недоверенным хранилищем данных (ВФС);
- элемент, реализующий обмен данными с доверенным хранилищем данных (ВФС);
- файловое хранилище для общих данных системы (недоверенное);

- файловое хранилище для секретов шифрования (доверенное);
- элемент, выполняющий терминацию TLS (инкапсуляцию в протокол TLS).

Терминатор TLS (точнее, тот его элемент, который выполняет непосредственно терминацию TLS) является монитором безопасности пересылок между приложением и внешней сетью. Для снижения сложности рекомендуется реализовать этот элемент из двух независимых компонентов, один из которых отвечает за установку соединения, а другой реализует передачу данных.

С точки зрения приложения терминатор TLS выглядит как обычный сетевой интерфейс, обращение к которому осуществляется с помощью стандартных запросов (к примеру, POSIX-совместимых системных вызовов — connect, accept и т. п.).

Взаимодействие элементов шаблона представлено на рисунке А.8.1.



Рисунок А.8.1 — Шаблон «Терминатор TLS»

А.8.5 Требования к технологии разработки элементов системы

Элемент, реализующий терминацию TLS, должен реализовать концепцию монитора безопасности пересылок, обеспечивая полное перекрытие потоков данных в/из сети.

Поскольку шаблон реализуется на основе шаблона «разделение потоков данных на уровне драйверов устройств», применяются требования к технологии, определенные для базового шаблона.

Необходимо реализовать подходы к обеспечению корректности реализации протокола TLS, в первую очередь методические и кооперационные подходы, обеспечивающие безопасность и корректность работы программного кода, реализующего установление соединения и обмен данными по протоколу TLS.

А.8.6 Ограничения на применение шаблона

Поскольку шаблон реализуется на основе шаблона «разделение потоков данных на уровне драйверов устройств», применяются ограничения, определенные для базового шаблона.

А.8.7 Допустимые модификации шаблона

Допустимость модификаций шаблона должна быть обоснована при проектировании архитектуры и формировании требований, предъявляемых к системе на основе целей и предположений безопасности для этой системы.

А.9 Шаблон «Безопасная регистрация»

А.9.1 Назначение шаблона

Шаблон предназначен для организации безопасного хранения журналов в системе, а именно для обеспечения их целостности, аутентичности и доступности.

А.9.2 Типовые ЦБ

Типовые ЦБ при применении шаблона: обеспечение целостности, аутентичности и доступности сообщений в журналах событий.

А.9.3 Предположения безопасности

ПБ включают доверие ядру операционной системы в смысле обеспечения целостности, аутентичности и доступности данных в выделенном буфере ядра.

Предположения и условия, при которых шаблон не может быть применен: наличие альтернативного канала доступа к журналам доступа, который позволяет обходить установленные на основе реализации шаблона ограничения доступа.

А.9.4 Описание решения

Элементы системы, реализующей шаблон:

- монитор событий;
- буфер ядра;
- агент сбора данных о событиях;
- хранилище данных о событиях.

Взаимодействие элементов шаблона представлено на рисунке А.9.1

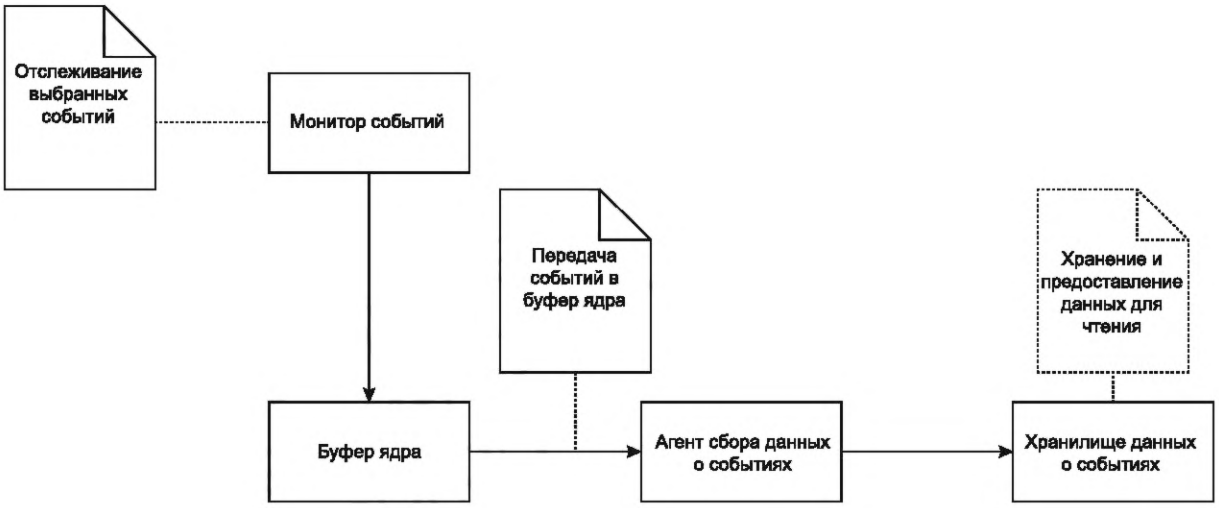

Рисунок А.9.1 — Шаблон «Безопасная регистрация»

Монитор событий (в том числе это может быть монитор безопасности) реализуется в соответствии с шаблоном «Монитор». Модуль реакции монитора отслеживает события аудита и автоматически отправляет их в буфер ядра через интерфейс по записи.

Агент сбора данных о событиях через специальный интерфейс по чтению (доступ к нему есть только у этого элемента) забирает данные о событиях из буфера ядра и отправляет их в хранилище.

Хранилище данных о событиях обрабатывает полученные события аудита и сохраняет в определенном формате. События могут выводиться в консоль, записываться на диск. Возможна реализация автоматического реагирования на определенные события аудита.

Разделение потоков данных по чтению и записи должно производиться с использованием шаблона «Разделение потоков данных на уровне драйвера ресурсов».

А.9.5 Требования к технологии разработки элементов системы

Поскольку шаблон реализуется на основе шаблона «Монитор», применяются требования к технологии, определенные для базового шаблона.

Поскольку шаблон реализуется на основе шаблона «Разделение потоков данных на уровне драйверов устройств», применяются требования к технологии, определенные для базового шаблона.

А.9.6 Ограничения на применение шаблона

Известны следующие ограничения на применение шаблона:

- поскольку шаблон реализуется на основе шаблона «Разделение потоков данных на уровне драйверов устройств», применяются ограничения, определенные для базового шаблона;

- поскольку шаблон реализуется на основе шаблона «Монитор», применяются ограничения, определенные для базового шаблона;

- регистрация на основе предлагаемого шаблона с задействованием буфера ядра применяется для важных событий безопасности в системе, в том числе таких, которые относятся к разделению доменов и соответствующим политикам безопасности в системе.

А.9.7 Допустимые модификации шаблона

Допустимо иметь несколько элементов-хранилищ данных с целью резервирования или хранения данных в различных форматах, с различными целями.

Допустимость модификаций, не входящих в указанный перечень, должна быть обоснована при проектировании архитектуры и формировании требований, предъявляемых к системе на основе целей и предположений безопасности для этой системы.

А.10 Шаблон «Безопасное обновление»

А.10.1 Назначение шаблона

Шаблон предназначен для организации безопасного обновления системы и приложений через канал связи с удаленным сервером обновлений.

А.10.2 Типовые ЦБ

Типовые ЦБ при применении шаблона: обеспечение целостности и аутентичности данных обновлений (бинарных образов, скриптов, конфигурационных данных обновлений и т. п.) в условиях доставки этих данных через каналы связи сетей общего доступа.

А.10.3 Предположения безопасности

Предположения безопасности отсутствуют.

Предположения и условия, при которых шаблон не может быть применен: наличие альтернативного канала доступа к хранилищу данных, который позволяет обходить установленные на основе реализации настоящего шаблона ограничения доступа.

А.10.4 Описание решения

Шаблон должен отвечать следующим требованиям:

- реализация шаблона должна обеспечивать аутентификацию сервера обновлений;

- реализация шаблона должна обеспечивать возможность отката обновления в случае, если оно неработоспособно;

- реализация шаблона должна обеспечивать проверку целостности, аутентичности и актуальности обновления;

- уязвимости реализации должны быть минимизированы, в том числе, с использованием методов разработки безопасного программного обеспечения (по ГОСТ 56939).

Элементы системы, реализующей шаблон:

- сервер обновлений — удаленный сервер, содержащий данные обновлений (бинарных образов, скриптов, конфигурационных данных обновлений и т. п.);

- элемент, реализующий обмен данными с внешней сетью (к примеру, реализующий ВФС для внешней сети);

- менеджер обновлений — элемент, управляющий процессом обновления и предоставляющий пользователю интерфейс управления обновлениями;

- загрузчик обновлений — элемент, обеспечивающий связь с сервером обновлений и загрузку обновления на устройство. Может выполнять проверку наличия обновлений при соответствующих настройках менеджера обновлений.

- аутентификация сервера должна осуществляться по безопасному каналу связи, к примеру, организованного посредством реализации шаблона «Терминатор TLS»;

- временное хранилище обновления и связанных с ним метаданных (номер версии, ЭП, контрольная сумма) используется для изоляции обновления на время проверок;

- верификатор данных — элемент, осуществляющий проверку обновления в соответствии с заложенной логикой и обеспечивающий вынесение вердикта (положительный или отрицательный) по результатам проверки файла обновления и связанных с ним метаданных. Типовые проверки могут включать: целостность (проверка контрольной суммы), аутентичность (проверка ЭП), номер версии;

- хранилище данных;

- монитор;

- установщик обновлений — компонент, осуществляющий запись в хранилище данных и должную установку обновления.

Разграничение доступа к временному хранилищу данных и хранилищу данных обеспечивается реализацией шаблона «Разделение потоков данных на уровне драйвера ресурсов».

Элемент «Монитор» реализуется на основе шаблона «Монитор».

Взаимодействие элементов шаблона представлено на рисунке А.10.1.

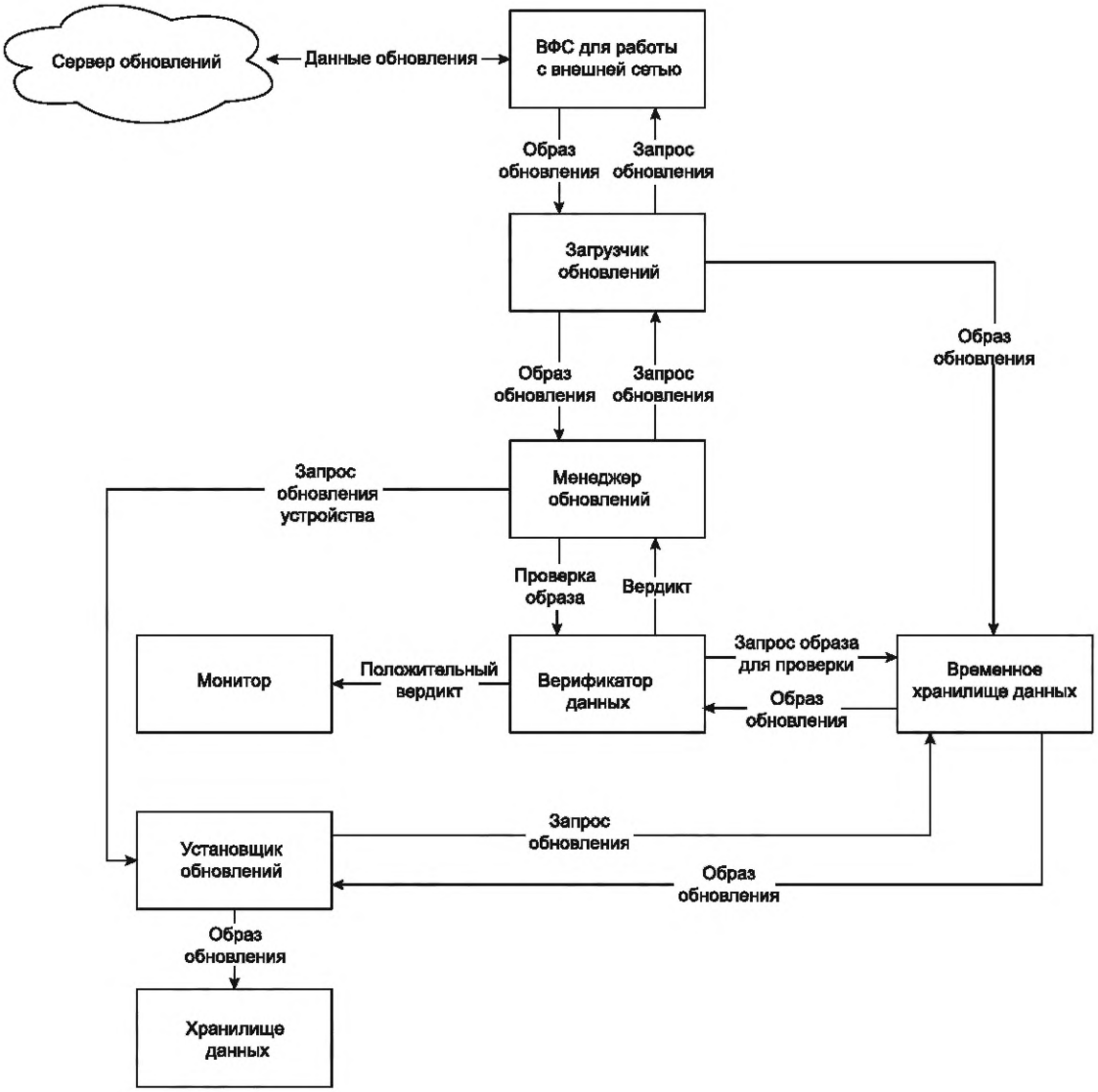

Рисунок А.10.1 — Шаблон «Безопасное обновление»

Система может находиться в одном из трех состояний конечного автомата:

1) Хранилище доступно для записи файла обновления. В этом состоянии временное хранилище данных доступно только для записи;

2) Хранилище запечатано. В этом состоянии временное хранилище данных доступно только для чтения и только компонентом верификатор данных. После верификации данные во временном хранилище данных могут считаться доверенными (целостными, аутентичными, актуальными);

3) Хранилище верифицировано. В этом состоянии данные во временном хранилище данных доступны только для чтения компонентом Установщик данных.

Алгоритм установки обновления, реализуемый на основе шаблона:

шаг 1. Менеджер обновлений запрашивает проверку наличия обновлений у загрузчика обновлений;

шаг 2. Загрузчик обновлений проверяет наличие обновлений и при наличии актуальной версии скачивает обновление и сопутствующую мета-информацию во временное хранилище данных;

шаг 3. Загрузчик обновлений уведомляет менеджера обновлений о загрузке файла обновления во временное хранилище данных;

шаг 4. После записи обновления во временное хранилище данных система переходит в состояние запечатывания временного хранилища данных;

шаг 5. Менеджер обновлений запрашивает у верификатора данных проверку файла обновления и метаданных;

шаг 6. Верификатор данных читает данные из временного хранилища данных, проводит проверки и в случае положительного вердикта передает данные в монитор; система переходит в состояние возможности передачи данных из временного хранилища данных;

шаг 7. В случае положительного вердикта верификатор данных информирует менеджер обновлений о том, что образ корректный;

шаг 8. Менеджер обновлений передает в Установщик обновлений команду на обновление устройства;

шаг 9. Установщик обновлений читает данные из временного хранилища данных, выбирает один из разделов для записи обновлений, записывает файл обновлений и инициирует процедуру установки обновления. После передачи файла обновления временное хранилище данных форматируется и переходит в стартовое состояние.

А.10.5 Требования к технологии разработки элементов системы

Поскольку шаблон включает элемент «Монитор», применяются требования к технологии, определенные для базового шаблона «Монитор».

Поскольку шаблон реализуется на основе шаблона «Разделение потоков данных на уровне драйверов устройств», применяются требования к технологии, определенные для базового шаблона.

Необходимо реализовать подходы к обеспечению корректности верификации данных обновления, в первую очередь методические и кооперационные подходы, обеспечивающие безопасность и корректность работы программного кода компонента, реализующего проверку целостности, аутентичности и актуальности данных обновления.

А.10.6 Ограничения на применение шаблона

Поскольку шаблон реализуется на основе шаблона «Разделение потоков данных на уровне драйверов устройств», применяются ограничения, определенные для базового шаблона и шаблона «Монитор».

А.10.7 Допустимые модификации шаблона

Допустимость модификаций шаблона должна быть обоснована при проектировании архитектуры и формировании требований, предъявляемых к системе на основе целей и предположений безопасности для этой системы.

А.11 Шаблон «Шлюз однонаправленной передачи данных»

А.11.1 Назначение шаблона

Шаблон предназначен для организации однонаправленной передачи данных из внутренней сети во внешнюю.

Примечание — Шаблон с некоторой модификацией может использоваться для организации однонаправленной передачи данных из внешней сети во внутреннюю. Модификация исключает использование исходного шаблона.

А.11.2 Типовые ЦБ

Типовые ЦБ при применении шаблона включают:

- отсутствие влияния агентов во внешней сети на внутреннюю сеть;
- обеспечение целостности ресурсов во внутренней сети;
- защиту внутренней компьютерной сети от атак.

Примечание — Шаблон с модификацией для организации однонаправленной передачи данных из внешней сети во внутреннюю используется в том случае, если целью является обеспечение конфиденциальности ресурсов во внутренней сети.

А.11.3 Предположения безопасности

ПБ включают доверие к элементу системы, обеспечивающему передачу данных (для ПО программного-аппаратного шлюза — к драйверу сетевой карты и сетевому стеку ОС).

Предположения и условия, при которых шаблон не может быть применен: существование альтернативных каналов связи внешней и внутренней сети.

А.11.4 Описание решения

Элементы системы, реализующей шаблон:

- агент источника данных;
- агент получателя данных;
- сервис обработки данных;
- монитор безопасности.

Примечание — Монитор безопасности является необязательным, но частым элементом системы, реализующей шаблон, поэтому здесь показано его типовое расположение. Монитор безопасности должен быть реализован изолированно так, чтобы только отслеживать происходящее в системе, но не быть подверженным прямой атаке, поэтому его взаимодействие с остальными элементами сведено к минимальному.

Разграничение доступа к внутренней и внешней сети обеспечивается использованием физически раздельных сетевых карт или реализацией шаблона «Разделение потоков данных на уровне драйвера ресурсов».

Элемент «Монитор» реализуется на основе шаблона «Монитор».

Взаимодействие элементов шаблона представлено на рисунке А.11.1.

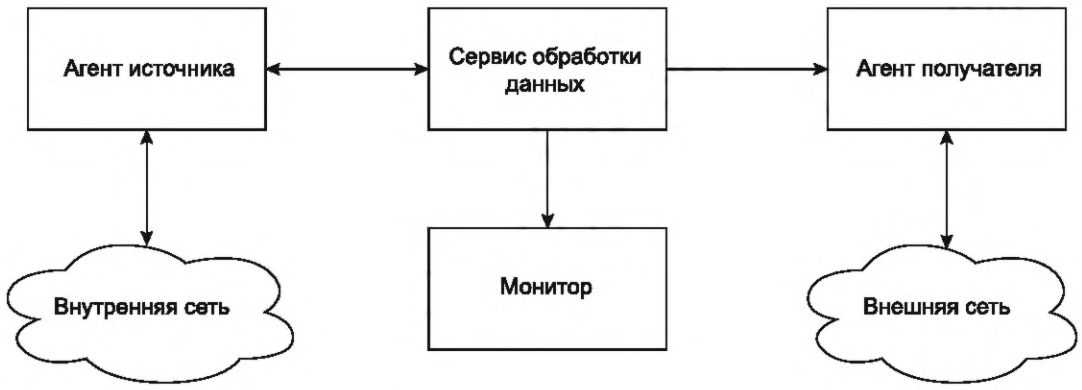

Рисунок А.11.1 — Шаблон «Шлюз однонаправленной передачи данных»

Алгоритм осуществления однонаправленной передачи данных на основе шаблона:

шаг 1. Агент источника передает в сервис обработки данных информацию, которую требуется передать агенту-получателю;

шаг 2. Сервис обработки данных устанавливает маршрут передачи между агентом источника и агентом получателя, монитор отслеживает факт выполнения запроса и его параметры как минимум, получая информацию от сервиса обработки данных. Монитор может также независимо получать данные для отслеживания запросов из внутренней и внешней сети, к примеру, на интерфейсах взаимодействия агентов источника и получателя с внутренней и внешней сетью соответственно;

шаг 3. Агент получателя принимает данные и отправляет их во внешнюю сеть.

При попытке передачи любых данных из агента-получателя в сервис обработки данных срабатывает политика, запрещающая выполнение передачи данных. Попытки установления прямого соединения с внешней сетью и запросы из внешней сети отслеживаются монитором.

Примечание — Шаблон с модификацией для организации однонаправленной передачи данных из внешней сети во внутреннюю предполагает смену направления потока данных и смену ролей агента источника и агента получателя.

А.11.5 Требования к технологии разработки элементов системы

Поскольку шаблон включает элемент «Монитор», применяются требования к технологии, определенные для базового шаблона «Монитор».

Поскольку шаблон реализуется на основе шаблона «Разделение потоков данных на уровне драйверов устройств», применяются требования к технологии, определенные для базового шаблона.

А.11.6 Ограничения на применение шаблона

Поскольку шаблон реализуется на основе шаблона «Разделение потоков данных на уровне драйверов устройств», применяются ограничения, определенные для базового шаблона и шаблона «Монитор».

А.11.7 Допустимые модификации шаблона

Допустимость модификаций шаблона должна быть обоснована при проектировании архитектуры и формировании требований, предъявляемых к системе на основе целей и предположений безопасности для этой системы.

А.12 Шаблон «Динамическое ограничение доступа к данным»

А.12.1 Назначение шаблона

Шаблон предназначен для организации динамического ограничения доступа к данным (обеспечение невозможности одновременного доступа к доверенному и недоверенному хранилищу данных). Шаблон может быть применен для организации однократного доступа к доверенным данным в одном сеансе работы системы (между перезагрузками).

Наименование шаблона происходит от термина «динамическое разделение обязанностей», когда решение о предоставлении доступа субъекту (например, процессу или пользователю) принимается на основании уже выполненных операций доступа в текущем сеансе авторизации этого субъекта в системе.

А.12.2 Типовые ЦБ

Типовые ЦБ при применении шаблона включают обеспечение определенного режима доступа к данным.

А.12.3 Предположения безопасности

ПБ включают доверие ядру безопасности, реализующему применение политики контроля доступа.

Предположения и условия, при которых шаблон не может быть применен: существует альтернативный канал доступа к данным, который позволяет обходить установленные на основе реализации шаблона ограничения доступа.

А.12.4 Описание решения

Элементы системы, реализующей шаблон:

- источник данных;
- получатель данных;
- доверенное хранилище;
- недоверенное хранилище;
- монитор безопасности.

Взаимодействие элементов шаблона представлено на рисунке А.12.1.

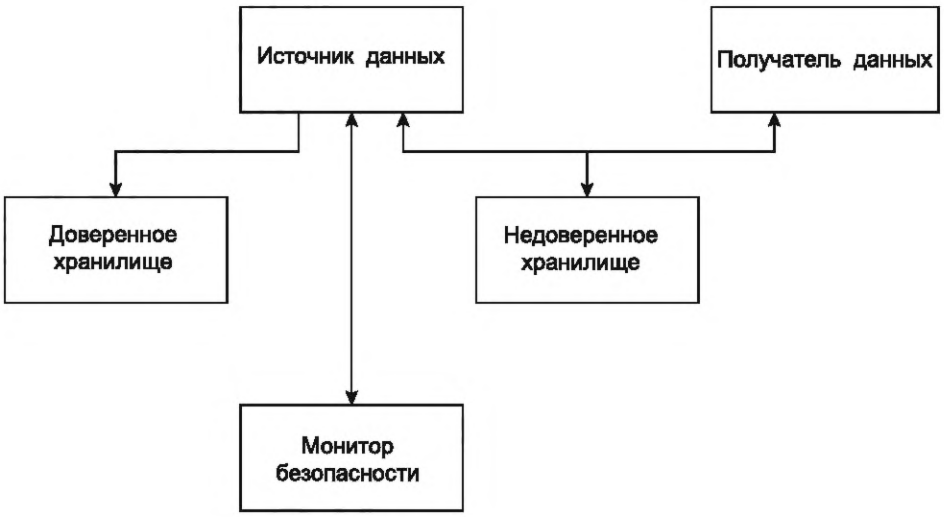

Рисунок А.12.1 — Шаблон «Динамическое ограничение доступа к данным»

Алгоритм динамического ограничения доступа к данным на основе шаблона требует создания конечного автомата, который позволяет системе находиться в одном из двух состояний:

- защищенном, когда источник данных имеет доступ только к доверенному хранилищу и не имеет доступ к внешней сети и другим компонентам системы;
- рабочем, когда ни один компонент не имеет доступа к доверенному хранилищу даннных.

Алгоритм представляет собой следующую последовательность шагов:

шаг 1. Система находится в защищенном состоянии. Источник данных имеет доступ к доверенному хранилищу и получает необходимые для работы конфигурации;

шаг 2. Источник совершает попытку обращения к недоверенному хранилищу;

шаг 3. Срабатывает политика, переводящая систему в рабочее состояние. Доступ к доверенному хранилищу запрещен для всех компонентов системы.

Система в защищенном состоянии представлена на рисунке А.12.2.

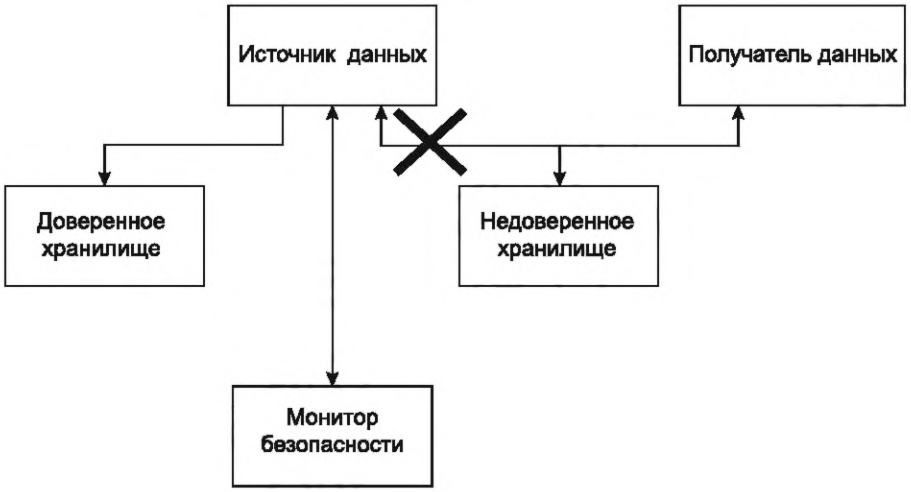

Рисунок А.12.2 — Шаблон «Динамическое ограничение доступа к данным», система в защищенном состоянии

Система в рабочем состоянии представлена на рисунке А.12.3.

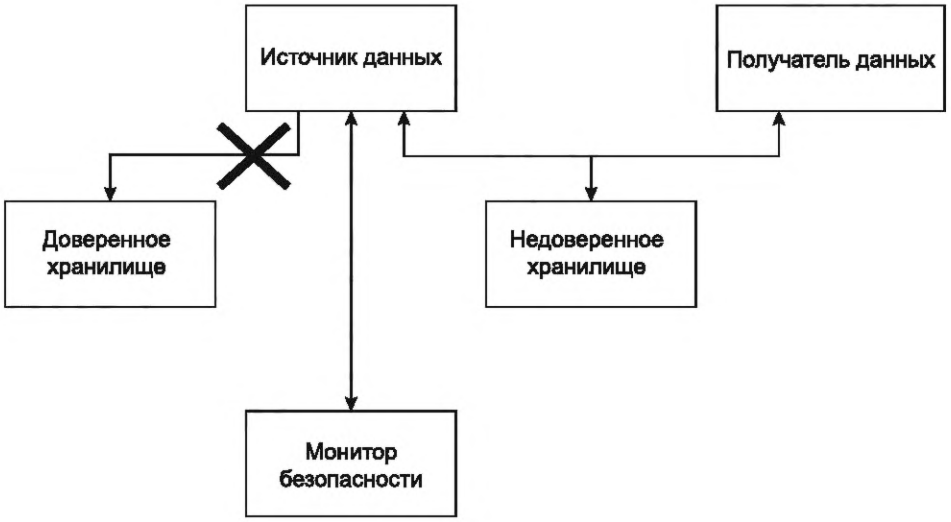

Рисунок А.12.3 — Шаблон «Динамическое ограничение доступа к данным», система в рабочем состоянии

А.12.5 Требования к технологии разработки элементов системы

Поскольку шаблон включает элемент «Монитор», применяются требования к технологии, определенные для базового шаблона «Монитор».

Поскольку шаблон реализуется на основе шаблона «Разделение потоков данных на уровне драйверов устройств», применяются требования к технологии, определенные для базового шаблона.

А.12.6 Ограничения на применение шаблона

Поскольку шаблон реализуется на основе шаблонов «Разделение потоков данных на уровне драйверов устройств» и «Монитор», применяются ограничения, определенные для данных базовых шаблонов.

А.12.7 Допустимые модификации шаблона

Допустимость модификаций шаблона должна быть обоснована при проектировании архитектуры и формировании требований, предъявляемых к системе на основе целей и предположений безопасности для этой системы.

УДК 004.05:006.354 ОКС 35.020

Ключевые слова: методология разработки, система, программное обеспечение, конструктивная информационная безопасность, требования безопасности информации, архитектура программного обеспечения, доверенная система

Редактор *Е.Ю. Митрофанова*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 09.06.2025. Подписано в печать 18.06.2025. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5,58. Уч.-изд. л. 5,12.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru