

Февраль 2026

ГОСТ Р 72118-2025

Методология создания систем с
конструктивной информационной
безопасностью

Обзор

Екатерина Рудина

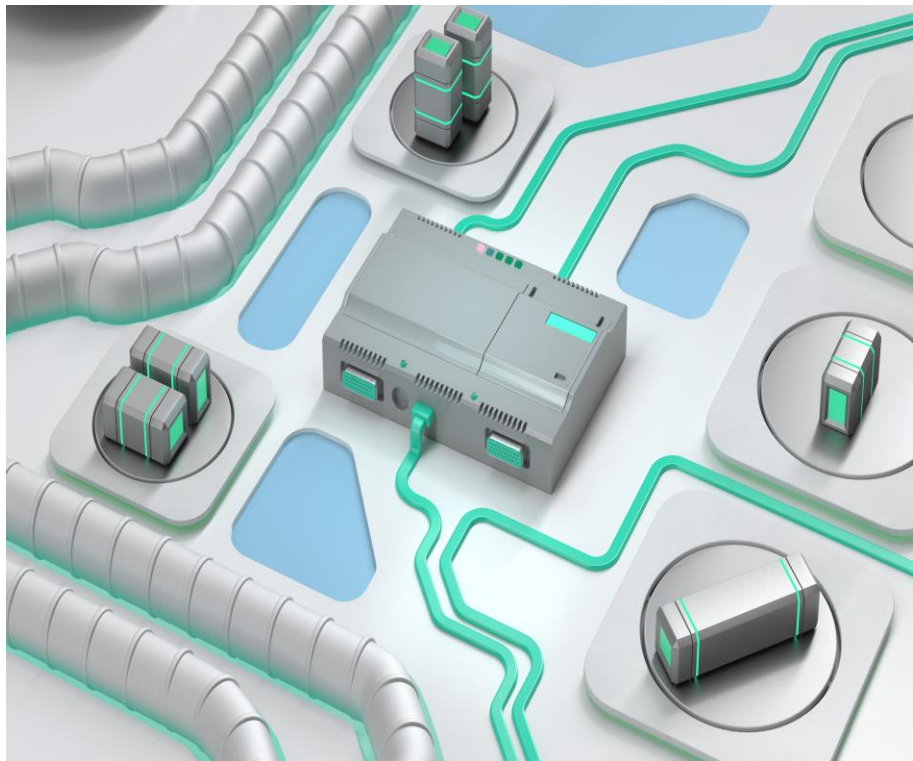
_____ Future Technologies
_____ Kaspersky

Конструктивная информационная безопасность

Удачные решения

Роль архитектуры и проектирования

Роль технологий и материалов



Назначение: обеспечить быстрое перемещение людей и грузов автомобильным транспортом

Ключевая цель/ограничение: безопасность жизни и здоровья людей, безопасность среды

Механизмы: ограничения скорости, дорожные знаки, ПДД

Каждая дорога (система) имеет свое назначение и устройство, плохое или хорошее

Дорожные знаки в чистом поле не работают

_____«конструкция» дороги обеспечивает
основу для безопасного движения и позволяет
использовать дорожную инфраструктуру
эффективнее

Архитектура, технологии и материалы

Принимаются во внимание
«законы физики» и сложность
(в т.ч. ненадежность)
связанных объектов

_____ Меры безопасности
соотносятся с назначением
системы

_____ (проектирование)

_____ Отбойники не должны
быть сделаны из картона

_____ (анализ проекта, выбор
технологии)

_____ «Дорожное покрытие»
важно для скорости и
безопасности

_____ (контроль качества)

Security by design

Удачные решения
Роль архитектуры и проектирования
Роль технологий и материалов

“ Конструктивная информационная безопасность

**безопасность, достигнутая
применением конструктивных
подходов**

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

Напомним, что такое цели безопасности

9

**набор согласованных
между собой
критериев,
выполнение которых
позволяет считать
систему безопасной**

**Системный подход в
информационной безопасности,
при котором цели и требования
безопасности рассматриваются
методично и согласованно с
функциональными требованиями
к системе**

Как определить цели безопасности

и как установить
приоритеты

**Заинтересованные стороны
(стейкхолдеры)**

Нормативные требования

**Аналогии, предметная область,
эвристики**



Методы проектирования

- Методический
(Method-based, rational)
- Кооперационный
(Participative)
- Нормативный
(Normative)
- Heuristic
(Эвристический)

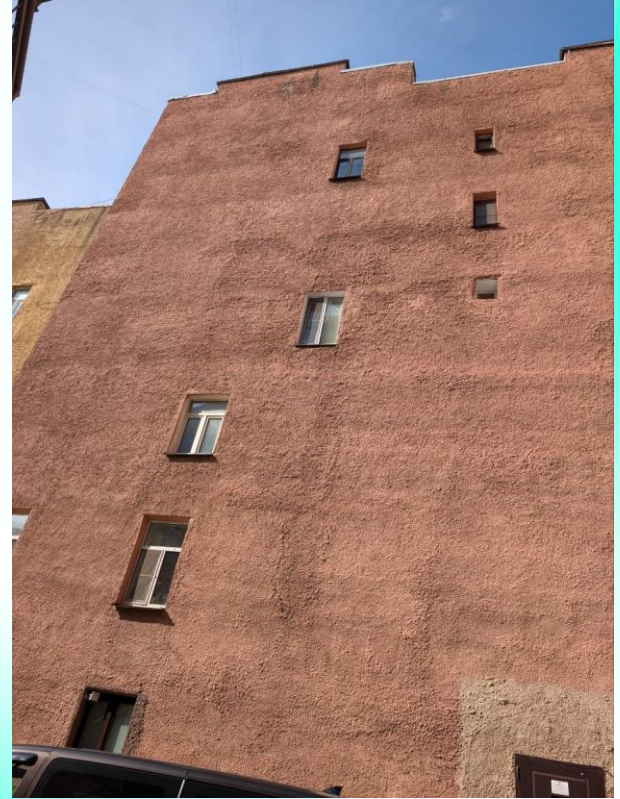
Виды архитектуры, важные для ИБ

(1) Информационная

(2) Безопасность

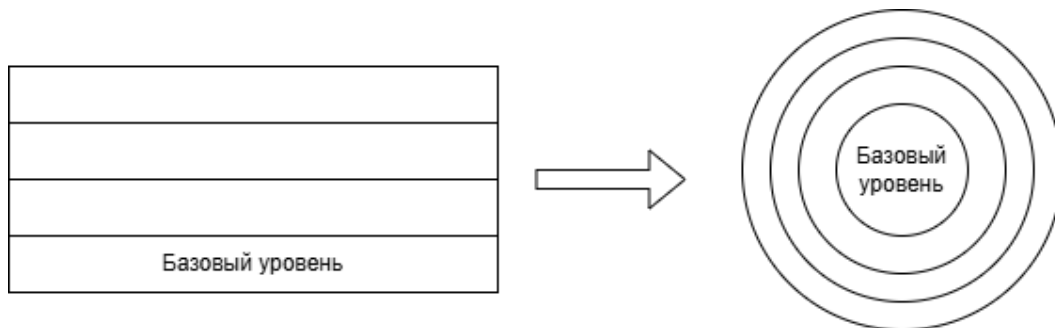
- **Правила работы с информацией в реальном мире**
- **Правила обеспечения безопасности в реальном мире**

```
____iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```



Уровневая архитектура

_____Разделение системы на уровни целостности (реже – конфиденциальности)



_____Ограничение потоков данных по записи «сверху вниз»,
ядро доверия – в центре или на нижнем уровне

Корень доверия и иерархия доверия

_____ Корень доверия, или базовый элемент безопасности – гарантированная целостность помогает удостоверять остальные элементы

_____ Как правило, на корне доверия выстраивают топологию доверия «звезда» или «иерархия»

Доменная архитектура

_____ Ее корни не в информационных моделях, а в функциональных областях (авионика)

_____ Основана на выделении доменов для изоляции сбоев

_____ Используется не только для обеспечения целостности среды, но и для реализации сложных политик

О стандарте ГОСТ Р 72118

Методология создания систем с
конструктивной ИБ

Содержание стандарта

ГОСТ Р 72118-2025

Методология создания систем с
конструктивной информационной
безопасностью

Введение

1. Область применения
2. Нормативные ссылки
3. Термины и определения
4. Сокращения и обозначения
5. Общие положения
6. Реализация подходов к созданию систем с конструктивной информационной безопасностью
7. Содержание основных работ при создании систем с конструктивной информационной безопасностью
8. Документирование конструктивных подходов к обеспечению информационной безопасности
9. Применение шаблонов проектирования и разработки при создании систем с конструктивной информационной безопасностью

Приложение А Примеры типовых шаблонов
проектирования ПО

Введение





Предисловие

Введение

...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),

_____ Отсылка на ГОСТ 57193 – системы систем, системная инженерия
_____ Наиболее общее применение, в т.ч. к киберфизическим системам



Предисловие

Введение

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

_____ Пример – малоресурсные устройства, в т.ч. интернета вещей

1. Область применения

2. Нормативные ссылки

Что делает: описывает, как разрабатывать системы с конструктивной информационной безопасностью.

К чему применяется: к системам, которые используют информационные технологии для управления различными процессами: информационными, производственными, технологическими. Это могут быть новые или модернизируемые системы

Для кого: определяет требования и даёт рекомендации по разработке для заказчиков и разработчиков систем, реализующих информационную технологию. Он будет полезен для систем, которые планируется полностью модернизировать, и для которых нельзя применить внешние средства защиты.

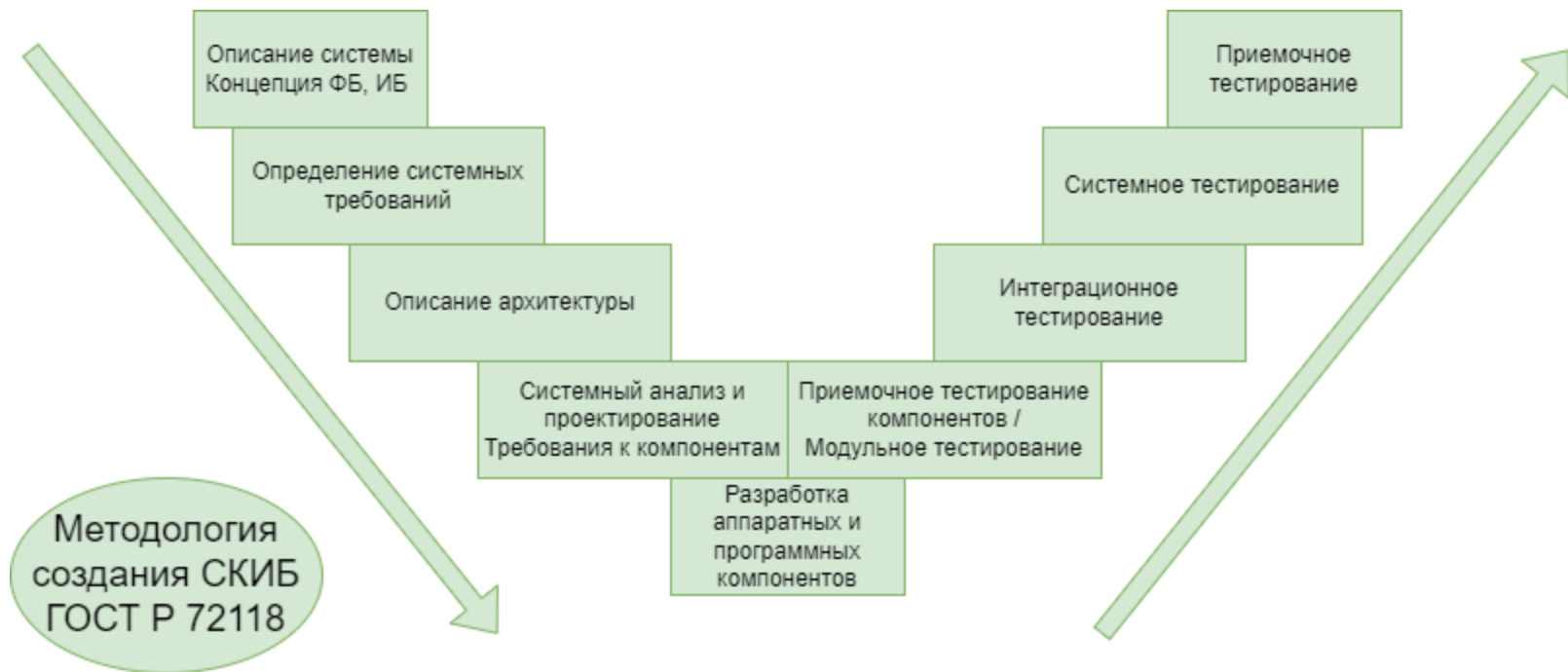
Если система является программным обеспечением, то вместе с этим стандартом можно использовать **ГОСТ Р 56939 («Разработка безопасного программного обеспечения»)**. Эти стандарты согласованы для совместного применения.

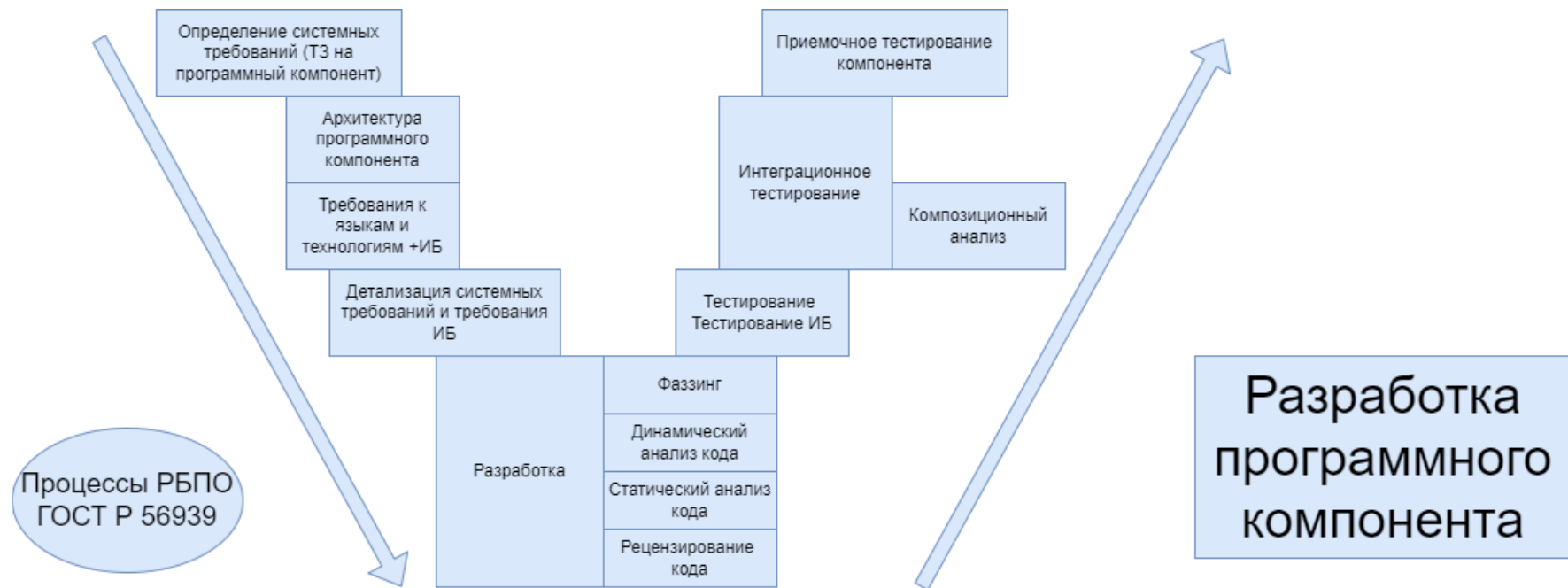
ГОСТ РБПО является может применяться безотносительно ГОСТ по СКИБ и наоборот. Но лучше всего, когда РБПО составляет часть конструктивного подхода

Стандарт можно применять для создания **автоматизированных систем в защищенном исполнении (АСЗИ)**. Важно понимать, что не каждая АСЗИ является системой с конструктивной информационной безопасностью.

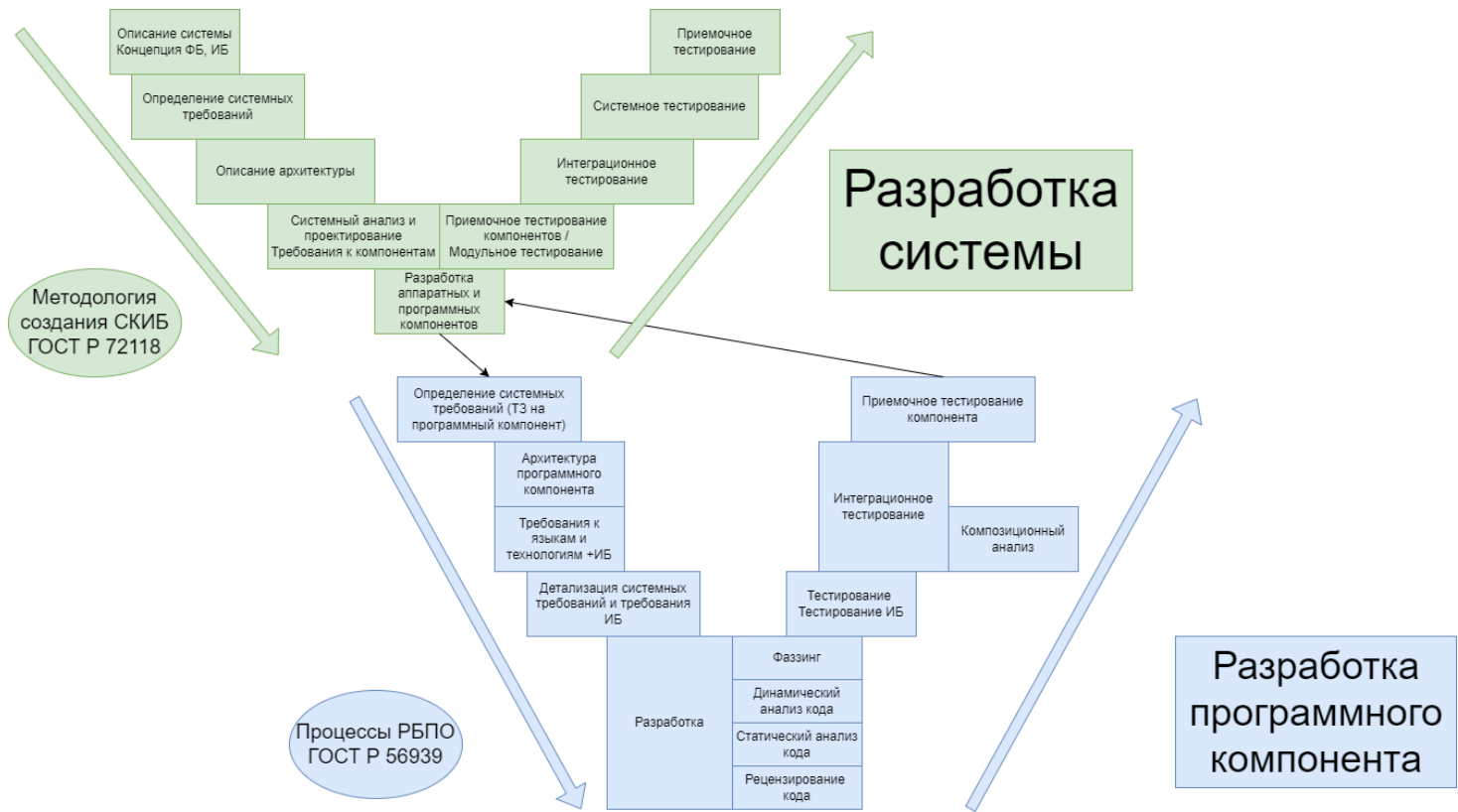
Пример создания системы с конструктивной ИБ

28





Разработка программного компонента как части системы с конструктивной ИБ



3. Термины и определения

4. Сокращения и обозначения

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

[ГОСТ Р 57193–2016, пункт 4.1.44]

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]

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

[ГОСТ Р 51583–2014, пункт 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.

П р и м е ч а н и е – 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.

П р и м е ч а н и е – 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.

П р и м е ч а н и я

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.

П р и м е ч а н и е – 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.

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

П р и м е ч а н и я

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.

5. Общие положения

Методология разработки СКИБ предназначена для реализации мероприятий по защите информации в ходе следующих процессов жизненного цикла систем

37

- 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.

_____ ГОСТ Р 57193 описывает процессы

Отдельные процессы жизненного цикла

ГОСТ Р 57193-2025 Системная и программная инженерия. Процессы жизненного цикла систем

Неэквивалентен (NEQ) ISO/IEEE 15288:2023

Процессы жизненного цикла системы		
Процессы соглашения	Процессы технического управления	Технические процессы
Процесс приобретения (6.1.1)	Процесс планирования проекта (6.3.1)	Процесс анализа бизнеса или назначения (6.4.1)
Процесс поставки (6.1.2)	Процесс оценки и контроля проекта (6.3.2)	Процесс определения потребностей и требований заинтересованной стороны (6.4.2)
Процессы организационного обеспечения проекта	Процесс управления решениями (6.3.3)	Процесс определения системных требований (6.4.3)
	Процесс управления рисками (6.3.4)	Процесс определения архитектуры (6.4.4)
	Процесс управления конфигурацией (6.3.5)	Процесс определения проекта (6.4.5)
	Процесс управления информацией (6.3.6)	Процесс системного анализа (6.4.6)
	Процесс измерений (6.3.7)	Процесс реализации (6.4.7)
	Процесс гарантии качества (6.3.8)	Процесс комплексирования (6.4.8)
		Процесс верификации (6.4.9)
Процесс управления моделью жизненного цикла (6.2.1)		Процесс передачи (6.4.10)
Процесс управления инфраструктурой (6.2.2)		Процесс валидации (6.4.11)
Процесс управления портфелем (6.2.3)		Процесс функционирования (6.4.12)
Процесс управления человеческими ресурсами (6.2.4)		Процесс сопровождения (6.4.13)
Процесс управления качеством (6.2.5)		Процесс изъятия и списания (6.4.14)
Процесс управления знаниями (6.2.6)		

Методология описывает, *как именно применять конструктивные подходы* к информационной безопасности на всех этапах ЖЦ системы.

Она детализирует основные работы по созданию системы, касающиеся обеспечения безопасности, даёт рекомендации по документированию.

Методология предлагает использовать готовые шаблоны для проектирования и разработки, что упрощает создание безопасных систем.

Где особенно полезны СКИБ

Рекомендуемая область включает следующие системы (но не ограничивается ими)

объекты критической
инфраструктуры (энергетика,
транспорт, промышленность)

телекоммуникационные
системы

системы автоматизации
зданий

бытовые устройства и
приборы

- по защите информации, начиная с этапа замысла, концепции, проектирования архитектуры системы, будь то вычислительная сеть, программно-аппаратный комплекс или программный продукт
- по безопасному взаимодействию с внешними системами
- по устойчивой работе системы под атакой или в нестабильных условиях (например, при потере сигнала)
- к процессам жизненного цикла системы и безопасной разработке ПО;
- по соответствию законодательству и нормативным документам

Система считается безопасной конструктивно, если решения, заложенные в её архитектуру и реализацию, упрощают обеспечение её безопасности и обоснование этого соответствия по сравнению с системами, где такие решения не применялись

- меры по защите информации являются частью всех этапов ЖЦ, согласованы между собой;
- ЦБ определяются задачами системы, требованиями к информации, моделью угроз;
- политики определяются составом системы, условиями её работы, человеческим фактором;
- требования по ЗИ определяются целями безопасности и политиками безопасности;
- при необходимости к списку требований добавляются обязательные требования от регуляторов;
- конструктивные подходы применяются с самых ранних этапов;
- выбранные конструктивные подходы рекомендуется обосновывать;
- реализация безопасности не должна нарушать нормальную работу системы, но может вводить дополнительные ограничения.

- Вычислимость безопасного состояния: можно проверить безопасность системы на основе достоверных данных о её работе.
- Подотчетность: можно отслеживать действия и события, влияющие на безопасность.
- Безопасные умолчания: по умолчанию запрещены все действия, влияющие на безопасность, кроме явно разрешённых.
- Минимальные возможности компрометации: у каждого элемента системы только необходимый набор функций и привилегий.
- Согласованность целей и политик безопасности: можно проверить корректность требований и работу системы.
- Невозможность подделки и несанкционированного изменения элементов системы.

6. Реализация подходов к созданию систем с КИБ

- Анализ предметной области с точки зрения ИБ: границы системы, её внешние взаимодействия, группы элементов системы по их функциям и по требованиям безопасности к ним, как элементы взаимодействуют между собой и с внешними системами
- Определение целей безопасности (ЦБ) и соответствующих требований стейкхолдеров
- Проектирование разных вариантов архитектуры СКИБ и выбор лучшего через моделирование
- Выбор шаблонов проектирования
- Применение методов организации жизненного цикла разработки
- Применение общих принципов проектирования и разработки элементов СКИБ (эвристики)

- Определение целей и политик безопасности (ЦБ и ПБ).
 - Определение и уточнение требований к СКИБ на основе ЦБ и ПБ.
 - Проектирование архитектуры СКИБ.
 - Выбор технологий для реализации системы и её элементов.
 - Реализация элементов, испытания на соответствие требованиям и ЦБ.
 - Сопровождение СКИБ во время эксплуатации для обеспечения качества и безопасности.
- В управление работами рекомендуется включать управление конфигурацией.

- проводят анализ конфликта интересов (определяют круг заинтересованных лиц, выясняют их интересы и находят общие цели);
- применяют метод аналогий (формулируют ЦБ, ориентируясь на системы похожего назначения);
- выполняют системный анализ угроз безопасности информации.

Для уточнения ЦБ также нужно анализировать требования безопасности в контексте функциональных требований к системе.

Требования безопасности могут уточняться в конце каждого этапа жизненного цикла системы.

Описание требований и выбор технологий для реализации КИБ проводится на этапе определения системных требований.

На этапах определения проекта и системного анализа эти требования могут уточняться

При уточнении требований учитывают результаты проектирования архитектуры и оценку безопасности современных технологий

Особое внимание нужно уделять прослеживаемости: должна быть видна связь между характеристиками проекта, архитектурными компонентами, результатами анализа ЦБ и ПБ, методами проверки и требованиями к элементам системы

Для создания архитектуры используют разные методы: логическое и имитационное моделирование, архитектурные представления и шаблоны, итерационную разработку, нормативные подходы и принципы информационной безопасности, перечисленные выше.

При формировании архитектуры к элементам СКИБ обычно применяют принципы информационной безопасности: минимизации зависимостей, наименьших привилегий и разделения привилегий.

Конкретных требований к виду архитектуры нет, но одни архитектуры обладают лучшими свойствами, чем другие, когда дело доходит до обоснования безопасности.

Требования регуляторов часто ограничивают эталонную архитектуру, чтобы контролировать поведение системы и обрабатываемую информацию.

После реализации элементов СКИБ нужно провести испытания на соответствие требованиям безопасности

Для этого реализуют процессы гарантии качества, проверки требований (верификации) и подтверждения целей безопасности (валидации). Исходные требования к этим процессам определяются ГОСТ Р 57193-2016 и отраслевыми стандартами.

Состав и документирование испытаний в нашей стране рекомендуется проводить по ГОСТ Р 51583-2014.

Результаты работ по созданию СКИБ рекомендуется документировать.

Это могут быть пояснительные записки, схемы, модели, описания, алгоритмы и т.п. ЕСПД, ЕСКД.

Документируются: Цели и политики безопасности (ЦБ и ПБ); описание архитектуры СКИБ, её связей с внешними системами и сетями, интерфейсов и способов доступа; модель угроз безопасности информации и типового нарушителя; описание потенциальных векторов атак, сценариев, тактик и техник воздействия вредоносных программ и НСД; требования безопасности информации, а также методы и средства её обеспечения; описание механизмов, которые обеспечивают надёжную работу СКИБ под атакой; ограничения, накладываемые на СКИБ; рекомендации по безопасному обновлению системного и прикладного ПО СКИБ; программа, методики и протоколы испытаний реализации КИБ.

7. Содержание основных работ при создании систем с КИБ

- 7.1.1 Когда определяют цели и предположения безопасности?
- 7.1.2 Как определяют цели и предположения безопасности?
- 7.1.3 Как выглядят цели безопасности? Чем они отличаются от требований?
- 7.1.4 Что такое предположения безопасности?
- 7.1.5 Зачем нужны предположения безопасности?
- 7.1.6 Что мешает предположить, что «все безопасно»?
- 7.1.7 Как анализировать интересы и мотивы, чтобы в итоге получить цели безопасности?
- 7.1.8 Цели и предположения безопасности «высечены в камне» или их можно менять?
- 7.1.9 Что в итоге получаем после опроса заинтересованных сторон?

7.2.1 На каком этапе определяют системные требования к СКИБ?

7.2.2 Что требуется для определения системных требований к безопасности?

7.2.3 Как выглядят результаты анализа при определении требований к СКИБ?

- 7.3.1 Какой подход к проектированию архитектуры СКИБ?
- 7.3.2 Какие требования предъявляются к архитектуре
- 7.3.3 Основные принципы проектирования архитектуры
- 7.3.4 Стоит ли использовать моделирование при создании архитектуры?
- 7.3.5 Как именно проводить моделирование архитектуры СКИБ?
- 7.3.6 Что должно быть результатом моделирования архитектуры?
- 7.3.7 У меня есть несколько вариантов архитектуры. Как их сравнить между собой?
- 7.3.8 Как еще сравнить различные варианты архитектуры?
- 7.3.9 Может ли архитектура меняться позднее? Насколько сильно?
- 7.3.10 Как понять, что архитектура подходит?

7.4.1 Когда нужно (и можно) утвердить технологии в составе системы: интерфейсы, готовые встраиваемые решения, платформы, протоколы, языки программирования

7.4.2 Как подбирают технологии реализации?

7.4.3 Что входит в «технологии»?

7.4.4 К кому предъявляют требования по безопасности технологий?

7.4.5 Как нужно действовать для обеспечения безопасности технологий?

7.4.6 Насколько «свежими» должны быть технологии? Что важнее - испытанные годами или новые технологии и протоколы?

- 7.5.1 Когда проводят первые испытания безопасности?
- 7.5.2 Есть ли особые требования к реализации СКИБ?
- 7.5.3 Что нужно показать в процессе испытаний?
- 7.5.4 Какие моменты, касающиеся безопасности можно уточнять в процессе реализации?
- 7.5.5 Что еще стоит сделать в процессе реализации (обеспечивающие системы)?
- 7.5.6 Что нужно проверять при реализации каждого элемента системы в отдельности?
- 7.5.7 Какие проверки нужно проводить в отношении разработчика, внешнего или внутреннего?
- 7.5.8 Какие испытания проводят по окончании разработки?

- 7.6.1 Что такое сопровождение СКИБ?**
- 7.6.2 В чем заключается сопровождение СКИБ?**
- 7.6.3 Что происходит, если при эксплуатации обнаружена уязвимость СКИБ?**

8. Документирование конструктивных подходов к обеспечению ИБ

Стандарт накладывает требования на документирование. Это сделано для того, чтобы нельзя было сказать «мы действительно все делали, но не записали, а на самом деле у нас СКИБ».

Реализацию конструктивных подходов к обеспечению информационной безопасности, согласно стандарту, нужно документировать в «Спецификации конструктивных подходов к информационной безопасности»

Спецификацию рекомендуется включать в комплект документов для оценки соответствия системы требованиям по защите информации.

9. Применение шаблонов проектирования и разработки при создании СКИБ

Шаблоны решают стандартные задачи разработки, такие как ограничения производительности, обеспечение высокой доступности, минимизация рисков или выполнение заданных целей безопасности

Шаблоны можно применять как для системы в целом, так и для её отдельных компонентов, на аппаратном или программном уровне, или совмещать

Следование шаблонам помогает обеспечить устойчивую работу системы под атакой и снижение поверхности атаки

Базовые шаблоны в Приложении А

Можно создавать свои шаблоны

Шаблоны для СКИБ рекомендуется создавать на основе общих принципов проектирования из раздела 6.1 и требований безопасности, установленных законодательством или заказчиком

Шаблоны включаются в спецификацию