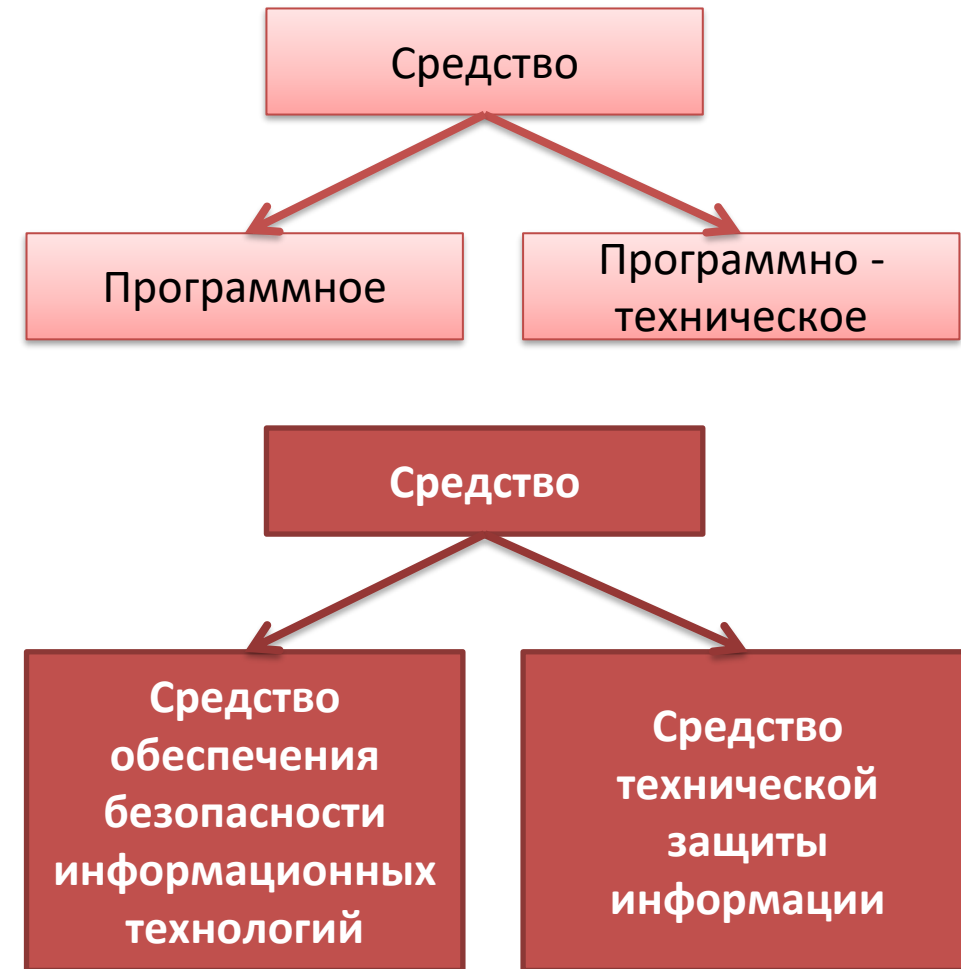


Сертификация СЗИ vs сертификация РБПО

Вареница Виталий

Общие положения

- **Требования по безопасности информации** - являются обязательными требованиями в области технического регулирования к продукции (работам, услугам), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа;
- Выполнение Требований является обязательным при проведении работ по сертификации, организуемых ФСТЭК России в пределах своих полномочий в соответствии с Положением о системе сертификации средств защиты информации.



Уровни доверия

Уровни доверия	Применение							
	КИИ, категория	ГИС, класс защищенности	АСУ ТП, класс защищенности	ИСПДн, уровень защищенности ПДн	ИСОП, класс	Секретно	Совершенно секретно	Особой важности
6	3	3	3	3 и 4	-	-	-	-
5	2	2	2	2	-	-	-	-
4	1	1	1	1	II	-	-	-
3	+	+	+	+	+	+	-	-
2	+	+	+	+	+	+	+	-
1	+	+	+	+	+	+	+	+

Соответствие классов СЗИ и СВТ уровням доверия

Уровни доверия	СЗИ	СВТ
6	6	-
5	5	-
4	4	5
3	3	4
2	2	3
1	1	2

Информационное сообщение о требованиях по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий от 29 марта 2019 г. N 240/24/1525 :

обязательная оценка соответствия СЗИ Требованиям к уровням доверия

~~Требования доверия к безопасности операционных систем должны соответствовать стандартным компонентам доверия, определяемым по ГОСТ Р ИСО/МЭК 15408-3, и специальным компонентам доверия к безопасности операционных систем, определяемым в соответствии с приложением № 4 к настоящим Требованиям.~~

Требования к разработке и производству средства

№ п/п	Наименование требования к уровню доверия	Уровень доверия					
		6	5	4	3	2	1
	Требования к разработке и производству средства:						
1.1	требования к разработке модели безопасности средства			+	+	=	=
1.2	требования к проектированию архитектуры безопасности средства	+	=	=	=	=	=
1.3	требования к разработке функциональной спецификации средства	+	+	+	+	=	=
1.4	требования к проектированию средства	+	=	=	+	+	=
1.5	требования к разработке проектной (программной) документации средства	+	+	+	+	+	=
1.6	требования к средствам разработки, применяемым для разработки средства	+	=	=	=	=	=
1.7	требования к управлению конфигурацией средства	+	+	+	+	+	=
1.8	требования к разработке документации по безопасной разработке средства	+	=	=	=	=	=
1.9	требования к разработке эксплуатационной документации средства	+	=	=	=	=	=

Требования к проведению испытаний средства и к поддержке безопасности средства

№ п/п	Наименование требования к уровню доверия	Уровень доверия					
		6	5	4	3	2	1
2	Требования к проведению испытаний средства:						
2.1	требования к тестированию средства	+	+	+	+	=	=
2.2	требования к испытаниям по выявлению уязвимостей и недеklarированных возможностей средства	+	+	+	+	+	+
2.3	требования к проведению анализа скрытых каналов в средстве			+	+	=	+
3.	Требования к поддержке безопасности средства:						
3.1	требования к устранению недостатков средства	+	+	+	+	=	=
3.2	требования к обновлению средства	+	+	+	+	=	=
3.3	требования к документированию процедур устранения недостатков и обновления средства	+	=	=	=	=	=
3.4	требования к информированию об окончании производства и (или) поддержки безопасности средства	+	=	=	=	=	=

Прослеживание требований к ГОСТ 15408

№ п/п	Наименование требования к уровню доверия	ТДБ из ГОСТ 15408
	Требования к разработке и производству средства:	
1.1	требования к разработке модели безопасности средства	ADV_SMP
1.2	требования к проектированию архитектуры безопасности средства	ADV_ARC
1.3	требования к разработке функциональной спецификации средства	ADV_FSP
1.4	требования к проектированию средства	ADV_TSD
1.5	требования к разработке представления реализации средства	ADV_IMP
1.6	требования к средствам, применяемым для разработки средства	ALC_TAT
1.7	требования к управлению конфигурацией средства	ALC_CMC, ALC_CMS, ALC_FLR, ALC_DEL
1.8	требования к разработке документации по безопасной разработке средства	ALC_DVS
1.9	требования к разработке руководства пользователя средства	AGD_OPE
1.10	требования к разработке руководства администратора средства	AGD_PRE

Прослеживание требований к ГОСТ 15408

№ п/п	Наименование требования к уровню доверия	Уровень доверия
2	Требования к проведению испытаний средства:	
2.1	требования к тестированию средства	ATE_FUN, ATE_IND, ATE_COV, ATE_DPT
2.2	требования к испытаниям по выявлению уязвимостей и недекларированных возможностей средства	AVA_VAN (AVA_VLA), ADV_IMP
2.3	требования к проведению анализа скрытых каналов в средстве	AVA_CCA
3.	Требования к поддержке безопасности средства:	
3.1	требования к устранению недостатков средства	ALC_FLR
3.2	требования к обновлению средства	ALC_FLR
3.3	требования к документированию процедур устранения недостатков и обновления средства	ALC_FLR

Модель безопасности. 4 уровень доверия

При разработке модели безопасности средства должны быть отражены следующие сведения:

- реализуемые политики управления доступом (для средств, в которых предусмотрена функция разграничения доступа);
- реализуемые политики фильтрации информационных потоков (для средств, в которых предусмотрена функция фильтрации информационных потоков).

Язык описания модели безопасности:

- математический;
- формализованный (машиночитаемый), например, Alloy, ASM, B, Event-B, TLA+, VDM, Z.

Модель безопасности должна включать:

- описание условий безопасности;
- взаимосвязь условий безопасности с режимами функционирования средства;
- формальное доказательство того, что условия безопасности выполняются, и в модели нет противоречий.

Модель безопасности

Пример условий безопасности:

■ Математический язык

Для каждого непривилегированного субъекта $x \in N_s$, субъекта $y \in S$ и сущности $e \in E$ таких, что $e \in [y]$ и $(x, e, write_m) \in F$, верно неравенство $i_s(y) \leq i_s(x)$ – если непривилегированным субъектом реализован информационный поток по памяти к сущности, функционально ассоциированной с другим субъектом, то его уровень целостности не выше уровня целостности непривилегированного субъекта;

■ Формализованный язык (Event-B)

invariants

@EntityHierarchy1

$$\forall x, y \cdot x \in \text{Entities} \wedge y \in \text{Entities} \wedge x \in \text{EntityHierarchy}(y) \\ \Rightarrow \text{EntityInt}(x) \subseteq \text{EntityInt}(y)$$

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ



НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

ГОСТ Р
(проект,
первая редакция)

Защита информации

ФОРМАЛЬНАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ

Часть 1

Общие требования

Настоящий проект стандарта не подлежит применению до его утверждения

Москва
Стандартинформ
201X

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ



НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

ГОСТ Р
(проект,
первая редакция)

Защита информации

ФОРМАЛЬНАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ

Часть 2

Руководство по верификации формальной модели управления доступом

Настоящий проект стандарта не подлежит применению до его утверждения

Москва
Стандартинформ
201X

Модель безопасности, 3 уровень доверия

- Модель безопасности средства должна быть верифицирована с использованием инструментальных средств (Rodin, Z3, CVC, Alt-Ergo, Vampire, E-Prover, Coq, PVS и т.д.);
- Формализованное (машиночитаемое) описание должно быть на языке, поддерживаемом реализуемыми этими инструментальными средствами формальными методами.
- Неформальным образом должен быть получен вывод о непротиворечивости модели безопасности и выполнении заданных в ее рамках условий безопасности.

Модель безопасности, 3 уровень доверия

File Edit Navigate Search Project Run Rename Window Help

Proof Tree

- ✓ simplification rewrites
 - ✓ type rewrites
 - ✓ simplification rewrites
 - ✓ remove \in in $\text{Accesses} \in \text{Machines} \rightarrow$ (
 - ✓ simplification rewrites
 - ✓ type rewrites
 - ✓ he with $\text{dom}(\text{Accesses}) = \text{Machines}$
 - ✓ remove \in in $\text{machine} \in \text{dom}(\text{Accesses})$
 - ✓ \exists hyp ($\exists x. \text{machine} \mapsto x \in \text{Accesses}$)
 - ✓ remove \in in Accesses
 - ✓ mp impl ($[[2]] \mapsto$
 - ✓ remove \neg in $\neg([$
 - ✓ NewPP


login/AccessesType/INV

 - ☐ $\text{user} \in \text{USERS} \setminus \text{Users}$
 - ☐ $\text{dom}(\text{Accesses}) = \text{Machines}$
 - ☐ $\text{machine} \mapsto x \in \text{Accesses}$
 - ☐ $\text{Accesses} \in \text{dom}(\text{Accesses}) \leftrightarrow (\text{Devices} \leftrightarrow \text{Users})$
 - ☐ $\forall x, x0, x1 .$
 - $\neg x0 = x1$
 - \Rightarrow
 - $\neg x \mapsto x0 \in \text{Accesses} \vee$
 - $\neg x \mapsto x1 \in \text{Accesses}$

Selected Hypotheses

Proof Control Statistics Rodin Problems

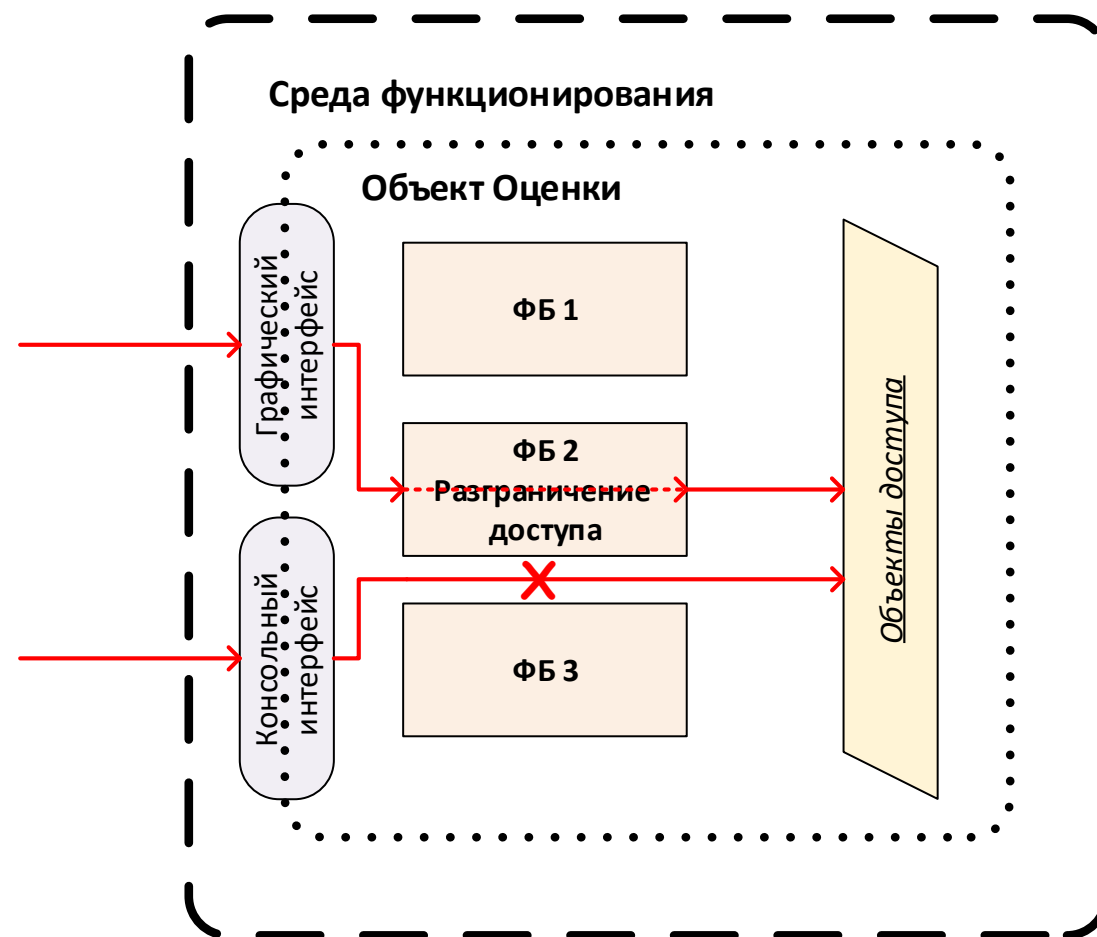
nPP R dc ah ae



Архитектура безопасности средства

На средство должно быть разработано описание архитектуры безопасности средства с обоснованием:

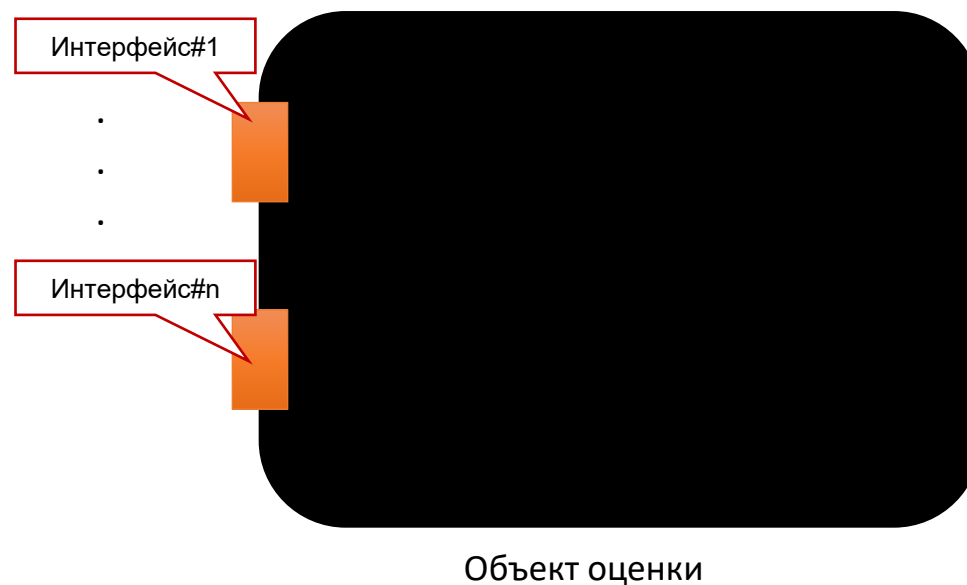
- безопасности процесса инициализации средства;
- обеспечения собственной защиты средства от несанкционированного доступа;
- невозможности обхода функций безопасности средства.



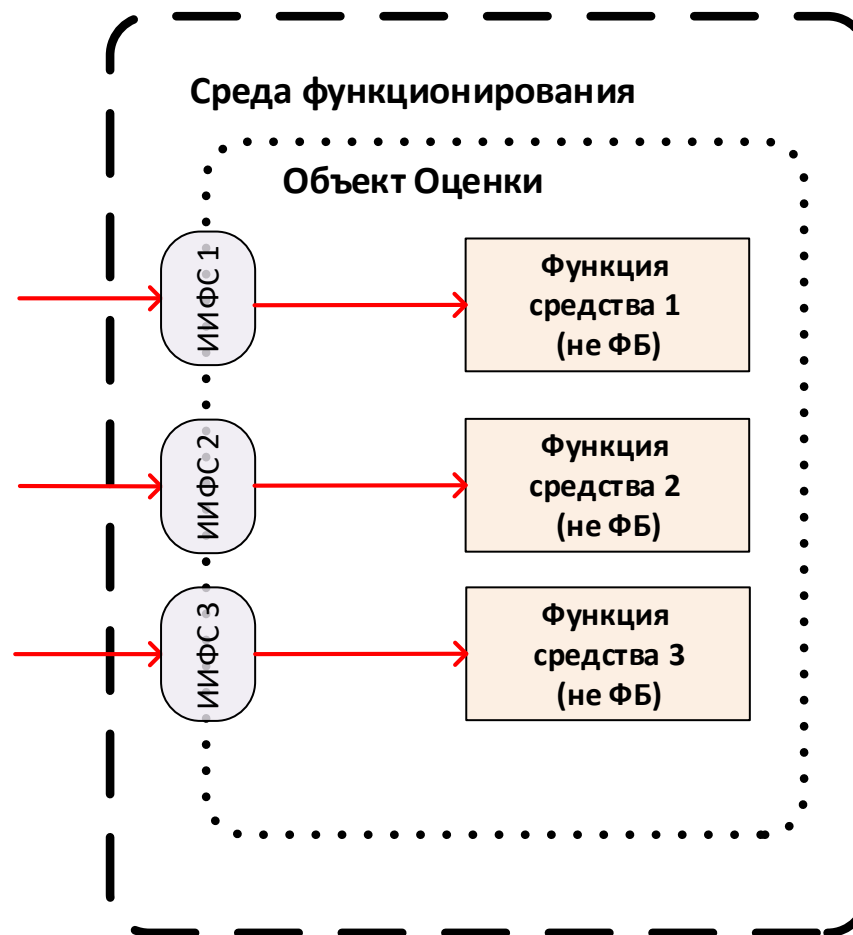
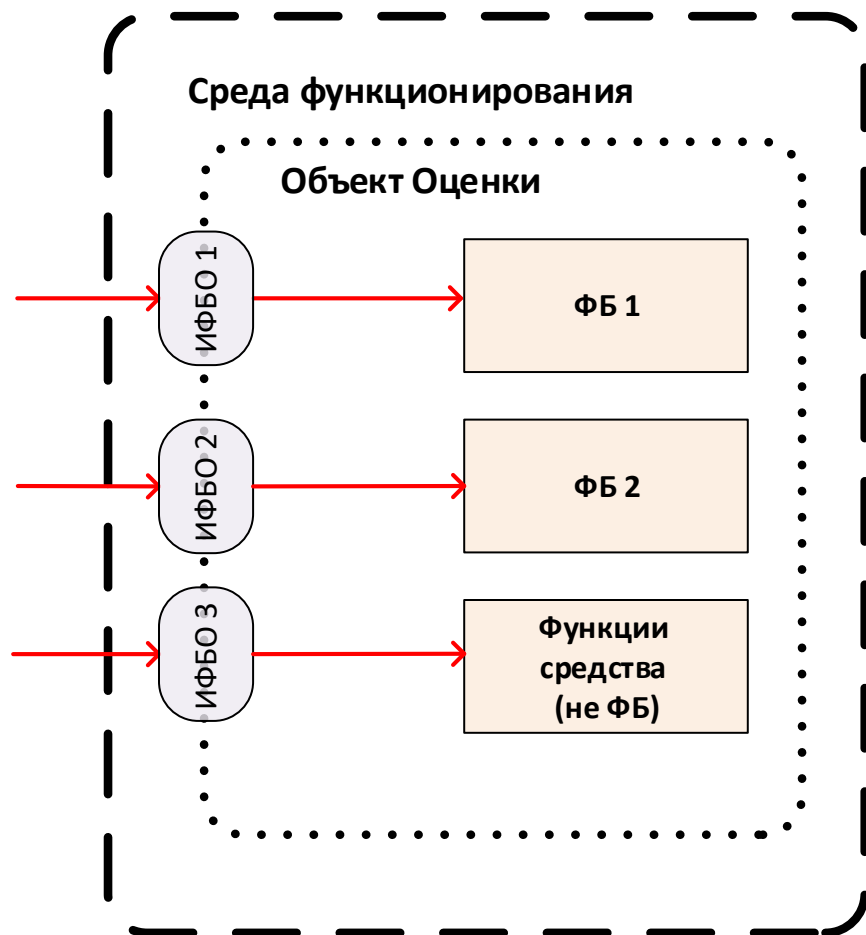
Функциональная спецификация средства, 6 уровень доверия

В функциональную спецификацию средства должны быть включены:

- описание назначения и способов использования каждого **интерфейса функций безопасности (при наличии функций безопасности)** и иных функций средства;
- описание параметров, связанных с каждым **интерфейсом функций безопасности (при наличии функций безопасности)** и иных функций средства;
- перечень интерфейсов, не влияющих на функции безопасности средства (при наличии функций безопасности и наличии таких интерфейсов).



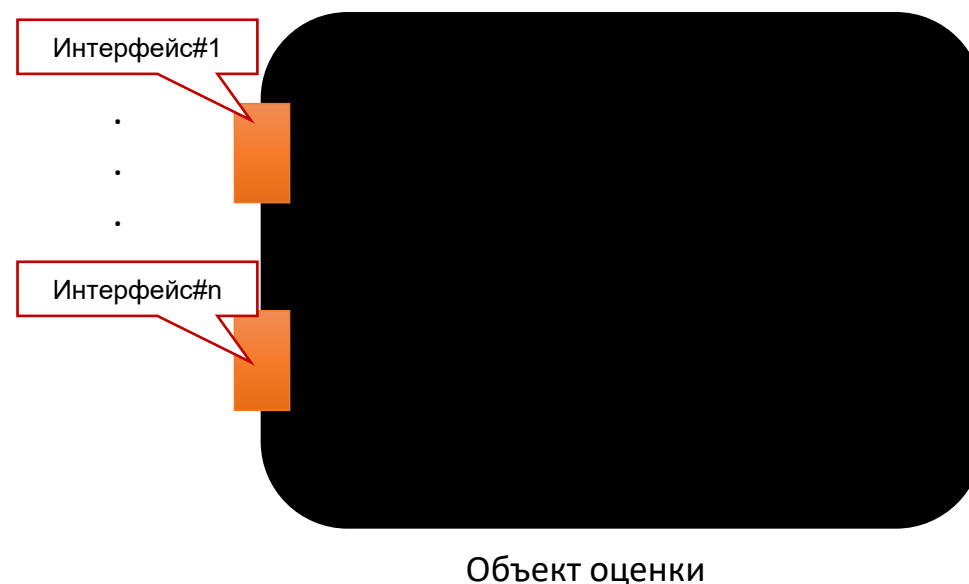
Функциональная спецификация средства, 6 уровень доверия



Функциональная спецификация средства, 6 уровень доверия

В функциональную спецификацию средства должны быть включены:

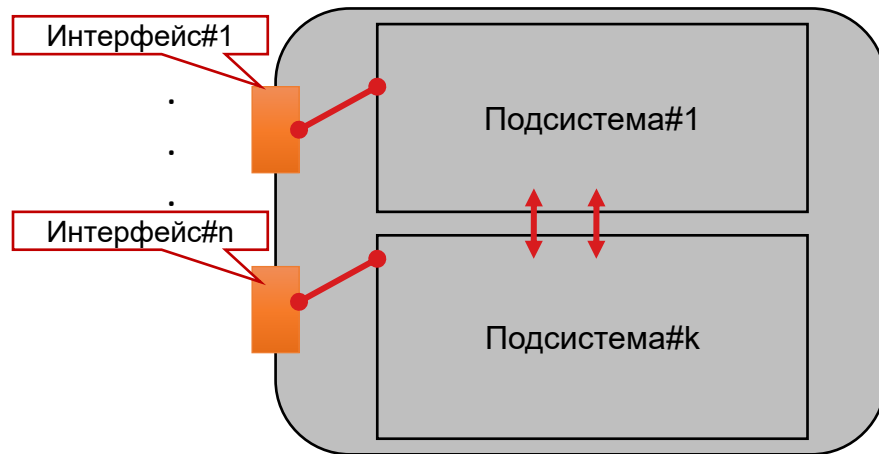
- описание **назначения и способов использования** каждого интерфейса функций безопасности (при наличии функций безопасности) и иных функций средства;
- описание **параметров**, связанных с каждым интерфейсом функций безопасности (при наличии функций безопасности) и иных функций средства;
- перечень интерфейсов, не влияющих на функции безопасности средства (при наличии функций безопасности и наличии таких интерфейсов).



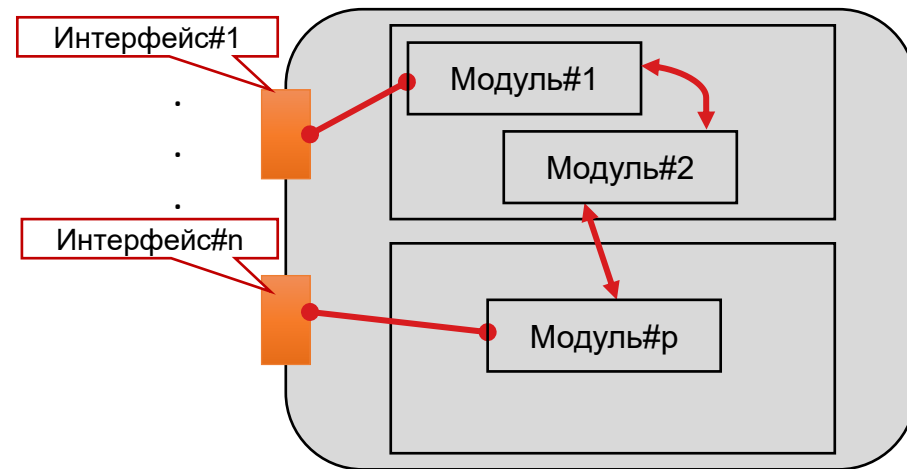
Проектирование средства, 6 уровень доверия

Проектная документация средства должна включать:

- проект на уровне подсистем средства (эскизный проект);
- проект на уровне модулей средства (технический проект).



Объект
оценки

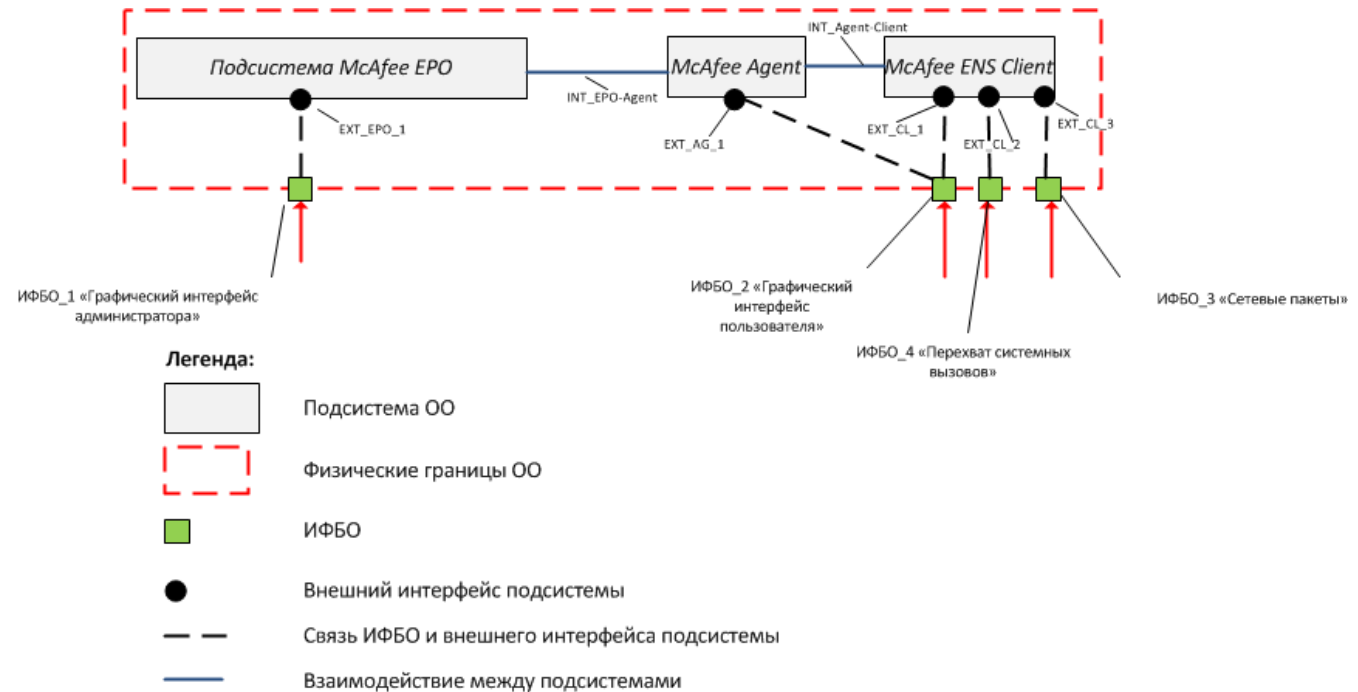


Объект
оценки

Проектирование средства, 6 уровень доверия

Эскизный проект должен включать:

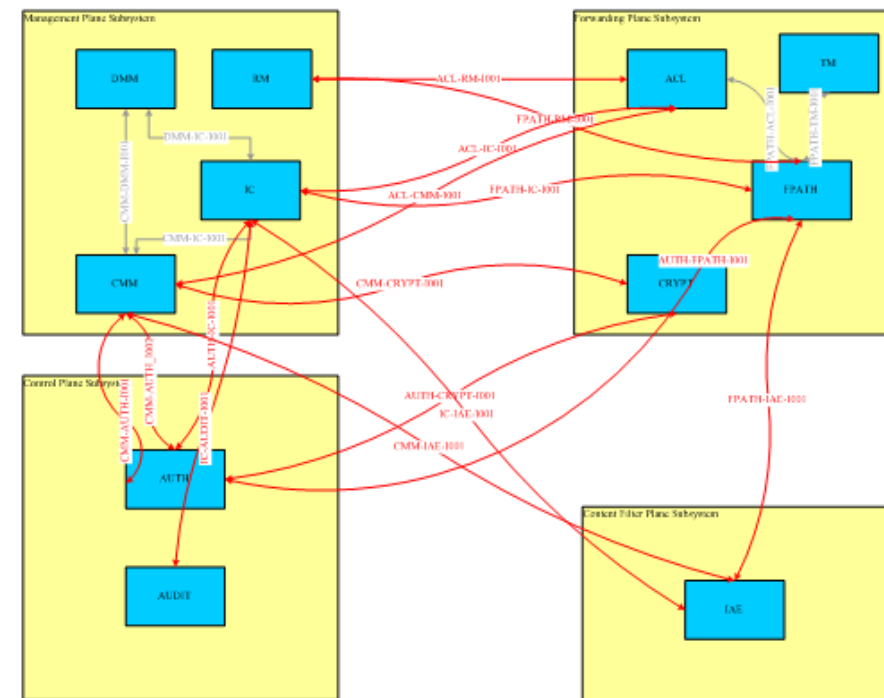
- описание структуры средства на уровне подсистем средства;
- описание всех подсистем средства;
- сопоставление функций средства и интерфейсов, описанных в функциональной спецификации, с подсистемами средства;
- описание взаимодействия подсистем средства между собой.



Проектирование средства, 6 уровень доверия

Технический проект должен включать:

- описание структуры средства на уровне модулей;
- описание всех модулей средства:
 - для модулей средства, реализующих функции безопасности:
 - описание интерфейсов,
 - описание возвращаемых модулями в ответ на запросы значений,
 - описание взаимодействий с другими модулями и вызываемыми интерфейсами этих модулей;
 - для модулей средства, не влияющих на выполнение функций безопасности:
 - описание назначения и взаимодействия с другими модулями;
- сопоставление подсистем средства, описанных в эскизном проекте, с модулями.



Проектирование средства, 3 уровень доверия

Эскизный проект дополнительно должен включать:

- формальное (математическое) описание подсистем средства, реализующих функции безопасности, и неформальное (нематематическое) описание иных подсистем средства;
- описание подсистем средства с сопровождающим пояснительным текстом.

Проектирование средства, 2 уровень доверия

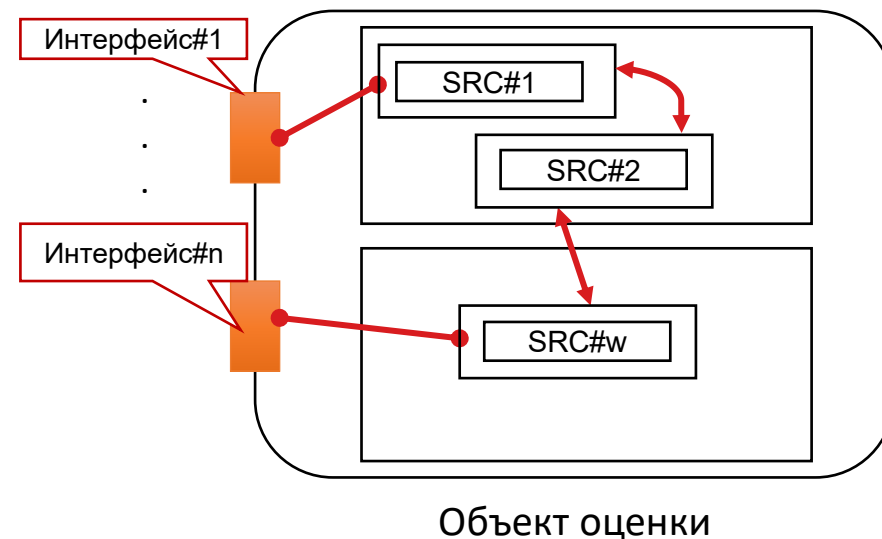
Эскизный проект дополнительно должен включать демонстрацию того, что все описанные режимы функционирования подсистем являются корректным и полным отображением соответствующих интерфейсов, описанных в функциональной спецификации.

Технический проект дополнительно должен включать:

- Неформальное (нематематическое) описание всех модулей средства, сопровождаемое пояснительным текстом (назначение, описание интерфейсов, возвращаемых ими в ответ на запросы значений, взаимодействий с другими модулями и вызываемыми интерфейсами этих модулей);
- Описание модулей средства должно включать описание процедур и функций, реализуемых этими модулями;
- Описание взаимодействия модулей средства должно включать описание взаимодействия соответствующих процедур и функций.

Представление реализации средства, 6 уровень доверия

- Формуляр средства должен содержать контрольные суммы дистрибутива и исполняемых файлов программного обеспечения средства.
- Контрольные суммы должны уточняться при обновлении средства.
- Для аппаратной платформы программно-технического средства должен быть представлен перечень аппаратных устройств (микросхем), которые влияют на выполнение функций безопасности и (или) могут быть использованы для реализации угроз безопасности информации.



Представление реализации средства, 5 уровень доверия

Представление реализации средства должно включать:

- для аппаратной платформы средства (при наличии аппаратной платформы) - структурные схемы и техническую документацию аппаратных средств (даташит на микросхемы), входящих в аппаратную платформу;
- для программного обеспечения - исходные тексты программного обеспечения, входящего в состав средства, с указанием значений контрольных сумм файлов с исходными текстами программного обеспечения, за исключением программного обеспечения, не реализующего функции безопасности и не влияющего на реализацию функций безопасности, заимствованного у сторонних изготовителей.

Представление реализации средства должно быть сопоставлено с модулями, описанными в проектной документации. Для модулей, реализующих функции безопасности средства, должно быть продемонстрировано соответствие представлению реализации средства.

Представление реализации средства, 1 - 4 уровни доверия

4 УД

1-3 УД

Представление реализации средства дополнительно должно включать

- | | |
|--|--|
| <ul style="list-style-type: none">■ для аппаратной платформы средства (при наличии аппаратной платформы) - функциональные схемы аппаратных средств (микросхем), входящих в аппаратную платформу, и представление (код) на языке описания аппаратных средств. | <ul style="list-style-type: none">■ исходные тексты программного обеспечения, входящего в состав средства, не реализующего функции безопасности и не влияющего на реализацию функций безопасности, заимствованного у сторонних изготовителей;■ для аппаратной платформы средства (при наличии аппаратной платформы) - принципиальные схемы аппаратных средств, входящих в аппаратную платформу. |
|--|--|

Требования к средствам, применяемым при разработке

На средства, применяемые для разработки средства, должна быть разработана документация, включающая описания:

- средств, применяемых для разработки средства;
- использованных опций средств, применяемых для разработки средства.

Пример:

В компиляторе GNU C 3 установлены следующие опции:

```
gcc -g -O2 -pipe -Wall -D_FORTIFY_SOURCE=2
-fstack-protector
```

| Система | Продукт | Версия | Разработчик |
|---|---|------------------|--|
| Система хранения документов проекта | Windows Server 2016 Standard | 10.0.14393 | Microsoft. Коммерческий проект.
https://docs.microsoft.com/ru-ru/windows-server/get-started/2016-edition-comparison |
| | Confluence | 6.11.0 | Atlassian. Коммерческий проект
https://ru.atlassian.com/software/bitbucket |
| | JIRA | 7.12.0 | Atlassian. Коммерческий проект
https://ru.atlassian.com/software/jira |
| Система хранения исходных текстов проекта | Bitbucket | 5.13.1 | Atlassian. Коммерческий проект
https://ru.atlassian.com/software/bitbucket |
| | Git | 2.19.1.windows.1 | Некоммерческий проект с открытым исходным кодом
https://git-scm.com/docs |
| Средства сборки продуктов | Microsoft Visual Studio Professional 2013 | 12.0 | Microsoft. Коммерческий проект.
https://docs.microsoft.com/ru-ru/visualstudio/ |
| | µVision | 5.25.2.0 | Keil. Коммерческий проект.
http://www.keil.com/support/man/ |

Управление конфигурацией средства, 6 уровень доверия

Документация по управлению конфигурацией средства должна включать:

- описание уникальной маркировки средства;
- список элементов конфигурации средства, включающий в том числе документацию;
- порядок управления изменениями средства и документации.



Управление конфигурацией средства

Вся документация на ОО маркируется уникальным шифром, составленным в соответствии с требованиями ЕСПД с учетом специфики рассматриваемых документов:

XXX.YYYYYYYYY.ZZZZZ-AA BB CC, где

- **XXX** – шифр страны-изготовителя ОО,
- **YYYYYYYYY** - Общероссийский классификатор предприятий и организаций (ОКПО) разработчика документации,
- **ZZZZZ** – порядковый регистрационный номер;
- **AA** - номер редакции документа;
- **BB** – код вида документа;
- **CC** – номер документа данного вида.

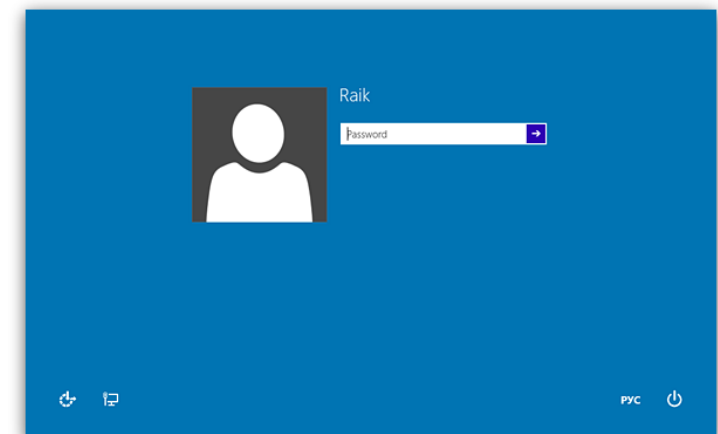
Управление конфигурацией средства

| Уровни доверия | Элементы конфигурации |
|----------------|---|
| 6 | средство и документация |
| 5 | + части (элементы, компоненты) средства |
| 4 | + представление реализации средства |
| 3 | = |
| 2 | + инструментальные средства разработки средства |
| 1 | = |

Документация по безопасной разработке средства

На средство должна быть разработана документация по безопасности разработки средства, которая должна включать:

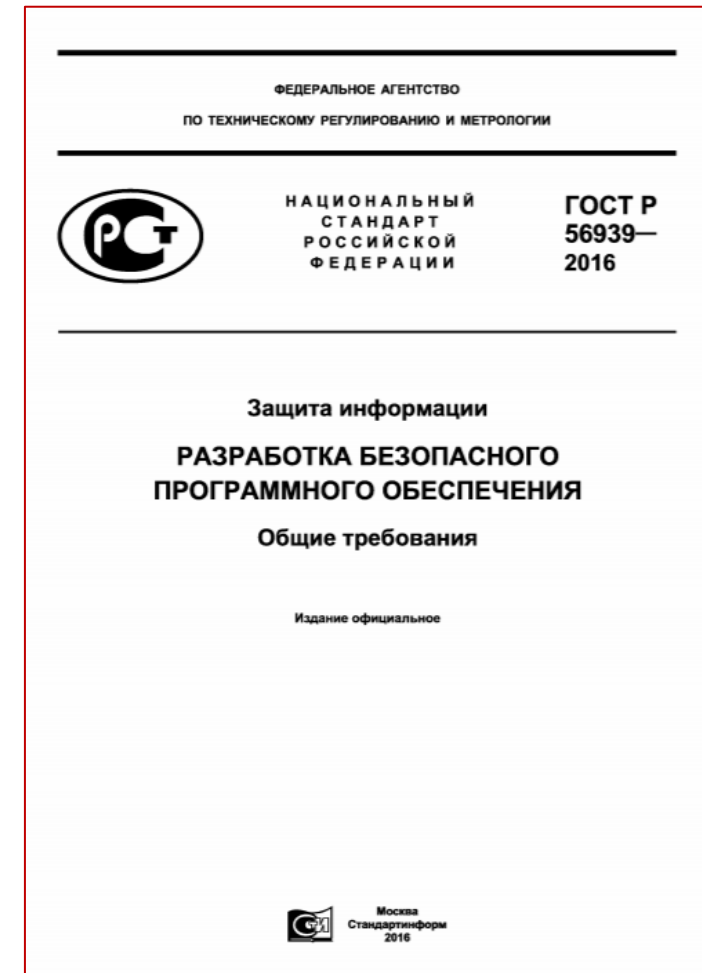
- описание всех физических, процедурных, организационных и других мер безопасности, применяемых в среде разработки средства для защиты конфиденциальности и целостности проектной документации и реализации средства;
- применяемые меры безопасности, направленные на снижение вероятности возникновения в средстве уязвимостей и иных недостатков, и их обоснование.



Документация по безопасной разработке средства

Примеры мер безопасности из ГОСТ Р 56939-2016:

- определение требований по безопасности, предъявляемые к разрабатываемому ПО;
- моделирование угроз безопасности информации;
- уточнение проекта архитектуры программы с учетом результатов моделирования угроз безопасности информации;
- использование при разработке ПО идентифицированных инструментальных средств;
- создание программы на основе уточненного проекта архитектуры программы;
- создание (выбор) и использование при создании программы порядка оформления исходного кода программы;
- статический анализ исходного кода программы и т.д.



Руководства пользователя средства

На средство должно быть разработано руководство пользователя средства (при наличии пользователей средства) с описанием:

- режимов работы средства;
- принципов безопасной работы средства;
- функций и интерфейсов функций средства, доступных каждой роли пользователей;
- параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасных значений;
- типов событий безопасности, связанных с доступными пользователю функциями средства;
- действий после сбоев и ошибок эксплуатации средства.

Руководства администратора средства

На средство должно быть разработано руководство администратора средства с описанием:

- действий по приемке поставленного средства;
- действий по безопасной установке и настройке средства;
- действий по реализации функций безопасности среды функционирования средства.

Таблица 2 – Минимальные требования к программному и аппаратному обеспечению

| Элемент | Параметр |
|--|---|
| Операционная система | Microsoft Windows Server 2016, сертификат соответствия ФСТЭК России от 22.08.2018 г. №4006

или Microsoft Windows Server Datacenter 2012 R2, сертификат соответствия ФСТЭК России от 19.03.2015 г. №3367

или Microsoft Windows Server Standard 2012 R2, сертификат соответствия ФСТЭК России от 17.03.2015 г. №3366. |
| Процессор | 64-разрядный |
| Оперативная память | 24 Гб |
| Жесткий диск (свободное пространство) | 500 Гб |
| Дополнительное программное обеспечение | СУБД одной из следующих версий: <ul style="list-style-type: none"> – Microsoft SQL Server версии 2012, 2016, 2017, 2019; – PostgreSQL версии 9, 10, 11, 12; – Postgres Pro версии 9, 10, 11. |

Пример действий по реализации ФБ среды функционирования средства:

в настройках IIS (Internet Information Services) веб-сервера, на котором установлено ПО ХХХ, для соответствующего узла (site) должен быть установлен режим аутентификации «Windows Authentication».

Требования к проведению испытаний средства

В отношении средства должны быть проведены испытания, предусматривающие:

- тестирование средства;
- испытания по выявлению уязвимостей и недеklarированных возможностей средства;
- проведение анализа скрытых каналов в средстве.

Тестирование и анализ скрытых каналов проводятся только для средств защиты информации.

Испытания средства проводятся в ходе сертификационных испытаний и (или) в ходе приемочных испытаний.

Требования к тестированию средства, 6+ уровень доверия

- Средство должно быть протестировано.
- Тестовая документация должна включать:
 - план тестирования, содержащий тесты, которые необходимо выполнить, описание сценариев проведения каждого теста, учитывающее зависимости последовательности выполнения тестов от результатов других тестов, описание ресурсов, необходимых для проведения тестирования;
 - описание сопоставления тестов с интерфейсами функций безопасности средства (при наличии функций безопасности), описанными в функциональной спецификации, демонстрирующее их полное покрытие тестами;
 - описание ожидаемых результатов тестирования, свидетельствующих об успешности выполнения тестов;
 - описание фактических результатов тестирования, их сопоставление с ожидаемыми результатами тестирования и на его основе - выводы об успешности тестов.

Требования к тестированию средства

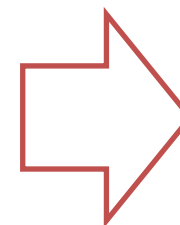
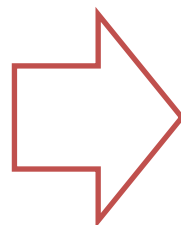
| Уровни доверия | Требования |
|---|--|
| Тестовая документация должна включать описание сопоставления тестов с | |
| 6 | интерфейсами функций безопасности средства (при наличии функций безопасности), описанными в функциональной спецификации, демонстрирующее их полное покрытие тестами |
| 5 | подсистемами средства, описанными в эскизном проекте, демонстрирующее их полное покрытие тестами |
| 4 | модулями средства, реализующими функции безопасности (при наличии функций безопасности) и описанными в техническом проекте, демонстрирующее полное покрытие тестами функций безопасности |
| 1 - 3 | модулями средства, не влияющими на выполнение функций безопасности и описанными в техническом проекте, демонстрирующее полное покрытие тестами функций безопасности |

Требования к тестированию средства

| 5 УД | 1-4 УД |
|---|---|
| <ul style="list-style-type: none">■ При проведении тестирования средства проводится оценка влияния на подсистемы средства, реализующие функции безопасности, иных подсистем средства. | <ul style="list-style-type: none">■ При проведении тестирования средства проводится оценка влияния (невлияния) на модули средства, реализующие функции безопасности, иных модулей средства. |

Испытания по выявлению уязвимостей и недекларированных возможностей средства

| Уровень доверия | Уровень контроля |
|-----------------|------------------|
| 6 | 6 |
| 5 | 5 |
| 4 | 4 |
| 3 | 3 |
| 2 | 2 |
| 1 | 1 |



ПОД

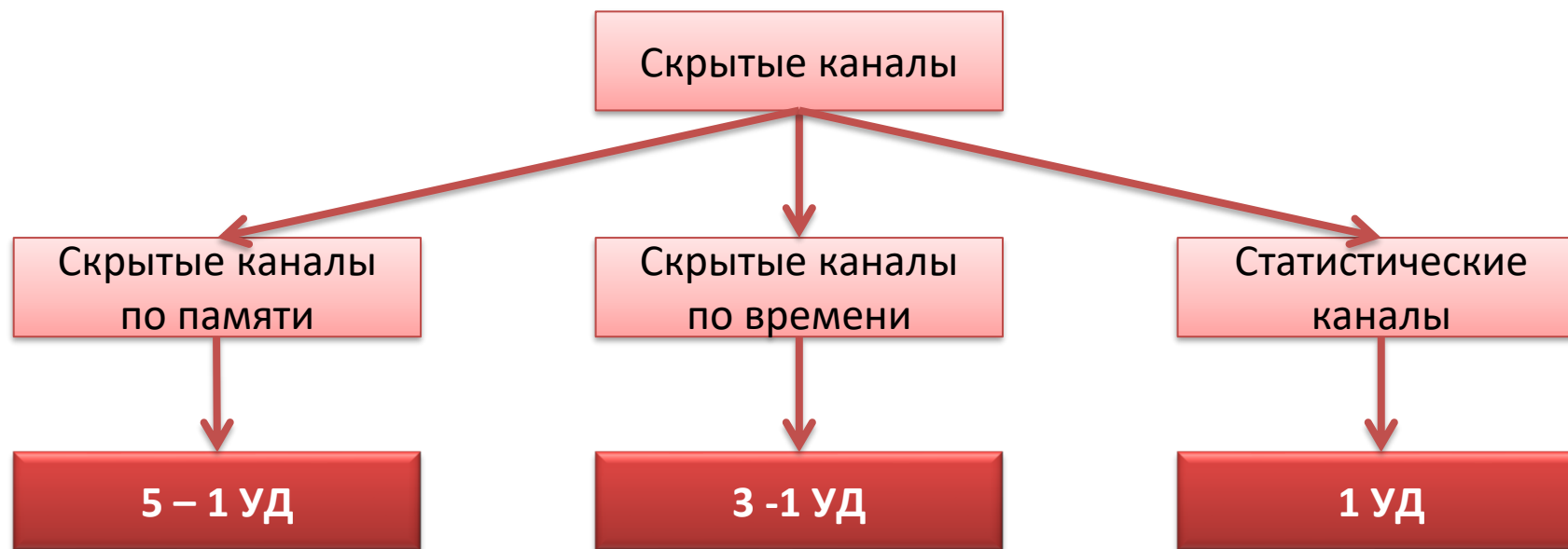
КАО

САО

ДАО

РАО

Анализ скрытых каналов в средстве



- ГОСТ Р 53113.1-2008 Информационная технология (ИТ). Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения;
- ГОСТ Р 53113.2-2009 Информационная технология (ИТ). Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.

Устранение недостатков средства

39

| Уровни доверия | Требования |
|----------------|---|
| | <ul style="list-style-type: none">разработка компенсирующих мер по защите информации или ограничений по применению средства, снижающих возможность эксплуатации недостатков (уязвимостей);доведение информации о недостатках средства, а также о компенсирующих мерах по защите информации или ограничений по применению средства до потребителей средства, ФСТЭК России и БДУ ФСТЭК России; |
| 6 | должны осуществляться; |
| 5 | должны осуществляться не позднее 72 часов с момента выявления недостатка; |
| 4 | должны осуществляться в срок не более 48 часов с момента выявления недостатка; доведение информации должно осуществляться до каждого потребителя средства путем: <ul style="list-style-type: none">отправки сообщений на электронные адреса потребителей;за счет применения компонента средства, обеспечивающего доведение указанной информации до потребителя автоматически. |
| 1 - 3 | доведение информации должно осуществляться способом, обеспечивающим подлинность и целостность доводимой информации (по сетям связи должны обеспечиваться за счет применения электронной цифровой подписи (далее – ЭЦП)). |

Требования к устранению недостатков средства

| Уровни доверия | | Требования |
|----------------|--|--|
| | | устранение недостатков средства путем доработки средства или его отдельных компонентов, принятие иных мер, снижающих возможность эксплуатации уязвимостей; |
| 6 | | должно осуществляться; |
| 5 - 1 | | должно осуществляться в срок не более 60 дней с момента выявления недостатка. |

Требования к обновлению средства

41

| Уровни доверия | Требования |
|----------------|---|
| 6 | информирование потребителей средства о выпуске обновлений;
обеспечение возможности получения обновления средства способами, обеспечивающими его целостность; |
| 5 | в случае получения обновления средства по сетям связи средство должно получать такие обновления с информационного ресурса заявителя;
при доведении обновлений средства до потребителей должны обеспечиваться подлинность и целостность обновлений за счет применения ЭЦП; |
| 4 | доведение информации о выпуске обновлений средства должно осуществляться до каждого потребителя средства; <ul style="list-style-type: none">• путем отправки сообщений на электронные адреса потребителей;• за счет применения компонента средства, обеспечивающего доведение указанной информации до потребителя автоматически; |
| 1 - 3 | доведение информации о выпуске обновлений средства должно осуществляться до каждого потребителя средства способом, обеспечивающим подлинность и целостность доводимой информации (по сетям связи должны обеспечиваться за счет применения ЭЦП). |

Требования к документированию процедур устранения недостатков и обновления средства и к информированию об окончании производства и (или) поддержки безопасности средства

Документирование процедур устранения недостатков и обновления средства должно предусматривать:

- включение в программную и конструкторскую документацию на средство процедур устранения недостатков;
- разработку регламента обновления средства потребителем, включающего порядок получения, установки и контроля установки обновления программного обеспечения средства.

Об окончании производства и (или) поддержки безопасности средства потребители и ФСТЭК России должны быть проинформированы не позднее чем за 1 год до окончания производства и (или) поддержки безопасности средства.

ВОПРОСЫ?