УТВЕРЖДЕНЫ
приказом ФСТЭК России
от 2 июня 2020 г. № 76

Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий
(выписка)

I. Общие положения

1. Настоящие Требования 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 (далее – требования по безопасности информации), применяются к программным и программно-техническим средствам технической защиты информации, средствам обеспечения безопасности информационных технологий, включая защищенные средства обработки информации (далее – средства), и устанавливают уровни, характеризующие безопасность применения средств для обработки и защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа, а также для обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (далее – уровни доверия).

2. Настоящие Требования разработаны в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации» (Собрание законодательства Российской Федерации, 1995, № 27, ст. 2579; 2010, № 18, ст. 2238), постановлением Правительства Российской Федерации от 15 мая 2010 г. № 330 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения», приказом ФСТЭК России от 3 апреля 2018 г. № 55 «Об утверждении Положения о системе сертификации средств защиты информации» (зарегистрирован Минюстом России 11 мая 2018 г., регистрационный № 51063; официальный интернет-портал правовой информации http://www.pravo.gov.ru, 14 мая 2018 г.).

3. Выполнение настоящих Требований является обязательным при проведении работ по оценке соответствия (включая работы по сертификации) средств технической защиты информации и средств обеспечения безопасности

информационных технологий, организуемых ФСТЭК России в пределах своих полномочий в соответствии с Положением о системе сертификации средств защиты информации, утвержденным приказом ФСТЭК России от 3 апреля 2018 г. № 55 «Об утверждении Положения о системе сертификации средств защиты информации».

II. Общие требования по безопасности информации

4. Для дифференциации требований по безопасности информации к средствам устанавливается 6 уровней доверия. Самый низкий уровень – шестой, самый высокий – первый.

Средства, соответствующие 6 уровню доверия, применяются в значимых объектах критической информационной инфраструктуры 3 категории[1], в государственных информационных системах 3 класса защищенности[**], в автоматизированных системах управления производственными и технологическими процессами 3 класса защищенности[***], в информационных системах персональных данных при необходимости обеспечения 3 и 4 уровня защищенности персональных данных[****].

Средства, соответствующие 5 уровню доверия, применяются в значимых объектах критической информационной инфраструктуры 2 категории[*], в государственных информационных системах 2 класса защищенности[**], в автоматизированных системах управления производственными и технологическими процессами 2 класса защищенности[***], в информационных системах персональных данных при необходимости обеспечения 2 уровня защищенности персональных данных[****].

Средства, соответствующие 4 уровню доверия, применяются в значимых объектах критической информационной инфраструктуры 1 категории[*], в государственных информационных системах 1 класса защищенности[**], в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности[***], в информационных системах персональных

---

1 Статья 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736), Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации, утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204; 2019, № 16, ст. 1955).

**[**] Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17 (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608) (с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. № 27 (зарегистрирован Минюстом России 14 марта 2017 г., регистрационный № 45933) и приказом ФСТЭК России от 28 мая 2019 г. № 106 (зарегистрирован Минюстом России 13 сентября 2019 г., регистрационный № 55924).

***[***] Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК России от 14 марта 2014 г. № 31 (зарегистрирован Минюстом России 30 июня 2014 г., регистрационный № 32919) (с изменениями, внесенными приказом ФСТЭК России от 23 марта 2017 г. № 49 (зарегистрирован Минюстом России 30 июня 2017 г., регистрационный № 32919) и приказом ФСТЭК России от 9 августа 2018 г. № 138 (зарегистрирован Минюстом России 5 сентября 2018 г., регистрационный № 52071).

****[****] Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 (Собрание законодательства Российской Федерации, 2012, № 45, ст. 6257).

данных при необходимости обеспечения 1 уровня защищенности персональных данных[****], в информационных системах общего пользования II класса[*****].

5. При проведении сертификации средства защиты информации должно быть подтверждено соответствие средства настоящим Требованиям.

Устанавливается следующее соответствие классов средств защиты информации и средств вычислительной техники уровням доверия:

средства защиты информации 6 класса должны соответствовать 6 уровню доверия;

средства защиты информации 5 класса должны соответствовать 5 уровню доверия;

средства защиты информации 4 класса и средства вычислительной техники 5 класса должны соответствовать 4 уровню доверия.

6. Средство соответствует уровню доверия, если оно удовлетворяет требованиям к разработке и производству средства, проведению испытаний средства, поддержке безопасности средства, приведенным в таблице 1.

Таблица 1

№ п/п	Наименование требования к уровню доверия	Уровень доверия		
		6	5	4
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)	+	+	+

2[*] Статья 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736), Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации, утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204; 2019, № 16, ст. 1955).

[**] Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17 (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608) (с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. № 27 (зарегистрирован Минюстом России 14 марта 2017 г., регистрационный № 45933) и приказом ФСТЭК России от 28 мая 2019 г. № 106 (зарегистрирован Минюстом России 13 сентября 2019 г., регистрационный № 55924).

[***] Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК России от 14 марта 2014 г. № 31 (зарегистрирован Минюстом России 30 июня 2014 г., регистрационный № 32919) (с изменениями, внесенными приказом ФСТЭК России от 23 марта 2017 г. № 49 (зарегистрирован Минюстом России 30 июня 2017 г., регистрационный № 32919) и приказом ФСТЭК России от 9 августа 2018 г. № 138 (зарегистрирован Минюстом России 5 сентября 2018 г., регистрационный № 52071).

[****] Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 (Собрание законодательства Российской Федерации, 2012, № 45, ст. 6257).

[*****] Требования о защите информации, содержащейся в информационных системах общего пользования, утвержденные приказом ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489 (зарегистрирован Минюстом России 13 октября 2010 г., регистрационный № 18704).

	документации			
1.6.	требования к средствам разработки, применяемым для создания 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	+	=	=
2.	Требования к проведению испытаний средства:			
2.1.	требования к тестированию средства	+	+	+
2.2.	требования к испытаниям по выявлению уязвимостей и недекларированных 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	+	=	=

Обозначение «+» в строке требования к уровню доверия указывает на наличие требований, предъявляемых к соответствующему уровню доверия.

Обозначение «=» означает, что требования к уровню доверия совпадают с требованиями, предъявляемыми к предыдущему уровню доверия.

Отсутствие обозначения «+» или «=» означает, что требования к уровню доверия не предъявляются.

III. Требования к разработке и производству средства

7. При разработке средства разработчиком должны быть выполнены процедуры, предусматривающие:

1) разработку модели безопасности средства;

2) проектирование архитектуры безопасности средства;

3) разработку функциональной спецификации средства;

4) проектирование средства;

5) разработку проектной (программной) документации;

6) выбор средств разработки, применяемых для создания средства;

7) управление конфигурацией средства;

8) разработку документации по безопасной разработке средства;

9) разработку эксплуатационной документации.

8. К разработке модели безопасности средства предъявляются следующие требования:

8.1. Требования к разработке модели безопасности средства, соответствующего 6 и 5 уровням доверия, не предъявляются.

8.2. При разработке модели безопасности средства, соответствующего 4 уровню доверия, должны быть указаны 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).

Модель безопасности средства, соответствующего 4 уровню доверия, должна включать описание условий безопасности, выполнение которых указывает на реализацию политик. Выполнение условий безопасности должно быть доказано формальным (математическим) способом. Для условий безопасности неформально (нематематически) должна быть показана их взаимосвязь с режимами функционирования средства. Язык описания модели безопасности должен быть математическим или формализованным (машиночитаемым) и допускать полную независимую от разработчика модели проверку корректности её описания, заданных в ней условий безопасности, а также всех выполненных в модели доказательств.

9. К проектированию архитектуры безопасности средства предъявляются следующие требования:

9.1. Архитектура безопасности средства, соответствующего 6 уровню доверия, должна обеспечивать:

невозможность обхода функций безопасности средства;

защиту функций безопасности средства от несанкционированного доступа к ним.

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.

9.2. Требования к проектированию архитектуры безопасности средства, соответствующего 5 и 4 уровням доверия, соответствуют требованиям к проектированию архитектуры безопасности средства, соответствующего 6 уровню доверия.

10. К разработке функциональной спецификации средства предъявляются следующие требования:

10.1. Разработка функциональной спецификации средства, соответствующего 6 уровню доверия, должна предусматривать:

разработку описания назначения и способов использования каждого интерфейса функций безопасности;

идентификацию параметров, связанных с каждым интерфейсом функций безопасности;

идентификацию интерфейсов средства, не влияющих на функции безопасности средства.

Функциональная спецификация средства должна включать:

перечень всех функций средства, включая функции безопасности, реализуемые программным обеспечением и аппаратной платформой средства;

описание назначения и способов использования каждого интерфейса функций безопасности и иных функций средства;

описание параметров, связанных с каждым интерфейсом функций безопасности и иных функций средства;

перечень интерфейсов, не влияющих на функции безопасности средства.

Функциональная спецификация аппаратной платформы средства должна включать описание назначения и способов использования каждого интерфейса аппаратной платформы средства.

10.2. При разработке функциональной спецификации средства, соответствующего 5 уровню доверия, наряду с требованиями, установленными пунктом 10.1 настоящих Требований, должны быть разработаны и включены в спецификацию описания:

действий с каждым интерфейсом функций безопасности;

сообщений о возможных ошибках, связанных с выполнением функций безопасности.

10.3. При разработке функциональной спецификации средства, соответствующего 4 уровню доверия, наряду с требованиями, установленными пунктами 10.1 и 10.2 настоящих Требований, должны быть разработаны и включены в спецификацию описания:

действий с каждым интерфейсом функций безопасности, не влияющим на выполнение требований, предъявляемых к средству;

сообщений об ошибках, которые могут возникнуть при выполнении функций безопасности и вызове каждого интерфейса функций безопасности;

параметров, связанных с каждым интерфейсом функций безопасности аппаратной платформы средства;

интерфейсов, не влияющих на функции безопасности аппаратной платформы средства;

всех функций безопасности, реализуемых аппаратной платформой средства.

11. К проектированию средства предъявляются следующие требования:

11.1. Проектирование средства, соответствующего 6 уровню доверия, должно предусматривать:

определение перечня подсистем, реализующих функции безопасности средства;

определение перечня подсистем, поддерживающих выполнение функций безопасности;

определение перечня подсистем, не влияющих на выполнение функций безопасности;

проектирование подсистем, реализующих функции безопасности средства;

проектирование иных подсистем таким образом, чтобы они не оказывали влияния на выполнение функций безопасности средства;

определение способов взаимодействия подсистем, реализующих функции безопасности, с иными подсистемами, обеспечивающих невозможность влияния на выполнение функций безопасности средства;

определение и проектирование для каждой подсистемы, реализующей функции безопасности, перечня входящих в ее состав модулей, осуществляющих выполнение функций безопасности;

определение способов взаимодействия модулей, осуществляющих выполнение функций безопасности, с иными модулями, обеспечивающих невозможность влияния на выполнение функций безопасности средства.

11.2. Требования к проектированию средства, соответствующего 5 и 4 уровням доверия, соответствуют требованиям к проектированию средства, соответствующего 6 уровню доверия.

12. К разработке проектной (программной) документации средства предъявляются следующие требования:

12.1. Проектная (программная) документация средства, соответствующего 6 уровню доверия, должна включать:

проект на уровне подсистем средства (эскизный проект);

проект на уровне модулей средства (технический проект).

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.

Технический проект должен включать:

описание структуры средства на уровне модулей;

описание всех модулей средства (для модулей средства, реализующих функции безопасности, – описание интерфейсов, возвращаемых ими в ответ на запросы значений, 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.

Положения эскизного и технического проектов могут быть объединены в одном документе.

Для аппаратной платформы средства должен быть разработан (представлен) перечень аппаратных устройств (микросхем), которые влияют на выполнение функций безопасности и (или) могут быть использованы для реализации угроз безопасности информации.

12.2. Проектная (программная) документация средства, соответствующего 5 уровню доверия, наряду с требованиями, установленными пунктом 12.1 настоящих Требований, должна включать:

для аппаратной платформы средства – структурную и функциональную схемы аппаратной платформы средства;

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, заимствованного у сторонних изготовителей, не реализующего функции безопасности и не влияющего на реализацию функций безопасности.

Документация на средство должна содержать информацию о соответствии указанных сведений модулям, описанным в проектной документации.

В случае отсутствия сведений о заимствованных компонентах средства должны быть спроектированы, реализованы и описаны в документации на средство меры защиты информации, направленные на блокирование эксплуатации возможных уязвимостей и реализуемых заимствованными элементами (компонентами) потенциально опасных возможностей.

Отсутствующие сведения о заимствованных компонентах средства могут быть получены путем использования методов обратной разработки (реверс-инжиниринга). Способы и методы получения отсутствующих сведений о заимствованных элементах должны быть описаны в документации на средство, представляемой на испытания, и могут быть использованы при проведении испытаний.

Сведения об аппаратной платформе средства должны быть включены в единый реестр российской радиоэлектронной продукции*.

12.3. Проектная (программная) документация средства, соответствующего 4 уровню доверия, наряду с требованиями, установленными пунктами 12.1 и 12.2 настоящих Требований, для аппаратной платформы средства должна включать:

структурные и функциональные схемы, техническую документацию аппаратных средств, входящих в аппаратную платформу;

представление (код) на языке описания аппаратных средств;

описание потенциально опасных элементов (компонентов), входящих в состав аппаратной платформы средства, которые влияют на выполнение функций безопасности и (или) могут быть использованы для реализации угроз безопасности информации.

Сведения о процессорах или микросхемах, выполняющих функции процессоров (микроконтроллеры), элементах памяти, сетевых картах, графических адаптерах аппаратной платформы средства должны быть включены в единый реестр российской радиоэлектронной продукции.

13. К средствам разработки, применяемым для создания средства, предъявляются следующие требования:

*Правила формирования и ведения единого реестра российской радиоэлектронной продукции утверждены постановлением Правительства Российской Федерации от 10 июля 2019 г. № 878 (Собрание законодательства Российской Федерации, 2019, № 29, ст. 4023; № 29, ст. 4023).

13.1. На выбранные средства разработки, применяемые для создания средства, соответствующего 6 уровню доверия, должна быть разработана документация, включающая описания:

средств разработки, применяемых для создания средства;

использованных опций средств разработки, применяемых для создания средства.

13.2. Требования к средствам разработки, применяемым для создания средства, соответствующего 5 и 4 уровням доверия, соответствуют требованиям к средствам разработки, применяемым для создания средства, соответствующего 6 уровню доверия.

14. К управлению конфигурацией средства предъявляются следующие требования:

14.1. Управление конфигурацией средства, соответствующего 6 уровню доверия, должно предусматривать управление изменениями средства и документации и обеспечение их уникальной маркировки.

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.

14.2. Управление конфигурацией средства, соответствующего 5 уровню доверия, наряду с требованиями, установленными пунктом 14.1 настоящих Требований, должно предусматривать:

управление изменениями частей (элементов, компонентов) средства;

обеспечение уникальной идентификации всех элементов конфигурации.

Документация по управлению конфигурацией средства дополнительно должна включать:

описание метода, используемого для уникальной идентификации элементов конфигурации;

описание уникальных идентификаторов всех элементов конфигурации;

части (элементы, компоненты) средства в списке элементов конфигурации.

Для каждого элемента конфигурации в списке элементов конфигурации должен быть указан разработчик.

14.3. Управление конфигурацией средства, соответствующего 4 уровню доверия, наряду с требованиями, установленными пунктами 14.1 и 14.2 настоящих Требований, должно предусматривать:

управление изменениями средства, в том числе изменениями исходных текстов программного обеспечения и аппаратной платформы средства;

применение автоматизированных мер контроля, обеспечивающих внесение в элементы конфигурации только санкционированных изменений;

организацию процедур приемки модифицированных или вновь созданных элементов конфигурации.

Документация по управлению конфигурацией средства дополнительно должна включать:

сведения о составе средства, в том числе сведения об исходных текстах и аппаратной платформе средства, в списке элементов конфигурации;

описание автоматизированных мер контроля, которые применяются для обеспечения внесения в элементы конфигурации только санкционированных изменений;

план управления конфигурацией, содержащий описание процедур, используемых для приемки модифицированных или вновь созданных элементов конфигурации.

Управление конфигурацией (настройкой) аппаратной платформы средства должно предусматривать изменение конфигурации (настройки) аппаратной платформы средства, её документации, обеспечение их уникальной маркировки.

Документация по изменению конфигурации (настройки) аппаратной платформы средства должна включать:

описание уникальной маркировки аппаратной платформы средства;

список элементов конфигурации (настройки) средства;

порядок управления изменениями аппаратной платформы средства и документации.

15. К разработке документации по безопасной разработке средства предъявляются следующие требования:

15.1. На средство, соответствующее 6 уровню доверия, должна быть разработана документация по безопасной разработке 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.

15.2. Требования к разработке документации по безопасной разработке средства, соответствующего 5 уровню доверия, соответствуют требованиям к разработке документации по безопасной разработке средства, соответствующего 6 уровню доверия.

15.3. Разработка документации по безопасной разработке средства, соответствующего 4 уровню доверия, наряду с требованиями, установленными пунктом 15.1 настоящих Требований, должна предусматривать разработку документации по безопасной разработке аппаратной платформы средства, которая должна включать описание организационных и технических мер безопасности, применяемых в среде разработки аппаратной платформы средства для защиты целостности проектной документации и аппаратной платформы средства.

16. К разработке эксплуатационной документации предъявляются следующие требования:

16.1. На средство, соответствующее 6 уровню доверия, включая его аппаратную платформу, должна быть разработана следующая эксплуатационная документация:

формуляр средства;

руководство пользователя средства;

руководство администратора средства.

Формуляр средства должен содержать контрольные суммы дистрибутива и исполняемых файлов программного обеспечения, которые должны уточняться при обновлении средства в соответствии с настоящими Требованиями, а также состав аппаратной платформы средства.

Руководство пользователя средства должно содержать описание:

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.

Руководство администратора средства должно содержать описание:

действий по приемке поставленного средства;

действий по безопасной установке и настройке средства;

действий по реализации функций безопасности среды функционирования средства.

16.2. Требования к разработке эксплуатационной документации средства, соответствующего 5 и 4 уровням доверия, соответствуют требованиям к разработке эксплуатационной документации средства, соответствующего 6 уровню доверия.

IV. Требования к проведению испытаний средства

17. В отношении средства должны быть проведены испытания, предусматривающие:

1) тестирование средства;

2) испытания по выявлению уязвимостей и недекларированных возможностей средства;

3) проведение анализа скрытых каналов в средстве.

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

Тестирование, испытания по выявлению уязвимостей и недекларированных возможностей, а также анализ скрытых каналов проводятся изготовителем в ходе приемочных испытаний средства и испытательной лабораторией в ходе сертификационных испытаний средства.

18. К тестированию средства предъявляются следующие требования:

18.1. Тестовая документация на средство, соответствующее 6 уровню доверия, 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, 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.

18.2. Тестовая документация на средство, соответствующее 5 уровню доверия, наряду с требованиями, установленными пунктом 18.1 настоящих Требований, должна включать описание сопоставления тестов с подсистемами средства, описанными в эскизном проекте, демонстрирующее их полное покрытие тестами.

При проведении тестирования средства проводится оценка влияния на подсистемы средства, реализующие функции безопасности, иных подсистем средства.

18.3. Тестовая документация на средство, соответствующее 4 уровню доверия, наряду с требованиями, установленными пунктами 18.1 и 18.2 настоящих Требований, должна включать описание сопоставления тестов с модулями средства, реализующими функции безопасности и описанными в техническом проекте, демонстрирующее полное покрытие тестами функций безопасности.

При проведении тестирования средства проводится оценка влияния на модули средства, реализующие функции безопасности, иных модулей средства.

19. К испытаниям по выявлению уязвимостей и недекларированных возможностей средства предъявляются следующие требования:

19.1. Испытания программного обеспечения средства, соответствующего 6 уровню доверия, должны быть проведены по 6 уровню контроля.

Для аппаратной платформы программно-технического средства должна быть выполнена проверка перечня аппаратных устройств (микросхем), которые влияют на выполнение функций безопасности и (или) могут быть использованы для реализации угроз безопасности информации.

19.2. Испытания программного обеспечения средства, соответствующего 5 уровню доверия, должны быть проведены по 5 уровню контроля.

Для аппаратной платформы программно-технического средства наряду с требованиями, установленными пунктом 19.1 настоящих Требований, должна быть выполнена проверка соответствия аппаратной платформы её структурной и функциональной схемам, а также сведениям, приведенным в формуляре средства.

19.3. Испытания программного обеспечения средства, соответствующего 4 уровню доверия, должны быть проведены по 4 уровню контроля.

Для аппаратной платформы программно-технического средства наряду с требованиями, установленными пунктами 19.1 и 19.2 настоящих Требований, должна быть выполнена проверка:

соответствия элементов (компонентов) аппаратной платформы структурной и функциональной схеме элементов (компонентов) аппаратной платформы средства;

потенциально опасных элементов (компонентов), входящих в состав аппаратной платформы, которые влияют на выполнение функций безопасности и (или) могут быть использованы для реализации угроз безопасности информации.

20. К проведению анализа скрытых каналов в средстве предъявляются следующие требования:

20.1. Требования к проведению анализа скрытых каналов в средстве, соответствующем 6 и 5 уровню доверия, не предъявляются.

20.2. В средстве, соответствующем 4 уровню доверия, должны быть проведены идентификация и анализ скрытых каналов по памяти, основанных на использовании ресурсов памяти, в которые записывается защищаемая информация (сокрытие информации в структурированных и неструктурированных данных) и которые не учитываются разработчиками системы защиты информации информационной (автоматизированной) системы и не выявляются применяемыми средствами защиты информации.

Анализ идентифицированных типов скрытых каналов должен включать:

оценку потенциальной пропускной способности идентифицированных скрытых каналов с использованием формальных (математических), технических методов и (или) методов моделирования;

разработку требований для среды функционирования средства с целью ограничения, мониторинга, полного или частичного устранения идентифицированных скрытых каналов, которые могут возникнуть в информационных (автоматизированных) системах вследствие использования в них средства.

Документация анализа скрытых каналов должна включать:

идентификацию скрытых каналов (если скрытые каналы выявлены);

оценку пропускной способности идентифицированных скрытых каналов (если скрытые каналы выявлены);

описание процедур, использованных для вынесения заключения о существовании и (или) отсутствии скрытых каналов, и информацию, использованную при анализе скрытых каналов;

описание предположений (быстродействие процессора, системная конфигурация, объем памяти и (или) иных), сделанных при анализе скрытых каналов;

описание способа, использованного для оценки пропускной способности канала для наиболее опасного сценария (если скрытые каналы выявлены);

описание наиболее опасного сценария использования каждого идентифицированного скрытого канала (если скрытые каналы выявлены);

сведения о включении в функциональную спецификацию и эскизный проект описания механизмов средства, направленных на ограничение, мониторинг, полное или частичное устранение идентифицированных скрытых каналов, которые могут возникнуть в информационных (автоматизированных) системах вследствие использования в них средства (если скрытые каналы выявлены и требуются соответствующие механизмы средства);

сведения о включении в руководство администратора и (или) руководство пользователя требований для среды функционирования средства с целью ограничения, мониторинга, полного или частичного устранения идентифицированных скрытых каналов, которые могут возникнуть в информационных (автоматизированных) системах вследствие использования в них средства (если скрытые каналы выявлены).

V. Требования к поддержке безопасности средства

21. Средство должно обеспечиваться поддержкой безопасности средства, предусматривающей:

1) устранение недостатков и дефектов средства, в том числе устранение уязвимостей и недекларированных возможностей средства (далее – устранение недостатков средства);

2) информирование потребителей об обновлении программного обеспечения средства и доведение до потребителей обновлений программного обеспечения средства, а также изменений в эксплуатационную документацию (далее – обновление средства);

3) документирование процедур устранения недостатков и обновления средства;

4) информирование об окончании производства и (или) поддержки безопасности средства.

Поддержка безопасности средства обеспечивается заявителем на осуществление сертификации средства с привлечением разработчика и изготовителя средства.

22. К устранению недостатков средства предъявляются следующие требования:

22.1. Устранение недостатков средства, соответствующего 6 уровню доверия, должно предусматривать:

поиск в доступных источниках информации о недостатках средства, в том числе о недостатках в компонентах средства, заимствованных у сторонних изготовителей;

получение сведений о недостатках средства от потребителей средства;

проведение испытаний средства по выявлению недостатков в средстве, в том числе по выявлению уязвимостей и недекларированных возможностей средства;

разработку 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 банка данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2018, № 20, ст. 2818);

устранение недостатков средства путем доработки средства или его отдельных компонентов, принятие иных мер, снижающих возможность эксплуатации уязвимостей;

тестирование (испытания) доработанного средства или его отдельных компонентов на предмет устранения влияния обновлений средства на его функции безопасности, подтверждения устранения уязвимостей, невнесения новых уязвимостей в средство.

22.2. Устранение недостатков средства, соответствующего 5 уровню доверия, наряду с требованиями, установленными пунктом 22.1 настоящих Требований, должно предусматривать:

разработку компенсирующих мер по защите информации или ограничений по применению средства, а также доведение информации о недостатках и указанных мерах и ограничениях до потребителей не позднее 72 часов с момента выявления недостатка;

доработку средства, в том числе разработку обновлений программного обеспечения средства, или разработку мер по защите информации, нейтрализующих недостаток, в срок не более 60 дней с момента выявления недостатка.

22.3. Устранение недостатков средства, соответствующего 4 уровню доверия, наряду с требованиями, установленными пунктами 22.1 и 22.2 настоящих Требований, должно предусматривать:

разработку компенсирующих мер по защите информации или ограничений по применению средства, а также доведение информации о таких мерах и ограничениях до потребителей в срок не более 48 часов с момента выявления недостатка;

доведение информации о недостатках средства, а также о компенсирующих мерах по защите информации или ограничениях по применению до каждого потребителя сертифицированного средства путем отправки сообщений на электронные адреса потребителей или за счет применения компонента средства, обеспечивающего доведение указанной информации до потребителя автоматически.

23. К обновлению средства предъявляются следующие требования:

23.1. Обновление средства, соответствующего 6 уровню доверия, должно предусматривать:

информирование потребителей средства о выпуске обновлений;

обеспечение возможности получения обновления средства способами, обеспечивающими его целостность.

23.2. Наряду с требованиями, установленными пунктом 23.1 настоящих Требований, к обновлению средства, соответствующего 5 уровню доверия, предъявляются следующие требования:

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 электронной цифровой подписи.

23.3. Наряду с требованиями, установленными пунктами 23.1 и 23.2 настоящих Требований, доведение информации о выпуске обновлений средства, соответствующего 4 уровню доверия, должно осуществляться до каждого потребителя сертифицированного средства путем отправки сообщений на электронные адреса потребителей или за счет применения компонента средства, обеспечивающего доведение указанной информации до потребителя автоматически.

24. К документированию процедур устранения недостатков и обновления средства предъявляются следующие требования:

24.1. Документирование процедур устранения недостатков и обновления средства, соответствующего 6 уровню доверия, 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.

24.2. Требования к документированию процедур устранения недостатков и обновления средства, соответствующего 5 и 4 уровням доверия, соответствуют требованиям к документированию процедур устранения недостатков и обновления средства, соответствующего 6 уровню доверия.

25. К информированию об окончании производства и (или) поддержки безопасности средства предъявляются следующие требования:

25.1. Об окончании производства и (или) поддержки безопасности средства, соответствующего 6 уровню доверия, потребители и ФСТЭК России должны быть проинформированы не позднее чем за 1 год до окончания производства и (или) поддержки безопасности средства.

25.2. Требования к информированию об окончании производства и (или) поддержки безопасности средства, соответствующего 5 и 4 уровням доверия, соответствуют требованиям к информированию об окончании производства и (или) поддержки безопасности средства, соответствующего 6 уровню доверия.

_____

Примечание

В соответствии с приказом ФСТЭК России от 2 июня 2020 г. № 76 настоящие Требования вступают в силу с 1 января 2021 г., за исключением:

абзаца седьмого пункта 12.2, который вступает в силу с 1 января 2022 г.;

абзаца пятого пункта 12.3, который вступает в силу с 1 января 2028 г.

Приказ ФСТЭК России от 30 июля 2018 г. № 131 «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (зарегистрирован Министерством юстиции Российской Федерации 14 ноября 2018 г., регистрационный № 52686) признается утратившим силу с 1 января 2021 г..