УТВЕРЖДЕНЫ
приказом ФСТЭК России
от «30» июля 2018 г. № 131

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 (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; 1996, № 18, ст. 2142; 1999, № 14, ст. 1722; 2004, № 52, ст. 5480; 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.).

Настоящие требования предназначены для организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по созданию

средств, заявителей на осуществление сертификации, а также для испытательных лабораторий и органов по сертификации, выполняющих работы по сертификации средств на соответствие обязательным требованиям по безопасности информации.

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.

II. Общие требования

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[*], 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

---

[*] Устанавливается в соответствии со статьей 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) и Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204).

[**] Устанавливается в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными 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; Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 15 марта 2017 г.).

[***] Устанавливается в соответствии с Требованиями 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, утвержденными 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; Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 26.04.2017

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

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

5. Средства защиты информации, в том числе средства вычислительной техники, при проведении сертификационных испытаний на соответствие требованиям по безопасности информации к функциям безопасности должны проходить сертификационные испытания на соответствие 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.

---

[*] Устанавливается в соответствии со статьей 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) и Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204).

[**] Устанавливается в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными 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; Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 15 марта 2017 г.).

[***] Устанавливается в соответствии с Требованиями 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, утвержденными 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; Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 26.04.2017).

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

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

6. Средство соответствует уровню доверия, если оно удовлетворяет соответствующим 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 представления реализации средства	+	+	+
1.6.	требования к средствам, 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 руководства пользователя средства	+	=	=
1.10.	требования к разработке руководства администратора средства	+	=	=
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	+	=	=

Обозначение «+» в строке требования к уровню доверия указывает на новые или дополнительные требования, предъявляемые к соответствующему уровню доверия.

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

III. Требования к разработке средства

7. При разработке средства 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 представления реализации средства;

6) выбор средств, применяемых при разработке средства;

7) управление конфигурацией средства;

8) разработку документации по безопасной разработке средства;

9) разработку руководства пользователя средства;

10) разработку руководства администратора средства.

Требования к разработке средства, соответствующего 6 уровню доверия

8. Требования к разработке модели безопасности средства, соответствующего 6 уровню доверия, не предъявляются.

9. Требования к проектированию архитектуры безопасности средства.

Спроектированная архитектура безопасности средства 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.

10. Требования к разработке функциональной спецификации средства.

Разработка функциональной спецификации средства должна предусматривать:

разработку описания назначения и способов использования каждого интерфейса функций безопасности (при наличии функций безопасности);

идентификацию параметров, связанных с каждым интерфейсом функций безопасности (при наличии функций безопасности);

идентификацию интерфейсов, не влияющих на функции безопасности средства (при наличии функций безопасности и наличии таких интерфейсов).

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).

11. Требования к проектированию средства.

Проектирование средства 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.

Проектная документация средства 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.

12. Требования к разработке представления реализации средства.

Формуляр средства должен содержать контрольные суммы дистрибутива и исполняемых файлов программного обеспечения средства. Контрольные суммы должны уточняться при обновлении средства в соответствии с настоящими Требованиями.

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.

13. Требования к средствам, применяемым для разработки средства.

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

средств, применяемых для разработки средства;

использованных опций средств, применяемых для разработки средства.

14. Требования к управлению конфигурацией средства.

Управление конфигурацией средства 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.

15. Требования к разработке документации 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.

16. Требования к разработке 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.

17. Требования к разработке 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.

Требования к разработке средства, соответствующего 5 уровню доверия

18. Требования к разработке модели безопасности средства, соответствующего 5 уровню доверия, не предъявляются.

19. Требования к проектированию архитектуры безопасности средства совпадают с требованиями, установленными пунктом 9 настоящих Требований.

20. При разработке функциональной спецификации средства наряду с требованиями, установленными пунктом 10 настоящих Требований, должны быть разработаны описания:

всех функций безопасности (при наличии функций безопасности);

действий с каждым интерфейсом функций безопасности (при наличии функций безопасности);

сообщений о возможных ошибках, связанных с действиями по выполнению функции безопасности (при наличии функций безопасности).

В функциональную спецификацию должны быть включены описания:

всех функций безопасности (при наличии функций безопасности);

действий с каждым интерфейсом функций безопасности (при наличии функций безопасности);

возможных сообщений об ошибках, связанных с выполнением функций безопасности (при наличии функций безопасности).

21. Требования к проектированию средства совпадают с требованиями, установленными пунктом 11 настоящих Требований.

22. Представление реализации средства наряду с требованием, установленным пунктом 12 настоящих Требований, должно включать:

для аппаратной платформы средства (при наличии аппаратной платформы) – структурные схемы и техническая документация 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.

23. Требования к средствам, применяемым для разработки средства, совпадают с требованиями, установленными пунктом 13 настоящих Требований.

24. Управление конфигурацией средства наряду с требованиями, установленными пунктом 14 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.

25. Требования к разработке документации по безопасности разработки средства совпадают с требованиями, установленными пунктом 15 настоящих Требований.

26. Требования к разработке руководства пользователя средства совпадают с требованиями, установленными пунктом 16 настоящих Требований.

27. Требования к разработке руководства администратора средства совпадают с требованиями, установленными пунктом 17 настоящих Требований.

Требования к разработке средства, соответствующего 4 уровню доверия

28. При разработке модели безопасности средства должны быть отражены следующие сведения:

реализуемые политики управления доступом (если применимо);

реализуемые политики фильтрации информационных потоков (если применимо).

Модель безопасности должна включать описание условий безопасности, выполнение которых указывает на реализацию политик. Доверие к модели безопасности должно быть достигнуто формальным (математическим) доказательством того, что в ней не содержится противоречий, то есть выполняются условия безопасности. 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.

29. Требования к проектированию архитектуры безопасности средства совпадают с требованиями, установленными пунктом 9 настоящих Требований.

30. Разработка функциональной спецификации средства наряду с требованиями, установленными пунктом 20 настоящих Требований, должна предусматривать разработку описаний:

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

сообщений обо всех ошибках, которые могут возникнуть при вызове каждого интерфейса функций безопасности.

В функциональную спецификацию дополнительно должны быть включены описания:

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

сообщений обо всех ошибках, которые могут возникнуть при вызове каждого интерфейса функций безопасности.

31. Требования к проектированию средства совпадают с требованиями, установленными пунктом 11 настоящих Требований.

32. Представление реализации средства наряду с требованиями, установленными пунктом 22 настоящих Требований, должно включать 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.

33. Требования к средствам, применяемым для разработки средства, совпадают с требованиями, установленными пунктом 13 настоящих Требований.

34. Управление конфигурацией средства наряду с требованиями, установленными пунктом 24 настоящих Требований, должно предусматривать:

управление изменениями представления реализации 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:

представление реализации 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.

35. Требования к разработке документации по безопасности разработки средства совпадают с требованиями, установленными пунктом 15 настоящих Требований.

36. Требования к разработке руководства пользователя средства совпадают с требованиями, установленными пунктом 16 настоящих Требований.

37. Требования к разработке руководства администратора средства совпадают с требованиями, установленными пунктом 17 настоящих Требований.

IV. Требования к проведению испытаний средства

68. 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.

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

Требования к проведению испытаний средства, соответствующего 6 уровню доверия

69. Для подтверждения выполнения требований по безопасности информации, предъявляемых к средству, средство должно быть протестировано в соответствии с разработанными для этой цели тестами.

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.

70. Испытания по выявлению уязвимостей и недекларированных возможностей средства 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.

71. Требования к проведению анализа скрытых каналов в средстве 6 уровня доверия не предъявляются.

Требования к проведению испытаний средства, соответствующего 5 уровню доверия

72. При проведении тестирования средства наряду с требованиями, установленными пунктом 69 настоящих Требований, тестовая документация должна включать описание сопоставления тестов с подсистемами средства, описанными в эскизном проекте, демонстрирующее их полное покрытие тестами.

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

73. Испытания по выявлению уязвимостей и недекларированных возможностей программного обеспечения средства должны быть проведены по 5 уровню контроля.

Для аппаратной платформы программно-технического средства наряду с требованиями, установленными пунктом 70 настоящих Требований, должна быть выполнена проверка соответствия аппаратной платформы его структурной схеме.

74. В средстве 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 описание 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).

Требования к проведению испытаний средства, соответствующего 4 уровню доверия

75. При проведении тестирования средства наряду с требованиями, установленными пунктом 72 настоящих Требований, тестовая документация должна включать описание сопоставления тестов с модулями средства, реализующими функции безопасности (при наличии функций безопасности) и описанными в техническом проекте, демонстрирующее полное покрытие тестами функций безопасности.

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

76. Испытания по выявлению уязвимостей и недекларированных возможностей программного обеспечения средства должны быть проведены по 4 уровню контроля.

Для аппаратной платформы программно-технического средства наряду с требованиями, установленными пунктом 74 настоящих Требований, должны быть выполнены:

проверка соответствия аппаратной платформы его функциональной схеме;

проверка применения микросхем в устройстве по назначению, а также параметров микросхем в соответствии с технической документацией.

77. Требования к проведению анализа скрытых каналов в средстве совпадают с требованиями, установленными пунктом 74 настоящих Требований.

V. Требования к поддержке безопасности средства

87. Средство должно обеспечиваться поддержкой безопасности, 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.

Требования к поддержке безопасности средства, соответствующего 6 уровню доверия

88. Устранение недостатков средства 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;

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.

89. Обновление средства должно предусматривать:

информирование потребителей средства о выпуске обновлений;

обеспечение возможности получения обновления средства способами, обеспечивающими его целостность.

90. 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.

91. 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.

Требования к поддержке безопасности средства, соответствующего 5 уровню доверия

92. Наряду с требованиями к устранению недостатков средства, установленными пунктом 88 настоящих Требований, дополнительно предъявляются следующие требования:

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

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

93. Наряду с требованиями к обновлению средства, установленными пунктом 89 настоящих Требований, дополнительно 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.

94. Требования к документированию процедур устранения недостатков и обновления средства совпадают с требованиями, установленными пунктом 90 настоящих Требований.

95. Требования к информированию об окончании производства и (или) поддержки безопасности средства совпадают с требованиями, установленными пунктом 91 настоящих Требований.

Требования к поддержке безопасности средства, соответствующего 4 уровню доверия

96. Наряду с требованиями к устранению недостатков средства, установленными пунктом 92 настоящих Требований, дополнительно предъявляются следующие требования:

разработка компенсирующих мер по защите информации или ограничений по применению средства, а также доведение информации о таких мерах и ограничениях до потребителей должны осуществляться 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 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.

97. Наряду с требованиями к обновлению средства, установленными пунктом 93 настоящих Требований, доведение информации о выпуске обновлений средства 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.

98. Требования к документированию процедур устранения недостатков и обновления средства совпадают с требованиями, установленными пунктом 90 настоящих Требований.

99. Требования к информированию об окончании производства и (или) поддержки безопасности средства совпадают с требованиями, установленными пунктом 91 настоящих Требований.