

ГОСУДАРСТВЕННАЯ КОРПОРАЦИЯ ПО АТОМНОЙ ЭНЕРГИИ «РОСАТОМ»

Сертификация программного обеспечения АСУТП для применения на объектах критической информационной инфраструктуры

Начальник научно-исследовательского
отдела по сертификации средств защиты
информации, руководитель испытательной
лаборатории ФГУП «РФЯЦ-ВНИИЭФ»

25.04.2019

Ужесточение требований по защите информации со стороны государства, как ответ на мировые киберугрозы (1/4)

В последние годы осуществляется непрерывное ужесточение требований к защите информации со стороны регуляторов

❖ Указом Президента РФ утверждена Доктрина информационной безопасности РФ №646

❖ С 1 января 2018 года вступил в силу Федеральный закон №187

“О безопасности критической информационной инфраструктуры Российской Федерации”



В развитие Федерального закона были выпущены, либо внесены изменения в следующие нормативные правовые акты:

❑ Указ Президента РФ от 22.12.2017 N 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ»

❑ Постановление Правительства РФ от 17.02.2018 N 162
«Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»



❑ Постановление Правительства РФ от 08.02.2018 N 127
"Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений«



❑ Приказ ФСТЭК России от 25.12.2017 N 239 (ред. от 09.08.2018)
«Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»(Зарегистрировано в Минюсте России 26.03.2018 N 50524)

Ужесточение требований по защите информации со стороны государства, как ответ на мировые киберугрозы (2/4)

В последние годы осуществляется непрерывное ужесточение требований к защите информации со стороны регуляторов

❖ Указом Президента РФ утверждена Доктрина информационной безопасности РФ №646

❖ С 1 января 2018 года вступил в силу Федеральный закон №187

“О безопасности критической информационной инфраструктуры Российской Федерации”

В развитие Федерального закона были выпущены, либо внесены изменения в следующие нормативные правовые акты:

- ❑ Приказ ФСБ России от 24.07.2018 N 366 «О Национальном координационном центре по компьютерным инцидентам» (вместе с "Положением о Национальном координационном центре по компьютерным инцидентам") (Зарегистрировано в Минюсте России 06.09.2018 N 52109)
- ❑ Приказ ФСТЭК России от 22.12.2017 N 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» (Зарегистрировано в Минюсте России 13.04.2018 N 50753)
- ❑ Приказ ФСТЭК России от 21.12.2017 N 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (Зарегистрировано в Минюсте России 22.02.2018 N 50118)
- ❑ Приказ ФСТЭК России от 11.12.2017 N 229 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (Зарегистрировано в Минюсте России 28.12.2017 N 49500)



Ужесточение требований по защите информации со стороны государства, как ответ на мировые киберугрозы (3/4)

❖ Утверждены требования безопасности к средствам:

- ✓ обнаружения вторжения (приказ ФСТЭК России от 06.12.2011 № 638);
- ✓ антивирусной защиты (приказ ФСТЭК России от 20.03.2012 № 28);
- ✓ доверенной загрузки (приказ ФСТЭК России от 27.09.2013 № 119);
- ✓ контроля съемных машинных носителей информации (от 28.07.2014 № 87);
- ✓ межсетевого экранирования (приказ ФСТЭК России от 09.02.2016 № 9);
- ✓ к операционным системам (приказ ФСТЭК России от 19.08.2016 №119).



❖ Утверждены «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (приказ ФСТЭК России от 30 июля 2018 г. № 131)



❖ Утверждена «Методика выявления уязвимостей и недеklarированных возможностей в программном обеспечении» (ФСТЭК России 11 февраля 2019 г)

❖ Анонсируются Требования безопасности к:

- ✓ системам управления базами данных;
- ✓ средствам виртуализации и средствам управления потоками (меткам конфиденциальности);
- ✓ автоматизированным рабочим местам в защищенном исполнении;
- ✓ средствам антивирусной защиты информации в автоматизированных системах управления производственными технологическими процессами;
- ✓ средствам однонаправленной передачи информации и мобильным средствам обработки информации.



Ужесточение требований по защите информации со стороны государства, как ответ на мировые киберугрозы (4/4)

- ❖ **Определен порядок классификации и требования для информационных систем, не обрабатывающих государственную тайну:**
 - ✓ Информационные системы персональных данных (ПП РФ от 01.11.2012 №1119, приказ ФСТЭК России от 18.02.2013 №21 с изменениями 2017года);
 - ✓ Государственные информационные системы (приказ ФСТЭК России от 11.02.2013 №17 с изменениями 2017года);
 - ✓ Автоматизированные системы управления ТП (приказ ФСТЭК России от 14.03.2014 №31 с изменениями 2017 года);
 - ✓ Информационные системы общего пользования (приказ ФСБ и ФСТЭК России от 31.08.2010 №416/489)
 - ✓ Информационные системы управления производством (приказ ФСТЭК России от 27.02.2017 №31).
- ❖ **Переход на сертификацию по требованиям ГОСТ Р ИСО/МЭК 15408-(1, 2, 3) (международные стандарты)**
- ❖ **Введено в действие «новое» Положение о системе сертификации средств защиты информации** (приказ ФСТЭК России от 03 апреля 2018 г. № 55)
- ❖ **С 2014 года обязательным этапом сертификационных испытаний является проведение анализа уязвимостей средств защиты информации и сред их функционирования** (информационным сообщением от 2016 года введена методика проверок).

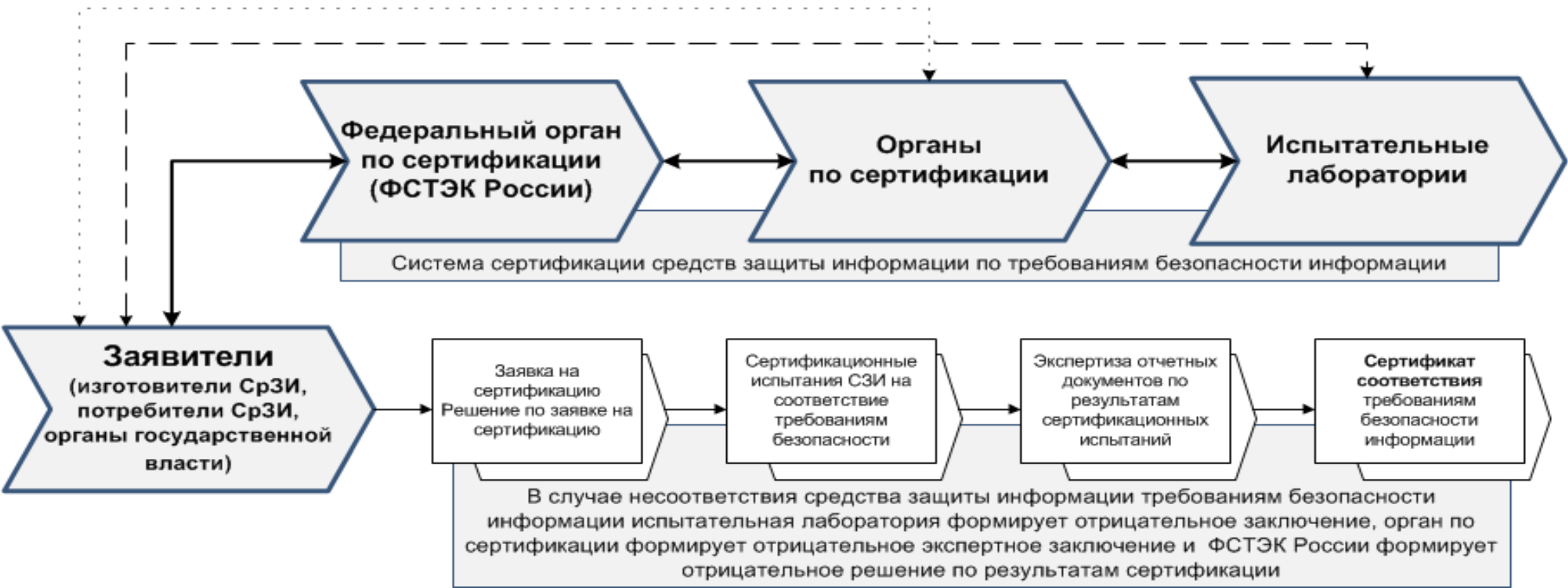


Система сертификации средств защиты информации

Система сертификация средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00. Базовые НМД



Организационная структура системы сертификации средств защиты информации ФСТЭК России



- * по состоянию на 25.04.2019г. данные взяты с официального сайта ФСТЭК России в сети общего доступа Интернет www.fstec.ru
- ** организации, имеющие лицензию ФСТЭК России на деятельность по разработке средств защиты конфиденциальной информации, в данной статистике не учтены организации, разрабатывающие СЗИ, составляющей государственную тайну

*	Органы по сертификации	Испытательные лаборатории	Разработчики средств защиты
Количество, шт.	8	30	1111**

Ключевые отличия «нового» Положения о системе сертификации средств защиты информации (1/6)

Положение (приказ №199)

Положение (приказ №55)

Заявитель на сертификацию, схемы сертификации

Разработчики,
изготовители,
поставщики и
потребители СЗИ

для **единичных** образцов средств защиты информации - **проведение испытаний образца** на соответствие требованиям по безопасности информации

для **партии** средств защиты информации - **проведение испытаний репрезентативной выборки** образцов средств на соответствие требованиям по безопасности информации

для **серийного производства** средств защиты информации - **проведение типовых испытаний** образцов продукции и **предварительная проверка (аттестация)** производства

Организация,
планирующая
применение СЗИ

для единичных образцов СЗИ - **проведение испытаний образца СЗИ** и **проверка организации** его технической поддержки

для партии СЗИ - **проведение испытаний выборки образцов СЗИ** и **проверка организации** их технической поддержки

Изготовители
(разработчик и/или
производитель СЗИ)

для **серийного производства СЗИ** - **проведение испытаний выборки образцов СЗИ** и **проверка организации производства** и **технической поддержки СЗИ**

Техническая поддержка СЗИ - устранение недостатков и дефектов СЗИ, в том числе устранение уязвимостей и недеklarированных возможностей программного обеспечения СЗИ, информирование потребителей об обновлении программного обеспечения СЗИ, доведение до потребителей обновлений программного обеспечения СЗИ, а также изменений в эксплуатационную документацию

Ключевые отличия «нового» Положения о системе сертификации средств защиты информации (2/6)

Положение
(приказ №199)

Положение (приказ №55)

Требования к заявителю и изготовителю СЗИ

Пункт 2.6
Положения гласит:

«Разработчики, изготовители и поставщики средств защиты информации должны иметь соответствующую лицензию Гостехкомиссии России»

Федеральная служба по техническому и экспортному контролю	
ЗАЯВКА (сертификацию средства защиты информации, продление срока действия сертификата соответствия)	
Наименование средства защиты информации:	_____
Назначение средства защиты информации:	_____
Заявитель:	_____
Адрес местонахождения заявителя:	_____
Почтовый адрес заявителя:	_____
Лицензии ФСТЭК России, имеющиеся у заявителя:	_____
Ф.И.О. руководителя заявителя:	_____
Ф.И.О. лица, ответственного за сертификацию средства защиты информации:	_____
Контактный телефон (телефоны) заявителя:	_____
Адрес электронной почты заявителя:	_____
Разработчик (разработчики) средства защиты информации:	_____

(при наличии разработчика средства защиты информации):	_____
Лицензии ФСТЭК России, имеющиеся у разработчика (разработчиков) средства защиты информации:	_____
Правообладатель (правообладатели) средства защиты информации (при наличии правообладателя (правообладателей) средства защиты информации):	_____
Испытательная лаборатория:	_____
Тип средства защиты информации:	_____
Требования по безопасности информации:	_____
Схема сертификации средства защиты информации:	_____
Заявляемый срок действия сертификата соответствия	_____
Место проведения сертификационных испытаний:	_____
Приложение	1. Документы, прилагаемые к заявке 2. Опись прилагаемых к заявке документов

Изготовители - разработчики и (или) производители средств защиты информации

Изготовители средств защиты информации, составляющей государственную тайну, должны иметь лицензию ФСТЭК России на проведение работ, связанных с созданием средств защиты информации, составляющей государственную тайну

Изготовители средств защиты информации ограниченного доступа, не составляющей государственную тайну, должны иметь лицензию ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации

Пункт 25 Положения: «Основанием для **ОТКАЗА** в проведении сертификации средств защиты информации являются: ...отсутствие у заявителя и (или) изготовителя лицензии ФСТЭК России в случае, если наличие такой лицензии предусмотрено Законодательством Российской Федерации

Ключевые отличия «нового» Положения о системе сертификации средств защиты информации (3/6)

Положение (приказ №199)

Положение (приказ №55)

Объект оценки, требования по безопасности информации, место проведения сертификационных испытаний

Объект оценки

технические, программные и другие средства защиты информации, предназначенные для защиты информации, содержащей сведения, составляющие государственную тайну, от утечки, несанкционированных и непреднамеренных воздействий, несанкционированного доступа и от технической разведки, а также средства контроля эффективности защиты информации (перечень приведен в Приложении)

Требования по безопасности информации

подтверждение характеристик средств защиты информации требованиям **государственных стандартов или иных нормативных документов по защите информации**, утвержденных Государственной технической комиссией при Президенте Российской Федерации (Гостехкомиссией России)

Место проведения сертификационных испытаний

Сертификационные испытания проводятся аккредитованными испытательными центрами (лабораториями) на **их материально-технической базе**. В отдельных случаях по согласованию с федеральным органом по сертификации (или органом по сертификации) допускается проведение испытаний на испытательной базе заявителя данного средства защиты информации

Объект оценки

средства противодействия иностранным техническим разведкам, а также средства контроля эффективности противодействия иностранным техническим разведкам;
средства технической защиты информации, включая средства, в которых они реализованы, а также средства контроля эффективности ТЗИ;
средства обеспечения безопасности информационных технологий, включая защищенные средства обработки информации

Требования по безопасности информации

на соответствие требованиям по безопасности информации, установленным:

- нормативными правовыми актами ФСТЭК России;
- техническими условиями, техническим заданием, заданием по безопасности, согласованными с ФСТЭК России

Место проведения сертификационных испытаний

Сертификационные испытания СЗИ проводятся на материально-технической базе испытательной лаборатории, а также на материально-технических базах заявителя и (или) изготовителя, **расположенных на территории Российской Федерации**

Ключевые отличия «нового» Положения о системе сертификации средств защиты информации (4/6)

Положение (приказ №199)

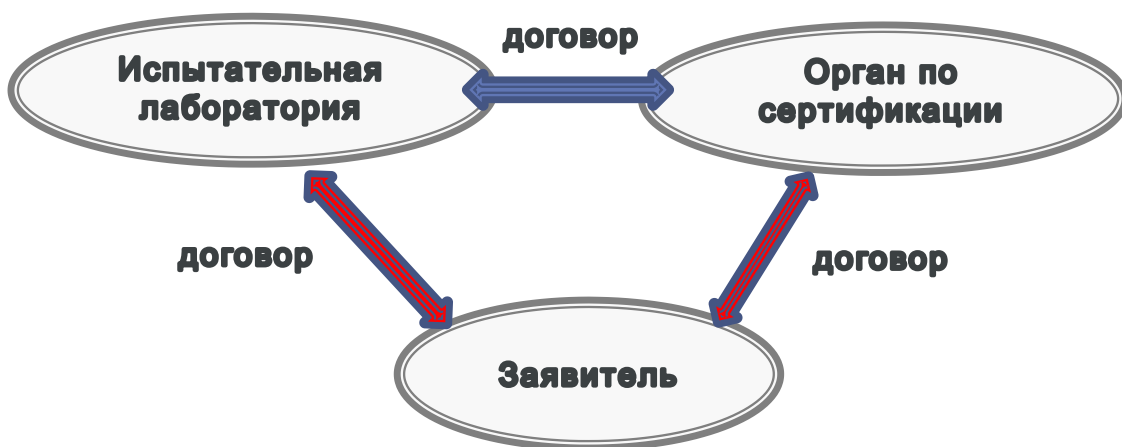
Положение (приказ №55)

Срок действия сертификата соответствия



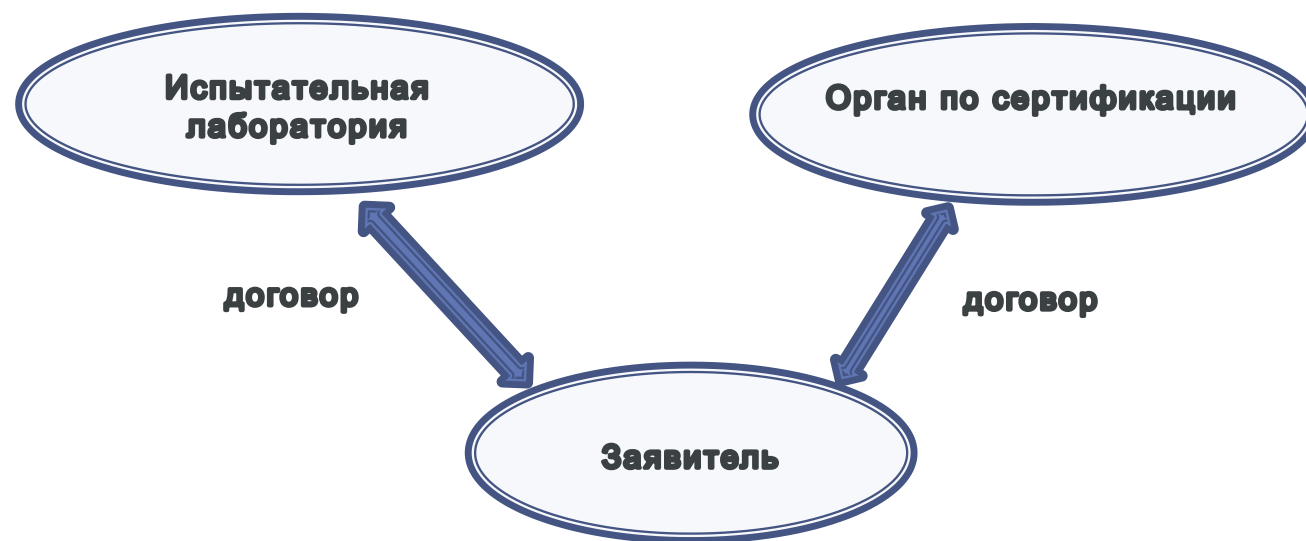
Положение (приказ №199)

Правила организации работ по сертификации



Оплата работ по сертификации средств защиты информации производится заявителем на основании договоров между участниками сертификации

Положение (приказ №55)



*Сертификация средств защиты информации осуществляется **на основании договоров, заключаемых заявителем с испытательной лабораторией и органом по сертификации***

Положение (приказ №199)

Положение (приказ №55)

Внесение изменений в сертифицированное СЗИ

ФСТЭК



И
Н
С
П
Е
К
Ц
И
О
Н
Н
Ы
Й

К
О
Н
Т
Р
О
Л
Ь

Заявитель

Испытательная
лаборатория



Заявитель –
разработчик СЗИ

привлекает **испытательную лабораторию** для проведения испытаний в случае добавления новых функций безопасности или изменения имеющихся функций безопасности

Заявитель, не
являющийся
разработчиком СЗИ

привлекает **испытательную лабораторию** для проведения испытаний в случае добавления новых функций безопасности или изменения имеющихся функций безопасности, а также в случае устранения выявленных уязвимостей и НДВ

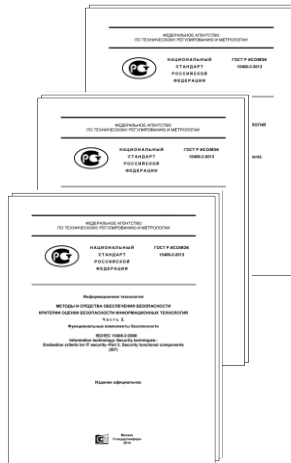
в случае внесения в СЗИ иных изменений заявитель может **самостоятельно** провести испытания

~~ИНСПЕКЦИОННЫЙ КОНТРОЛЬ~~

Дополнительные требования к изготовителю при сертификации согласно «новому» Положению

Проверка организации технической поддержки средства защиты информации, предусматривающую оценку соответствия работ (услуг) по технической поддержке средства защиты информации в ходе его эксплуатации, проводимых (предоставляемых) заявителем, требованиям по безопасности информации

При проверке организации производства программных и программно-технических средств защиты информации проверяется внедрение заявителем **процедур безопасной разработки программного обеспечения**



ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»

ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования

Критическая информационная инфраструктура Российской Федерации



**Федеральный закон
№187-ФЗ от 26 июля 2017 года
«О безопасности критической информационной инфраструктуры
Российской Федерации»
вступил в силу
с 1 января 2018 года**

Закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

□ Объекты КИИ

Информационные системы

Информационно-телекоммуникационные сети

Автоматизированные системы управления

□ Субъекты КИИ

Владелец объекта КИИ

(государственные и частные структуры в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности)

Оператор связи

(лица и организации, обеспечивающие взаимодействие объектов КИИ между собой)

Субъекты КИИ обязаны осуществлять мероприятия по обеспечению безопасности объектов КИИ

Основные мероприятия по обеспечению безопасности объектов ключевой информационной инфраструктуры:

Категорирование объектов КИИ

Интеграция с ГосСОПКА

Создание системы обеспечения безопасности объектов КИИ

Цели создания системы обеспечения безопасности объектов КИИ:

- предотвращение неправомерного доступа к информации;
- недопущение воздействия на технические средства обработки информации;
- восстановление функционирования значимого объекта КИИ.

Приняты нормативно-правовые акты:

[illegible]

Информация об объектах КИИ (реестр) предположительно будет отнесена к государственной тайне

**Статья 14. Ответственность за нарушение требований
настоящего Федерального закона и принятых в
соответствии с ним иных нормативных правовых
актов**

Нарушение требований настоящего Федерального закона и принятых
в соответствии с ним иных нормативных правовых актов влечет за собой
ответственность в соответствии с законодательством Российской
Федерации.

**Субъекты КИИ несут уголовную
ответственность за нарушение
требований по защите информации**

статья 274.1 УК РФ

Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой информации, содержащейся в объектах КИИ, либо правил доступа к объекту КИИ и содержащейся в нем информации

повлекло причинение вреда КИИ:

- принудительные работы на срок до 5 лет или лишение свободы - до 6 лет
- лишение права занимать определенные должности или заниматься определенной деятельностью до 3 лет

повлекло тяжкие последствия:

- лишение свободы на срок от 5 до 10 лет
- лишение права занимать определенные должности или заниматься определенной деятельностью до 5 лет

Сертификация программного обеспечения АСУТП для применения на объектах критической информационной инфраструктуры

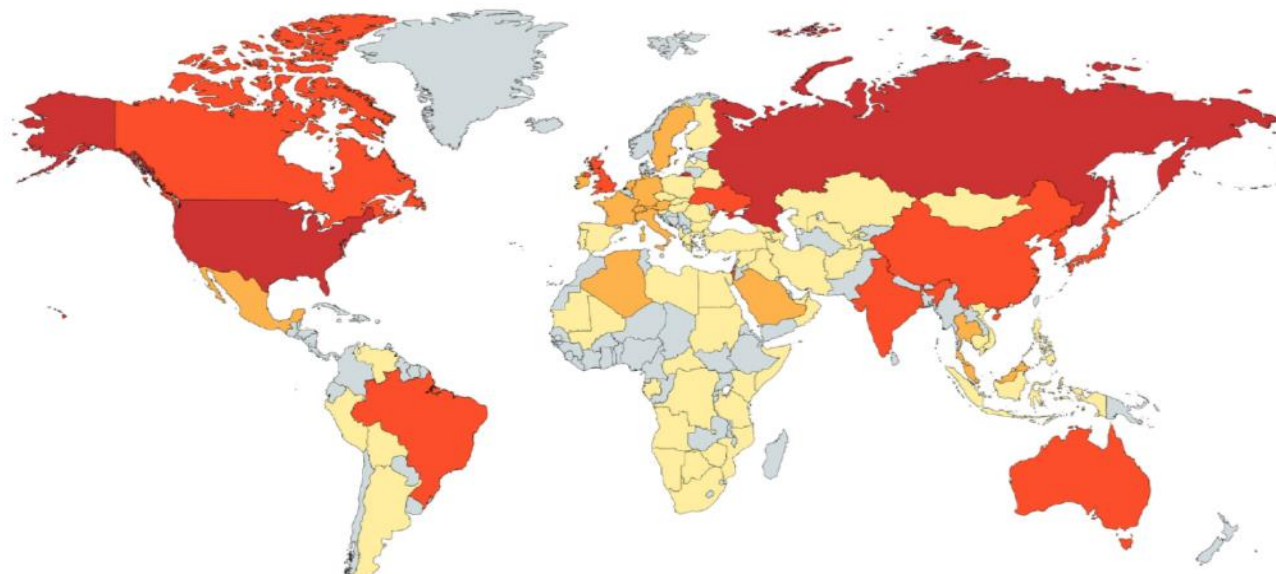
Решения по информационной безопасности невозможно «накрутить» на типовые ИТ-решения



Часто системы автоматизации процессов разрабатывают специалисты в проектировании систем управления технологическими процессами, вычислительной технике, сетевых технологиях и т.д. Они действуют, исходя из «Лучших практик», исследуют ПО, нанимают консалтинг, организывают обучение, оставляя вопросы ИБ на «потом».

Привлеченный проектировщик средств защиты информации не может построить АС в защищенном исполнении, не зная особенностей **технологии обработки информации предприятия**.

В результате, когда деньги потрачены и система готова, оказывается, что ее невозможно запустить по требованиям ИБ, а программное обеспечение систем содержит недостатки, которые могут привести к возникновению уязвимостей, а продукт в целом не содержит необходимых и достаточных встроенных функций безопасности.



Кибератаки 2017 года

Вирус WannaCry - 45 000 атак, 74 страны

Вирус-вымогатель ExPetr – более 80 компаний, 13 тысяч компьютеров на базе MS Windows, 1,5 тысячи юридических и физических лиц

Кибер атака на Bithumb – украдены персональные данные 32 000 пользователей

Уход в облака Windows 10 Cloud Shell – полное отсутствие контроля над хранимыми данными

Потери российских компаний составили
116 млрд. руб.*

Кибер-угрозы 2018 года**

Технологические сети промышленных предприятий

Сетевая инфраструктура

Разработчики легитимного ПО

Интернет вещей

Автомобили и медицинские приборы

С 25 мая 2018 GOOGLE официально ввел политику тотального слежения за пользователями, в т.ч. через конечные устройства пользователей

В июне 2018 года киберкомандование ВС США наделено правом проводить хакерские атаки с целью предотвращения готовящихся кибернападений.



* По данным РБК

** По данным Лаборатории Касперского



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

утверждены приказом
ФСТЭК России от 30 июля 2018 г. № 131

приказ зарегистрирован Минюстом России 14 ноября 2018 г. № 52686, вступил в силу с 14 ноября 2018 г., применяется при проведении сертификационных испытаний с 1 мая 2019 г.



Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении

утверждена ФСТЭК России
11 февраля 2019 г.

методика применяется при проведении
сертификационных испытаний с 1 мая 2019 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

УТВЕРЖДЕНЫ
приказом ФСТЭК России
от 19 августа 2016 г. № 119

**ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
К ОПЕРАЦИОННЫМ СИСТЕМАМ**

МОСКВА
2016

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ



НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК

ГОСТ Р ИСО/МЭК 15408-2-2013.
Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности.
Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности

Издание официальное

Москва
Стандартинформ

ЗАДАНИЕ ПО БЕЗОПАСНОСТИ* на конкретный программный продукт ГОСТ Р ИСО/МЭК 15408-1-2008

*в задании по безопасности должны быть изложены функциональные требования безопасности, относящиеся к конкретной реализации программного изделия, с учётом особенностей функционирования, среды эксплуатации, общей политики безопасности

** допускается изложение функциональных требований безопасности не только в ЗБ, но и в ТУ и/или Техническом задании



Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

утверждены приказом
ФСТЭК России от 27 декабря 2017 г. № 239

приказ зарегистрирован Минюстом России 26
марта 2018 года, регистрационный N 50524

12.7. В ходе приемочных испытаний значимого объекта и его подсистемы безопасности должен быть проведен комплекс организационных и технических мероприятий (испытаний), в результате которых подтверждается соответствие значимого объекта и его подсистемы безопасности настоящим Требованиям, а также требованиям технического задания на создание значимого объекта и (или) технического задания (частного технического задания) на создание подсистемы безопасности значимого объекта.

В случае если значимый объект является государственной информационной системой, в иных случаях, установленных законодательством Российской Федерации, а также в случае принятия решения субъектом критической информационной инфраструктуры, оценка значимого объекта и его подсистемы безопасности проводится в форме аттестации значимого объекта 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. N 17.](#)

27. Технические меры по обеспечению безопасности в значимом объекте реализуются посредством использования программных и программно-аппаратных средств, применяемых для обеспечения безопасности значимых объектов - средств защиты информации (в том числе встроенных в общесистемное, прикладное программное обеспечение).

При этом в приоритетном порядке подлежат применению средства защиты информации, встроенные в программное обеспечение и (или) программно-аппаратные средства значимых объектов (при их наличии).



Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

**утверждены приказом
ФСТЭК России от 27 декабря 2017 г. № 239**

**приказ зарегистрирован Минюстом России 26
марта 2018 года, регистрационный N 50524**

28. Для обеспечения безопасности значимых объектов критической информационной инфраструктуры должны применяться средства защиты информации, прошедшие оценку на соответствие требованиям по безопасности в формах обязательной сертификации, испытаний или приемки.

Средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации, применяются в случаях, установленных законодательством Российской Федерации, а также в случае принятия решения субъектом критической информационной инфраструктуры.

В иных случаях применяются средства защиты информации, прошедшие оценку соответствия в форме испытаний или приемки, которые проводятся субъектами критической информационной инфраструктуры самостоятельно или с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации лицензии на деятельность в области защиты информации.

Испытания (приемка) средств защиты информации проводятся отдельно или в составе значимого объекта критической информационной инфраструктуры в соответствии с программой и методиками испытаний (приемки), утверждаемыми субъектом критической информационной инфраструктуры.



Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

утверждены приказом
ФСТЭК России от 27 декабря 2017 г. № 239

приказ зарегистрирован Минюстом России 26
марта 2018 года, регистрационный N 50524

29. В случае использования в значимом объекте сертифицированных на соответствие требованиям по безопасности информации средств защиты информации:

а) в значимых объектах 1 категории применяются средства защиты информации не ниже 4 класса защиты, а также средства вычислительной техники не ниже 5 класса;

б) в значимых объектах 2 категории применяются средства защиты информации не ниже 5 класса защиты, а также средства вычислительной техники не ниже 5 класса;

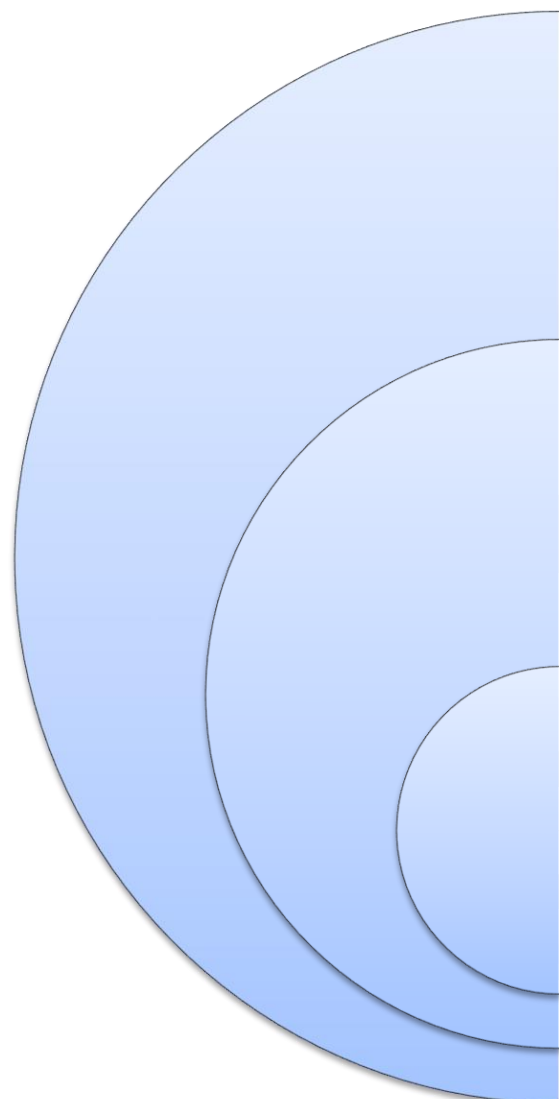
в) в значимых объектах 3 категории применяются средства защиты информации 6 класса защиты, а также средства вычислительной техники не ниже 5 класса.

При этом в значимых объектах 1 и 2 категорий значимости применяются сертифицированные средства защиты информации, прошедшие проверку не ниже чем по 4 уровню контроля отсутствия недеklarированных возможностей. Субъектом критической информационной инфраструктуры может быть принято решение о повышении уровня контроля отсутствия недеklarированных возможностей средств защиты информации.

Классы защиты определяются в соответствии с нормативными правовыми актами ФСТЭК России, изданными в соответствии с [подпунктом 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю](#), утвержденного [Указом Президента Российской Федерации от 16 августа 2004 г. N 1085](#).

При использовании в значимом объекте средств защиты информации, сертифицированных по требованиям безопасности информации, указанные средства должны быть сертифицированы на соответствие обязательным требованиям по безопасности информации, установленным нормативными правовыми актами, или требованиям, указанным в технических условиях (заданиях по безопасности).

Функции безопасности средств защиты информации должны обеспечивать выполнение настоящих Требований.



ОБЪЕКТ ОЦЕНКИ	• неверное определение границ ОО • неверное определение требований к ОО
Степень ГОТОВНОСТИ ОО	• отсутствие корректно реализованных ФБО • несоответствующее с точки зрения ТБИ документирование ОО
Специфика реализации	• не все продукты, возможно, сертифицировать по ТБИ, сформулированным в нормативных правовых актах ФСТЭК России • использование промышленных протоколов, в которых отсутствует возможность реализации ФТБ



ИСПЫТАТЕЛЬНАЯ ЛАБОРАТОРИЯ
ПО СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ