

О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г....

Приказ Федеральной службы по техническому и экспортному контролю · № 27 · от 15.02.2017 · Действует без изменений

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ПРИКАЗ

МОСКВА

15 февраля 2017 г. № 27

О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17

Зарегистрирован Минюстом России 14 марта 2017 г.

Регистрационный № 45933

Внести в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608), изменения согласно приложению к настоящему приказу.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ В.СЕЛИН

УТВЕРЖДЕНЫ
приказом ФСТЭК России
от 15 февраля 2017 г. № 27

Изменения, которые вносятся
в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17

1. В Требованиях о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный

№ 28608):

1) в абзаце втором пункта 3 слова ", Высшего Арбитражного Суда Российской Федерации" исключить;

2) в абзаце первом пункта 12 слова "и в ходе эксплуатации" заменить словами ", в ходе эксплуатации и вывода из эксплуатации";

3) в абзаце втором пункта 14.2 слово "четыре" заменить словом "три", слово "четвертый" заменить словом "третий";

4) в пункте 14.3:

в абзаце первом слова ", оснащенности и мотивации" исключить;
дополнить абзацем вторым следующего содержания:

"В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации (bdu.fstec.ru), 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; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818; 2013, № 26, ст. 3314; № 53, ст. 7137; 2014, № 36, ст. 4833; № 44, ст. 6041; 2015, № 4, ст. 641; 2016, № 1, ст. 211) (далее - банк данных угроз безопасности информации ФСТЭК России), а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации.";

5) в пункте 14.4:

после абзаца седьмого дополнить абзацами следующего содержания:

"стадии (этапы работ) создания системы защиты информационной системы;

требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации;

функции заказчика и оператора по обеспечению защиты информации в информационной системе;

требования к защите средств и систем, обеспечивающих функционирование информационной системы (обеспечивающей инфраструктуру);";

слова "в случае их разработки по ГОСТ Р ИСО/МЭК 27001

"Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования" исключить;

6) в абзаце восьмом пункта 15.1 слова "параметры настройки" заменить словами "требования к параметрам настройки";

7) абзац пятый пункта 15.3 исключить;

8) пункт 16.6 дополнить абзацем следующего содержания:

"По результатам анализа уязвимостей должно быть подтверждено, что в информационной системе отсутствуют уязвимости, содержащиеся в банке данных угроз безопасности информации ФСТЭК России, а также в иных источниках, или их использование (эксплуатация) нарушителем невозможно";

9) пункт 17 дополнить абзацем следующего содержания:

"Проведение аттестационных испытаний информационной системы должностными лицами, осуществляющими проектирование и (или) внедрение системы защиты информации информационной системы, не допускается";

10) пункт 17.2 дополнить абзацами следующего содержания:

"При проведении аттестационных испытаний должны применяться следующие методы проверок (испытаний):

экспертно-документальный метод, предусматривающий проверку соответствия системы защиты информации информационной системы установленным требованиям по защите информации, на основе оценки эксплуатационной документации, организационно-распорядительных документов по защите информации, а также условий функционирования информационной системы;

анализ уязвимостей информационной системы, в том числе вызванных неправильной настройкой (конфигурированием) программного обеспечения и средств защиты информации;

испытания системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к информационной системе в обход ее системы защиты информации.";

11) в пункте 17.4 слова "в случае окончания срока действия аттестата соответствия" заменить словами "по окончании срока действия аттестата соответствия, который не может превышать 5 лет,";

12) дополнить пунктом 17.6 следующего содержания:

"17.6. Информационные системы, функционирующие на базе общей инфраструктуры (средств вычислительной техники, серверов телекоммуникационного оборудования) в качестве прикладных сервисов, подлежат аттестации в составе указанной инфраструктуры.

В случае, если информационная система создается на базе центра обработки данных уполномоченного лица, такой центр обработки данных должен быть аттестован по классу защищенности не ниже класса защищенности, установленного для создаваемой информационной системы.

При аттестации информационной системы должны использоваться результаты аттестации общей инфраструктуры оператора информационной системы.";

13) пункт 25 изложить в следующей редакции:

"25. Организационные меры и средства защиты информации, применяемые в информационной системе, должны обеспечивать: в информационных системах 1 класса защищенности - защиту от угроз безопасности информации, связанных с действиями нарушителей с высоким потенциалом;

в информационных системах 2 класса защищенности - защиту от угроз безопасности информации, связанных с действиями нарушителей с потенциалом не ниже усиленного базового;

в информационных системах 3 класса защищенности - защиту от угроз безопасности информации, связанных с действиями нарушителей с

потенциалом не ниже базового.

Потенциал нарушителей определяется в ходе оценки их возможностей, проводимой при определении угроз безопасности информации в соответствии с пунктом 14.3 настоящих Требований.

Оператором может быть принято решение о применении в информационной системе соответствующего класса защищенности мер защиты информации, обеспечивающих защиту от угроз безопасности информации, реализуемых нарушителями с более высоким потенциалом.";

14) пункт 26 изложить в следующей редакции:

"26. Технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности. При этом: в информационных системах 1 класса защищенности применяются средства защиты информации не ниже 4 класса, а также средства вычислительной техники не ниже 5 класса; в информационных системах 2 класса защищенности применяются средства защиты информации не ниже 5 класса, а также средства вычислительной техники не ниже 5 класса; в информационных системах 3 класса защищенности применяются средства защиты информации 6 класса, а также средства вычислительной техники не ниже 5 класса.

В информационных системах 1 и 2 классов защищенности применяются средства защиты информации, прошедшие проверку не ниже чем по 4 уровню контроля отсутствия недеklarированных возможностей.

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. № 1085.

В информационных системах применяются средства защиты информации, сертифицированные на соответствие обязательным требованиям по безопасности информации, установленным ФСТЭК России, или на соответствие требованиям, указанным в технических условиях (заданиях по безопасности). При этом функции безопасности таких средств должны обеспечивать выполнение настоящих Требований.";

15) абзац пятый пункта 27 исключить.

2. В приложении № 1 к указанным Требованиям:

1) в абзаце первом пункта 1 слова ", четвертый класс (K4)" исключить;

2) абзац седьмой пункта 2 исключить;

3) в пункте 4 таблицу изложить в следующей редакции:

"

-----	-----
Уровень	Масштаб информационной системы
значимости	-----
информации	Федеральный Региональный Объектовый
-----	-----

УЗ 1	K1	K1	K1
УЗ 2	K1	K2	K2
УЗ 3	K2	K3	K3

3. Приложение № 2 к указанным Требованиям изложить в новой редакции:

"Приложение № 2 к
Требованиям о защите информации, не
составляющей государственную тайну,
содержащейся в государственных
информационных системах

Состав мер защиты информации и их базовые наборы для соответствующего класса
защищенности информационной системы

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Классы защищенности информационной системы
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)		
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+++
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	+++
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+++
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+++
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+++
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+++
ИАФ.7	Идентификация и аутентификация объектов файловой системы,	+++

| |запускаемых и исполняемых модулей, объектов систем управления| | |
| |базами данных, объектов, создаваемых прикладным и специальным| | |
	программным обеспечением, иных объектов доступа		
II. Управление доступом субъектов доступа к объектам доступа (УПД)			
-----	-----	-----	-----
УПД.1	Управление (заведение, активация, блокирование и уничтожение)	+	+
	учетными записями пользователей, в том числе внешних		
	пользователей		
---	---	---	---
УПД.2	Реализация необходимых методов (дискреционный, мандатный,	+	+
	ролевой или иной метод), типов (чтение, запись, выполнение или		
	иной тип) и правил разграничения доступа		
-----	-----	-----	-----
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений,	+	+
	однонаправленная передача и иные способы управления)		
	информационными потоками между устройствами, сегментами		
	информационной системы, а также между информационными		
	системами		
-----	-----	-----	-----
УПД.4	Разделение полномочий (ролей) пользователей, администраторов	+	+
	и лиц, обеспечивающих функционирование информационной системы		
-----	-----	-----	-----
УПД.5	Назначение минимально необходимых прав и привилегий	+	+
	пользователям, администраторам и лицам, обеспечивающим		
	функционирование информационной системы		
-----	-----	-----	-----
УПД.6	Ограничение неуспешных попыток входа в информационную систему	+	+
	(доступа к информационной системе)		
-----	-----	-----	-----
УПД.7	Предупреждение пользователя при его входе в информационную		
	систему о том, что в информационной системе реализованы меры		
	защиты информации, и о необходимости соблюдения им		
	установленных оператором правил обработки информации		
-----	-----	-----	-----
УПД.8	Оповещение пользователя после успешного входа в		
	информационную систему о его предыдущем входе в информационную		
	систему		
-----	-----	-----	-----
УПД.9	Ограничение числа параллельных сеансов доступа для каждой		+
	учетной записи пользователя информационной системы		
-----	-----	-----	-----
УПД.10	Блокирование сеанса доступа в информационную систему после	+	+
	установленного времени бездействия (неактивности) пользователя		
	или по его запросу		
-----	-----	-----	-----
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до	+	+
	идентификации и аутентификации		

УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки	+	+	+	+
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+	+
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+	+
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники	+	+	+	+
III. Ограничение программной среды (ОПС)					
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения	+	+	+	+
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения	+	+	+	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	+	+	+	+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов	+	+	+	+
IV. Защита машинных носителей информации (ЗНИ)					
ЗНИ.1	Учет машинных носителей информации	+	+	+	+
ЗНИ.2	Управление доступом к машинным носителям информации	+	+	+	+
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны	+	+	+	+

ЗНИ.4	Исключение возможности несанкционированного ознакомления с			
	содержанием информации, хранящейся на машинных носителях, и			
	(или) использования носителей информации в иных информационных			
 | |системах ||||
 |-----|-----|----|----|
 | ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации || + | + |
 | |на машинные носители информации ||||
 |-----|-----|----|----|
 | ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители ||||
 | |информации ||||
 |-----|-----|----|----|
 | ЗНИ.7 | Контроль подключения машинных носителей информации ||||
 |-----|-----|----|----|
 | ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях при | + | + | + |
 | |их передаче между пользователями, в сторонние организации для ||||
 | |ремонта или утилизации, а также контроль уничтожения ||||
 | |(стирания) ||||
 |-----|-----|----|----|
 | V. Регистрация событий безопасности (РСБ) |
 |-----|-----|----|----|
 | РСБ.1 | Определение событий безопасности, подлежащих регистрации, и | + | + | + |
 | |сроков их хранения ||||
 |-----|-----|----|----|
 | РСБ.2 | Определение состава и содержания информации о событиях | + | + | + |
 | |безопасности, подлежащих регистрации ||||
 |-----|-----|----|----|
 | РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в | + | + | + |
 | |течение установленного времени хранения ||||
 |-----|-----|----|----|
 | РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в | + | + | + |
 | |том числе аппаратные и программные ошибки, сбои в механизмах ||||
 | |сбора информации и достижение предела или переполнения объема ||||
 | |(емкости) памяти ||||
 |-----|-----|----|----|
 | РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий| + | + | + |
 | |безопасности и реагирование на них ||||
 |-----|-----|----|----|
 | РСБ.6 | Генерирование временных меток и (или) синхронизация | + | + | + |
 | |системного времени в информационной системе ||||
 |-----|-----|----|----|
 | РСБ.7 | Защита информации о событиях безопасности | + | + | + |
 |-----|-----|----|----|
 | РСБ.8 | Обеспечение возможности просмотра и анализа информации о ||||
 | |действиях отдельных пользователей в информационной системе ||||
 |-----|-----|----|----|
 | VI. Антивирусная защита (АВЗ) |
 |-----|-----|----|----|
 | АВЗ.1 | Реализация антивирусной защиты | + | + | + |

AB3.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+
VII. Обнаружение вторжений (COB)					
COB.1	Обнаружение вторжений	+	+	+	
COB.2	Обновление базы решающих правил	+	+	+	
VIII. Контроль (анализ) защищенности информации (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	+	+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения средств защиты информации	+	+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	+	+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе	+	+	+	+
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)					
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	+	+	+	
ОЦЛ.2	Контроль целостности информации, содержащейся в базах данных информационной системы	+	+	+	
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций	+	+	+	+
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)	+	+	+	

ОЦЛ.5	Контроль содержания информации, передаваемой из			
информационной системы (контейнерный, основанный на свойствах				
объекта доступа, и контентный, основанный на поиске				
запрещенной к передаче информации с использованием сигнатур,				
масок и иных методов), и исключение неправомерной передачи				
информации из информационной системы					
ОЦЛ.6	Ограничение прав пользователей по вводу информации в			+	
информационную систему					
-----	-----	-----	----	----	----
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в				
информационную систему					
-----	-----	-----	----	----	----
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или)				
передаче информации и предупреждение пользователей об					
ошибочных действиях					
-----	-----	-----	----	----	----
X. Обеспечение доступности информации (ОДТ)					
-----	-----	-----	----	----	----
ОДТ.1	Использование отказоустойчивых технических средств			+	
---	---	---	---	---	---
ОДТ.2	Резервирование технических средств, программного обеспечения,			+	
каналов передачи информации, средств обеспечения					
функционирования информационной системы					
-----	-----	-----	----	----	----
ОДТ.3	Контроль безотказного функционирования технических средств,			+ +	
обнаружение и локализация отказов функционирования, принятие					
мер по восстановлению отказавших средств и их тестирование					
-----	-----	-----	----	----	----
ОДТ.4	Периодическое резервное копирование информации на резервные			+ +	
машинные носители информации					
-----	-----	-----	----	----	----
ОДТ.5	Обеспечение возможности восстановления информации с резервных			+ +	
машинных носителей информации (резервных копий) в течение					
установленного временного интервала					
-----	-----	-----	----	----	----
ОДТ.6	Кластеризация информационной системы и (или) ее сегментов				
-----	-----	-----	----	----	----
ОДТ.7	Контроль состояния и качества предоставления уполномоченным			+ +	
лицом вычислительных ресурсов (мощностей), в том числе по					
передаче информации					
-----	-----	-----	----	----	----
XI. Защита среды виртуализации (ЗСВ)					
-----	-----	-----	----	----	----
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов			+ + +	
доступа в виртуальной инфраструктуре, в том числе					
администраторов управления средствами виртуализации					
-----	-----	-----	----	----	----

| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в | + | + | + |
 | виртуальной инфраструктуре, в том числе внутри виртуальных | | |
машин				
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	+	+	+
-----	-----	-----	-----	
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения,	+	+	+
односторонняя передача) потоками информации между				
компонентами виртуальной инфраструктуры, а также по периметру				
виртуальной инфраструктуры				
-----	-----	-----	-----	
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной			
машины (контейнера), серверов управления виртуализацией				
-----	-----	-----	-----	
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и	+	+	+
обрабатываемых на них данных				
-----	-----	-----	-----	
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее	+	+	+
конфигураций				
-----	-----	-----	-----	
ЗСВ.8	Резервное копирование данных, резервирование технических	+	+	+
средств, программного обеспечения виртуальной инфраструктуры,				
а также каналов связи внутри виртуальной инфраструктуры				
-----	-----	-----	-----	
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной	+	+	+
инфраструктуре				
-----	-----	-----	-----	
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты	+	+	+
(сегментирование виртуальной инфраструктуры) для обработки				
информации отдельным пользователем и (или) группой				
пользователей				
-----	-----	-----	-----	
XII. Защита технических средств (ЗТС)				
-----	-----	-----	-----	
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от			
ее утечки по техническим каналам				
---	---	---	---	---
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно	+	+	+
размещаются стационарные технические средства, обрабатывающие				
информацию, и средства защиты информации, а также средства				
обеспечения функционирования				
-----	-----	-----	-----	
ЗТС.3	Контроль и управление физическим доступом к техническим	+	+	+
средствам, средствам защиты информации, средствам обеспечения				
функционирования, а также в помещения и сооружения, в которых				
они установлены, исключая несанкционированный физический				
доступ к средствам обработки информации, средствам защиты				
информации и средствам обеспечения функционирования				

| информационной системы и помещения и сооружения, в которых они | | |
установлены				
ЗТС.4	Размещение устройств вывода (отображения) информации,	+	+	+
исключающее ее несанкционированный просмотр				
-----	-----	-----	-----	
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды,		+	
нестабильности электроснабжения, кондиционирования и иных				
внешних факторов)				
-----	-----	-----	-----	
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)				
-----	-----	-----	-----	
ЗИС.1	Разделение в информационной системе функций по управлению	+	+	
	(администрированию) информационной системой, управлению			
	(администрированию) системой защиты информации, функций по			
	обработке информации и иных функций информационной системы			
---	---	---	---	---
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с			
	высоким приоритетом со стороны процессов с низким приоритетом			
-----	-----	-----	-----	
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и	+	+	+
	навязывания (ввода ложной информации) при ее передаче			
	(подготовке к передаче) по каналам связи, имеющим выход за			
	пределы контролируемой зоны, в том числе беспроводным каналам			
	связи			
-----	-----	-----	-----	
ЗИС.4	Обеспечение доверенных канала, маршрута между			
	администратором, пользователем и средствами защиты информации			
	(функциями безопасности средств защиты информации)			
-----	-----	-----	-----	
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер,	+	+	+
	микрофонов и иных периферийных устройств, которые могут			
	активироваться удаленно, и оповещение пользователей об			
	активации таких устройств			
-----	-----	-----	-----	
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток			
	безопасности), связанных с информацией, при обмене информацией			
	с иными информационными системами			
-----	-----	-----	-----	
ЗИС.7	Контроль санкционированного и исключение несанкционированного	+	+	
	использования технологий мобильного кода, в том числе			
	регистрация событий, связанных с использованием технологий			
	мобильного кода, их анализ и реагирование на нарушения,			
	связанные с использованием технологий мобильного кода			
-----	-----	-----	-----	
ЗИС.8	Контроль санкционированного и исключение несанкционированного	+	+	
	использования технологий передачи речи, в том числе			
	регистрация событий, связанных с использованием технологий			

| |передачи речи, их анализ и реагирование на нарушения,| | |
	связанные с использованием технологий передачи речи			
ЗИС.9	Контроль санкционированной и исключение несанкционированной	+	+	
	передачи видеoinформации, в том числе регистрация событий,			
	связанных с передачей видеoinформации, их анализ и			
	реагирование на нарушения, связанные с передачей			
	видеoinформации			
-----	-----	-----	-----	
ЗИС.10	Подтверждение происхождения источника информации, получаемой			
	в процессе определения сетевых адресов по сетевым именам или			
	определения сетевых имен по сетевым адресам			
-----	-----	-----	-----	
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов	+	+	
	взаимодействия), в том числе для защиты от подмены сетевых			
	устройств и сервисов			
-----	-----	-----	-----	
ЗИС.12	Исключение возможности отрицания пользователем факта отправки	+	+	
	информации другому пользователю			
-----	-----	-----	-----	
ЗИС.13	Исключение возможности отрицания пользователем факта	+	+	
	получения информации от другого пользователя			
-----	-----	-----	-----	
ЗИС.14	Использование устройств терминального доступа для обработки			
	информации			
-----	-----	-----	-----	
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты	+	+	
	информации и программного обеспечения и иных данных, не			
	подлежащих изменению в процессе обработки информации			
-----	-----	-----	-----	
ЗИС.16	Выявление, анализ и блокирование в информационной системе			
	скрытых каналов передачи информации в обход реализованных мер			
	защиты информации или внутри разрешенных сетевых протоколов			
-----	-----	-----	-----	
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование	+	+	
	информационной системы) и обеспечение защиты периметров			
	сегментов информационной системы			
-----	-----	-----	-----	
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с			
	машинных носителей информации, доступных только для чтения, и			
	контроль целостности данного программного обеспечения			
-----	-----	-----	-----	
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области			
	памяти			
-----	-----	-----	-----	
ЗИС.20	Защита беспроводных соединений, применяемых в информационной	+	+	+
	системе			
-----	-----	-----	-----	

ЗИС.21	Исключение доступа пользователя к информации, возникшей в		+
	результате действий предыдущего пользователя через реестры,		
	оперативную память, внешние запоминающие устройства и иные		
	общие для пользователей ресурсы информационной системы			
ЗИС.22	Защита информационной системы от угроз безопасности	+	+	
	информации, направленных на отказ в обслуживании			
	информационной системы			
-----	-----	----	----	----
ЗИС.23	Защита периметра (физических и (или) логических границ)	+	+	
	информационной системы при ее взаимодействии с иными			
	информационными системами и			
	информационно-телекоммуникационными сетями			
-----	-----	----	----	----
ЗИС.24	Прекращение сетевых соединений по их завершении или по	+	+	
	истечении заданного оператором временного интервала			
	неактивности сетевого соединения			
-----	-----	----	----	----
ЗИС.25	Использование в информационной системе или ее сегментах			
	различных типов общесистемного, прикладного и специального			
	программного обеспечения (создание гетерогенной среды)			
-----	-----	----	----	----
ЗИС.26	Использование прикладного и специального программного			
	обеспечения, имеющих возможность функционирования в средах			
	различных операционных систем			
-----	-----	----	----	----
ЗИС.27	Создание (эмуляция) ложных информационных систем или их			
	компонентов, предназначенных для обнаружения, регистрации и			
	анализа действий нарушителей в процессе реализации угроз			
	безопасности информации			
-----	-----	----	----	----
ЗИС.28	Воспроизведение ложных и (или) скрытие истинных отдельных			
	информационных технологий и (или) структурно-функциональных			
	характеристик информационной системы или ее сегментов,			
	обеспечивающее навязывание нарушителю ложного представления об			
	истинных информационных технологиях и (или)			
	структурно-функциональных характеристиках информационной			
	системы			
-----	-----	----	----	----
ЗИС.29	Перевод информационной системы или ее устройств (компонентов)			
	в заранее определенную конфигурацию, обеспечивающую защиту			
	информации, в случае возникновения отказов (сбоев) в системе			
	защиты информации информационной системы			
-----	-----	----	----	----
ЗИС.30	Защита мобильных технических средств, применяемых в	+	+	+
	информационной системе			
-----	-----	----	----	----

"+" - мера защиты информации включена в базовый набор мер для

соответствующего класса защищенности информационной системы. Меры защиты информации, не обозначенные знаком "+", применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер защиты информации в информационной системе соответствующего класса защищенности."
