ЗИС.27 Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации

Требования к реализации ЗИС.27: В информационной системе должны применяться специально созданные (эмулированные) ложные компоненты информационной системы или создаются ложные информационные системы, предназначенные для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации.

Ложные информационные системы или их компоненты должны выступать в качестве целей для нарушителя при реализации им компьютерной атаки и обеспечивать имитацию функционирования реальной информационной системы с целью обнаружения, регистрации и анализа действий этих нарушителей по реализации компьютерной атаки, а также принятия мер по предотвращению указанных угроз.

Правила и процедуры применения ложных информационных систем или их компонентов регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗИС.27:

1) в информационной системе применяются ложные компоненты информационной системы, выступающие в качестве цели для вредоносного программного обеспечения (вируса) и провоцирующие преждевременное (до воздействия на защищаемый объект доступа) проявление его признаков.

Содержание базовой меры ЗИС.27:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.27				
Усиление ЗИС.27				

ЗИС.28 Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание у нарушителя ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы

Требования к реализации ЗИС.28: Оператором должно обеспечиваться воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание у нарушителя ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы.

Воспроизведение (визуализация) ложных и (или) скрытие (маскирование) истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов должны быть направлены на снижение возможности успешной реализации нарушителем угрозы безопасности информации (компьютерной атаки) путем введения в заблуждение нарушителя относительно возможных способов и средств компьютерных атак на информационную систему.

При этом визуализация ложных и (или) маскирование истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы позволяют снизить или исключить затраты на внедрение сложных средств защиты информации.

Требования к усилению ЗИС.28:

1) визуализация ложных информационных технологий и (или) структурно-функциональных характеристик осуществляется в произвольном порядке с периодичностью, определяемой оператором.

Содержание базовой меры ЗИС.28:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.28				
Усиление ЗИС.28				

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

Требования к реализации ЗИС.29: В информационной системе должен осуществляться перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы.

Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию должен обеспечивать защиту информации при наступлении (возникновении) отказов (сбоев) в функционировании информационной системы или ее сегментов, которые могут привести к нарушению конфиденциальности, целостности и (или) доступности этой информации.

Оператором должны быть определены типы отказов (сбоев) в системе защиты информации информационной системы, которые могут привести к нарушению конфиденциальности, целостности и (или) доступности этой информации, и при наступлении (возникновении) которых должен обеспечиваться перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию.

Заранее определенная конфигурация информационной системы должна содержать информацию о состоянии информационной системы и ее системе защиты информации (системная информация, параметры настроек программного обеспечения, включая средств защиты информации), достаточной для перезапуска информационной системы и обеспечения ее функционирования в штатном режиме, при котором также обеспечивается защита информации.

Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы осуществляется в соответствии с ОДТ.2, резервное копирование информации - в соответствии с ОДТ.4.

Контроль безотказного функционирования технических средств информационной системы осуществляется в соответствии с ОДТ.3.

Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала осуществляется в соответствии с ОДТ.5.

Требования к усилению ЗИС.29:

Не установлены.

Содержание базовой меры ЗИС.29:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.29				
Усиление ЗИС.29				

ЗИС.30 Защита мобильных технических средств, применяемых в информационной системе

Требования к реализации ЗИС.30: Оператором должна осуществляться защита применяемых в информационной системе мобильных технических средств.

К мобильным техническим средствам относятся съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные носители), а также портативные вычислительные устройства и устройства связи с возможностью обработки информации (например, ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные средства).

Защита мобильных технических средств включает:

Реализацию в зависимости от мобильного технического средства (типа мобильного технического средства) мер по идентификации и аутентификации в соответствии с ИАФ.1 и ИАФ.5, управлению доступом в соответствии с УПД.2, УПД.5, УПД.13 и УПД.15, ограничению программной среды в соответствии с ОПС.3, защите машинных носителей информации в соответствии с ЗНИ.1, ЗНИ.2, ЗНИ.4, ЗНИ.8, регистрации событий безопасности в соответствии с РСБ.1, РСБ.2, РСБ.3 и РСБ.5, антивирусной защите в соответствии с АВЗ.1 и АВЗ.2, контролю (анализу) защищенности в соответствии с АНЗ.1, АНЗ.2 и АНЗ.3, обеспечению целостности в соответствии с ОЦЛ.1.

очистку (удаление) информации в мобильном техническом средстве после завершения сеанса удаленного доступа к защищаемой информации или принятие иных мер, исключающих несанкционированный доступ к хранимой защищаемой информации;

уничтожение съемных машинных носителей информации, которые не подлежат очистке;

выборочные проверки мобильных технических средств (на предмет их наличия) и хранящейся на них информации (например, на предмет отсутствия информации, не соответствующей маркировке носителя информации);

запрет возможности автоматического запуска (без команды пользователя) в информационной системе программного обеспечения на мобильных технических средствах.

Правила и процедуры защиты мобильных технических средств регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗИС.30:

1) оператором должны применяться средства ограничения доступа к информации на съемных машинных носителях информации с использованием специализированных съемных машинных носителей информации и средств контроля съемных машинных носителей информации с учетом ЗНИ.4;

2) оператором должна обеспечиваться очистка (удаление) информации в мобильном техническом средстве:

а) при превышении допустимого числа неуспешных попыток входа в информационную систему под конкретной учетной записью (доступа к информационной системе), осуществляемых с мобильного устройства;

б) при превышении допустимого интервала времени с начала осуществления попыток входа в информационную систему под конкретной учетной записью, осуществляемых с мобильного устройства;

3) оператором должно обеспечиваться применение технических средств защиты периметра уровня узла, устанавливаемых на портативные вычислительные устройства;

4) оператором должно обеспечиваться использование радиометок (RFID-меток) для контроля вноса или выноса мобильных технических устройств из помещения и (или) контролируемой зоны в

целом;

5) оператором обеспечивается шифрование хранимой на носителе мобильного технического средства информации с применением криптографических методов защиты информации в соответствии с законодательством Российской Федерации.

Содержание базовой меры ЗИС.30:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.30		+	+	+
Усиление ЗИС.30				

Приложение N 1
к Мерам защиты информации
в государственных информационных системах

Термины и определения, применяемые для целей настоящего методического документа

Администратор [системный, безопасности]**:** пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) информационной системы (администратор системный) и (или) ее системы защиты информации (администратор безопасности) в соответствии с установленной ролью.

Анализ уязвимостей: мероприятия по выявлению, идентификации и оценке уязвимостей информационной системы в интересах определения возможности реализации угроз безопасности информации и способов предотвращения ущерба.

Аутентификационная информация [информация аутентификации]**:** информация, используемая для установления подлинности (верификации) субъекта доступа в информационной системе.

Аутентификация: проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе).

Базовый набор мер защиты информации: минимальный набор мер защиты информации, установленный для соответствующего класса защищенности информационной системы.

Виртуализация: технология преобразование формата или параметров программных или сетевых запросов к компьютерным ресурсам с целью обеспечения независимости процессов обработки информации от программной или аппаратной платформы информационной системы.

Виртуальная машина: вычислительная система, эмулируемая с помощью технологии виртуализации, в которой установлена гостевая операционная система и обеспечивается выполнение прикладного программного обеспечения.

Внешняя информационная система: информационная система, взаимодействующая с информационной системой оператора из-за пределов границ информационной системы оператора.

Внешняя информационно-телекоммуникационная сеть: информационно-телекоммуникационная сеть, взаимодействующая с информационной системой оператора из-за пределов границ информационной системы оператора.

Временный файл: файл, создаваемый операционной системой или иным программным обеспечением для сохранения промежуточных результатов в процессе функционирования или передачи данных другому программному обеспечению.

Гипервизор: программа (программное обеспечение), создающая среду функционирования других программ (в том числе других гипервизоров) за счёт имитации аппаратных средств вычислительной техники, управления данными средствами и гостевыми операционными системами, функционирующими в данной среде.

Гостевая операционная система: операционная система, установленная на виртуальной машине.

Демилитаризованная зона: экранированный сегмент информационной системы, размещенный на ее внешней границе и выполняющий функции "нейтральной зоны" (буферной зоны безопасности) между защищаемой информационной системой оператора и внешней информационной системой или информационно-телекоммуникационной сетью.

Доверенная загрузка: загрузка операционной системы средства вычислительной техники с заранее определенных постоянных машинных носителей при обязательном успешном прохождении процедур проверки целостности программной и аппаратной среды и идентификации и аутентификации.

Доверенный канал: механизм взаимодействия между средствами защиты информационной системы или между средством защиты информации и программным обеспечением информационной системы.

Доверенный маршрут: механизм взаимодействия между субъектом доступа и средством защиты информации информационной системы.

Доступность информации: свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать.

Защищенные линии связи: линии (каналы) связи, при передаче информации по которым обеспечивается требуемый уровень ее защищенности (конфиденциальность, целостность и (или) доступность информации).

Идентификатор: представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной системе.

Идентификация: присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

Информационная система: совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Инцидент: непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

Компонент программного обеспечения: составная часть (программный модуль) программного обеспечения, выполняющая определенную функцию.

Компонент информационной системы: часть информационной системы, включающая некоторую совокупность информации и обеспечивающих ее обработку отдельных информационных технологий и технических средств.

Контролируемая зона: пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств.

Конфиденциальность информации: свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право.

Локальный доступ: доступ субъектов доступа к объектам доступа, осуществляемый непосредственно через подключение (доступ) к компоненту информационной системы или через локальную вычислительную сеть (без использования информационно-телекоммуникационной сети).

Многофакторная аутентификация: аутентификация с использованием двух (двухфакторная) или более различных факторов аутентификации.

Мобильный код: несамостоятельное программное обеспечение или компонент программного обеспечения (скрипты, макросы, иные компоненты) получаемые из мест распространения мобильного кода, передаваемые по сети и выполняемые на компонентах информационной системы (в местах использования мобильного кода) без предварительной установки (инсталляции) пользователем для расширения возможностей системного и (или) прикладного программного обеспечения.

Непривилегированная учетная запись: учетная запись пользователя (процесса, выполняемого от его имени) информационной системы.

Объект доступа: единица информационного ресурса информационной системы (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции.

Оператор информационной системы: гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Отказ в обслуживании: препятствие санкционированному доступу к ресурсам информационной системы или задержка операций и функций информационной системы.

Периметр информационной системы: физическая и (или) логическая граница информационной системы (сегмента информационной системы), в пределах которой оператором обеспечивается защита информации в соответствии с едиными правилами и процедурами, а также контроль за

реализованными мерами защиты информации.

Пользователь: лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования.

Потенциал нарушителя: мера усилий, затрачиваемых нарушителем при реализации угроз безопасности информации в информационной системе.

Привилегированная учетная запись: учетная запись администратора информационной системы.

Программная среда: совокупность программного обеспечения, используемого в информационной системе для решения одной или нескольких задач.

Роль: предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной системой.

Сегмент информационной системы: совокупность нескольких компонентов информационной системы, использующих общую (в том числе разделяемую) среду передачи и объединенных для единства решения функциональных задач.

Событие безопасности (информационной)**:** идентифицированное возникновение состояния информационной системы (сегмента, компонента информационной системы), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации.

Субъект доступа: пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

Техническое средство: аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации в информационной системе.

Технологии мобильного кода: реализованные в программном обеспечении процессы создания и использования мобильного кода (в частности технологии Java, JavaScript, ActiveX, VBScript).

Удаленный доступ: процесс получения доступа (через внешнюю сеть) к объектам доступа информационной системы из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически или логически с информационной системой, к которой он получает доступ.

Управление доступом: ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа.

Устройство: конструктивно законченный технический элемент, имеющий определенное функциональное назначение в информационной системе.

Уязвимость "нулевого дня": уязвимость, которая становится известной до момента выпуска разработчиком программного обеспечения информационной системы мер защиты информации по ее устранению, исправлений ошибок или соответствующих обновлений.

Уязвимость информационной системы: недостаток (слабость) информационной системы, который (которая) создает потенциальные или реально существующие условия для реализации или проявления угроз безопасности информации.

Хостовая операционная система: операционная система, в среде которой функционирует гипервизор.

Целостность информации: свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право.

Приложение N 2
к Мерам защиты информации
в государственных информационных системах

Содержание базовых мер защиты информации для соответствующего класса защищенности информационной системы

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Классы защищенности информационной системы			
		4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+ 1а, 2а, 3	+ 1а, 2а, 3, 4
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+ 1а, 2а	+ 1а, 2а	+ 1б, 2б
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	+ 1а	+ 1б	+ 1в	+ 1г
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	+	+ 1, 2	+ 1, 2, 3а	+ 1, 2, 3б
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+ 1, 2, 3	+ 1, 2, 3	+ 1, 2, 3, 4
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 обязанностей полномочий (ролей), администраторов и лиц, обеспечивающих функционирование информационной системы		+	+	+ 1
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы		+	+	+ 1
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+	+ 1
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				+ 1а, 3
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+ 1а, 2	+ 1б, 2
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	+	+ 2, 3	+ 2, 3, 5	+ 1, 2, 3, 5
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+ 1	+ 1, 3	+ 1, 3, 4, 5
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+ 1, 2	+ 1, 2
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+ 1а	+ 1а, 1б	+ 1а, 1б	+ 1а, 1б
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+ 1	+ 2
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				+ 1, 2, 3
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			+	+ 1
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	+	+	+ 1а	+ 1а, 1б
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			+	+ 1
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)	+ 5а	+ 1,5б	+ 1, 5в	+ 1, 2, 3, 5г
V. Регистрация событий безопасности (РСБ)					
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+ 1,3, 4а	+ 1, 2, 3, 4б
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+ 1а	+ 1а
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+ 1	+ 1
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	+	+	+	+ 1а, 2
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	+	+	+	+ 1
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	+	+	+	+ 1
РСБ.7	Защита информации о событиях безопасности	+	+	+ 1	+ 1
РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе				
VI. Антивирусная защита (АВЗ)					
АВЗ.1	Реализация антивирусной защиты	+	+ 1	+ 1, 2	+ 1, 2
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+ 1	+ 1
VII. Обнаружение вторжений (СОВ)					

СОВ.1	Обнаружение вторжений			+ 2	+ 2
СОВ.2	Обновление базы решающих правил			+	+ 1, 2, 3
VIII. Контроль (анализ) защищенности информации (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+ 1,4	+ 1, 2,4	+ 1, 2,4,7
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 и средств защиты информации		+	+ 1	+ 1
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+ 1	+ 1, 2
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе		+	+ 1	+ 1
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)					
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+ 1, 3	+ 1, 3
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	+	+	+	+ 1
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			+	+ 1
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации			+ 1, 2	+ 1, 3
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала			+	+ 1
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	+	+	+ 1	+ 1
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+ 1, 2	+ 1, 2	+ 1, 2
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между			+	+ 1, 2

	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			+ 1	+ 1, 2
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+ 3	+ 1, 3
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+ 1, 2, 3
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+ 1	+ 1
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей			+	+ 2
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, исключающие 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			+ 3	+ 3
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	+	+	+ 1	+ 1, 2
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			+ 1	+ 1, 2
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 видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации			+	+
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			+	+ 1
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			+ 1, 2, 3, 4а, 4б, 4в, 5	+ 1, 2, 3, 4а, 4б, 4в, 4г, 4д, 5, 6, 7
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 возникновении 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 и должны выполняться требования к реализации данной меры защиты информации, указанные в разделе 3 настоящего документа под рубрикой "требования к реализации".

"цифра" или "цифра" "буква" - должны выполняться требования к усилению данной меры защиты информации, указанные в разделе 3 настоящего документа в подразделе "требования к усилению меры защиты информации". Цифры и буквы, не включенные в таблицу и указанные под рубриками "требования к усилению" 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.

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.