ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

Утвержден ФСТЭК России
11 февраля 2014 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

2014

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах» (далее – методический документ) разработан и утвержден в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

Методический документ детализирует организационные и технические меры защиты информации (далее – меры защиты информации), принимаемые в государственных информационных системах (далее – информационные системы) в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17 (зарегистрирован Минюстом России 31 мая 2013 г., рег. № 28608), а также определяет содержание мер защиты информации и правила их реализации.

В методическом документе не рассматриваются содержание, правила выбора и реализации мер защиты информации, связанных с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации. Принятие таких мер защиты информации обеспечивается в соответствии с законодательством Российской Федерации.

Методический документ предназначен для обладателей информации, заказчиков, заключивших государственный контракт на создание информационной системы (далее – заказчики), операторов информационных систем (далее – операторы), лиц, обрабатывающих информацию, являющуюся государственным информационным ресурсом, по поручению обладателя информации (заказчика) или оператора и (или) предоставляющих им вычислительные ресурсы (мощности) для обработки информации на основании заключенного договора (далее – уполномоченные лица), а также лиц, привлекаемых в соответствии с законодательством Российской Федерации для проведения работ по созданию (проектированию) информационных систем в защищенном исполнении и (или) их систем защиты информации (далее – разработчики (проектировщики)).

Методический документ применяется для выбора и реализации в соответствии с пунктом 21 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17, мер защиты информации в информационных системах, направленных на обеспечение:

конфиденциальности информации (исключение неправомерного доступа, копирования, предоставления или распространения информации);

целостности информации (исключение неправомерного уничтожения или модифицирования информации);

доступности информации (исключение неправомерного блокирования информации).

Настоящий методический документ может применяться для защиты общедоступной информации, содержащейся в государственных информационных системах, для достижения целей, указанных в пунктах 1 и 3 части 1 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также для защиты информации, содержащейся в негосударственных информационных системах.

По решению оператора персональных данных настоящий методический документ применяется для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, защита которых обеспечивается в соответствии с Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18 февраля 2013 г. № 21 (зарегистрирован Минюстом России 14 мая 2013 г., рег. № 28375).

Для целей настоящего методического документа используются термины и определения, установленные законодательством Российской Федерации об информации, информационных технологиях и о защиты информации, термины и определения, установление национальными стандартами в области защиты информации, а также термины и определения, приведенные в приложении № 1 к настоящему методическому документу.

2. ВЫБОР МЕР ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ РЕАЛИЗАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ В РАМКАХ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Выбор мер защиты информации для их реализации в информационной системе осуществляется в ходе проектирования системы защиты информации информационной системы в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание системы защиты информации информационной системы.

Выбор мер защиты информации осуществляется исходя из класса защищенности информационной системы, определяющего требуемый уровень защищенности содержащейся в ней информации, и угроз безопасности информации, включенных в модель угроз безопасности информационной системы, а также с учетом структурно-функциональных характеристик информационной системы, к которым относятся структура и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, взаимосвязи с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

Правила и процедуры по реализации требований о защите информации и мер защиты информации в конкретной информационной системе определяются в эксплуатационной документации на систему защиты информации и организационно-распорядительных документах по защите информации.

Эксплуатационная документация на систему защиты информации разрабатывается с учетом национальных стандартов и, как правило, включает руководства пользователей и администраторов, инструкцию по эксплуатации комплекса средств защиты информации и иных технических средств, описание технологического процесса обработки информации, общее описание информационной системы, формуляр и паспорт информационной системы.

Организационно-распорядительные документы по защите информации включают, как правило, политики, стандарты организации, положения, планы, перечни, инструкции или иные виды документов, разрабатываемые оператором для регламентации процедур защиты информации в информационной системе в ходе ее эксплуатации.

2.1. Классификация информационной системы по требованиям защиты информации

Определение класса защищенности информационной системы проводится в соответствии с пунктом 14.2 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных

информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17.

Устанавливаются четыре класса защищенности информационной системы (первый класс (К1), второй класс (К2), третий класс (К3), четвертый класс (К4)), определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс – четвертый, самый высокий – первый.

Класс защищенности информационной системы определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый).

Класс защищенности (К) = [уровень значимости информации; масштаб системы].

Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности, целостности или доступности информации:

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)],

где степень возможного ущерба определяется обладателем информации (заказчиком) и (или) оператором самостоятельно экспертным или иными методами и может быть:

высокой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции;

средней, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций;

низкой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

Для определения степени возможного ущерба от нарушения конфиденциальности, целостности или доступности могут применяться национальные стандарты и (или) методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

Масштаб информационной системы определяется назначением и распределенностью сегментов информационной системы.

Информационная система имеет федеральный масштаб, если она функционирует на территории Российской Федерации (в пределах федерального округа) и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях.

Информационная система имеет региональный масштаб, если она функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях.

Информационная система имеет объектовый масштаб, если она функционирует на объектах одного федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

При обработке персональных данных в информационной системе определение класса защищенности информационной системы осуществляется с учетом требуемого уровня защищенности персональных данных, установленного в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119. При этом в соответствии с пунктом 27 Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17, должно быть обеспечено соответствующее соотношение класса защищенности государственной информационной системы с уровнем защищенности персональных данных. В случае, если определенный в установленном порядке уровень защищенности персональных данных выше чем установленный класс защищенности государственной информационной системы, то осуществляется повышение класса защищенности до значения, обеспечивающего выполнение пункта 27 Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17.

2.2 Определение угроз безопасности информации в информационной системе

Угрозы безопасности информации (УБИ) определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и

внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности)

УБИ = [возможности нарушителя; уязвимости информационной системы; способ реализации угрозы; последствия от реализации угрозы].

При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, применяемые информационные технологии и особенности (условия) функционирования информационной системы.

Эффективность принимаемых мер защиты информации в информационной системе зависит от качества определения угроз безопасности информации для конкретной информационной системы в конкретных условиях ее функционирования.

Модель угроз безопасности информации представляет собой формализованное описание угроз безопасности информации для конкретной информационной системы или группы информационных систем в определенных условиях их функционирования. Модель угроз безопасности информации разрабатывается обладателем информации (оператором, разработчиком (проектировщиком)) и должна по содержанию соответствовать Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы, разрабатываемые и утверждаемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

2.3 Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации

Меры защиты информации реализуются в информационной системе в рамках ее системы защиты информации в зависимости от класса защищенности информационной системы, угроз безопасности информации, структурно-функциональных характеристик информационной системы, применяемых информационных технологий и особенностей функционирования информационной системы.

В информационной системе подлежат реализации следующие меры защиты информации:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;
защита машинных носителей информации;
регистрация событий безопасности;
антивирусная защита;
обнаружение (предотвращение) вторжений;
контроль (анализ) защищенности информации;
обеспечение целостности информационной системы и информации;
обеспечение доступности информации;
защита среды виртуализации;
защита технических средств;
защита информационной системы, ее средств и систем связи и передачи данных.

Меры защиты информации, выбираемые для реализации в информационной системе, должны обеспечивать блокирование одной или нескольких угроз безопасности информации, включенных в модель угроз безопасности информации.

Содержание мер защиты информации для их реализации в информационных системах приведено в приложении № 2 к настоящему методическому документу. Описание представленных в приложении № 2 мер защиты информации приведено в разделе 3 настоящего методического документа.

Выбор мер защиты информации для их реализации в информационной системе включает (см. рисунок):

определение базового набора мер защиты информации для установленного класса защищенности информационной системы;

адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы;

уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации для блокирования (нейтрализации) всех угроз безопасности информации, включенных в модель угроз безопасности информации;

дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных.

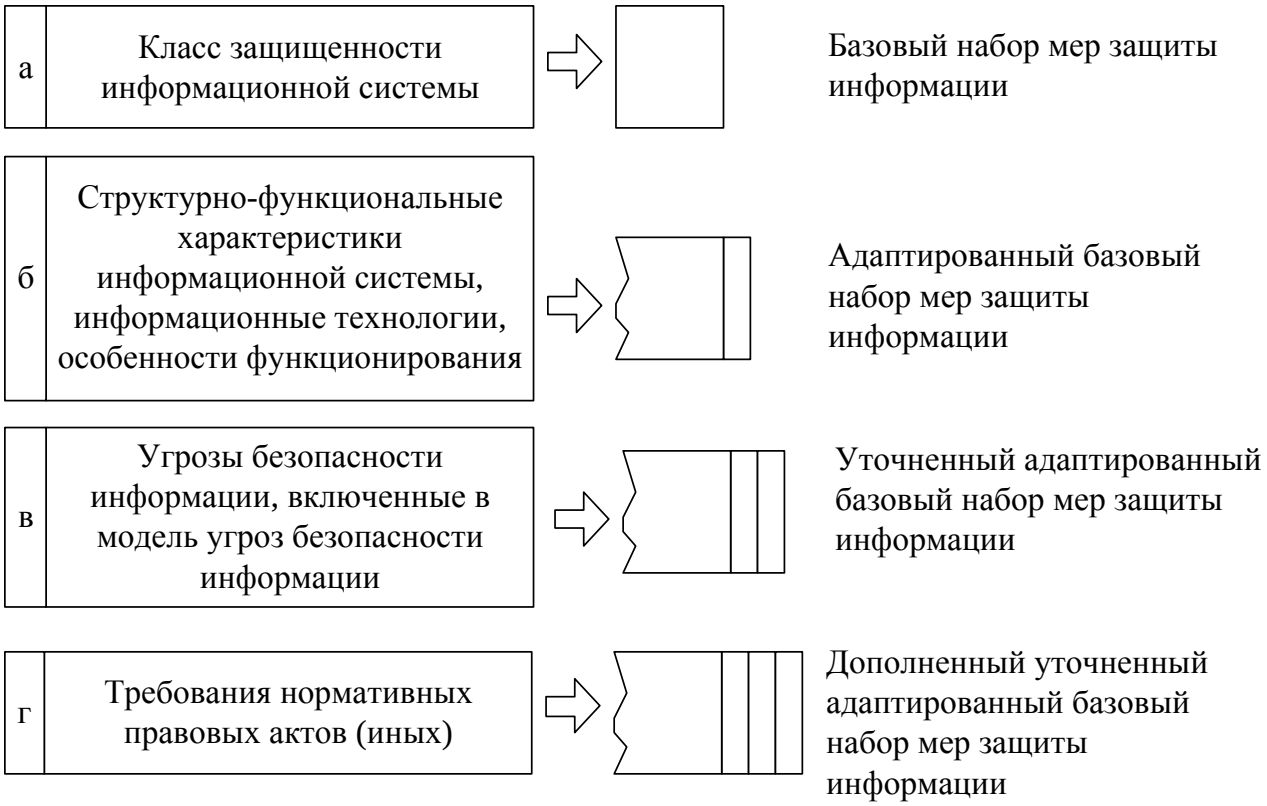

Рисунок – Общий порядок действий по выбору мер защиты информации для их реализации в информационной системе

При невозможности реализации в информационной системе в рамках ее системы защиты информации отдельных выбранных мер защиты информации на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

а) определение базового набора мер защиты информации

Определение базового набора мер защиты информации для установленного класса защищенности информационной системы является первым шагом в выборе мер защиты информации, подлежащих реализации в информационной системе. Определение базового набора мер защиты информации основывается на классе защищенности информационной системы, установленном в соответствии с пунктом 2.1 настоящего методического документа. В соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17, и приложением № 2 к настоящему методическому документу в качестве начального выбирается один из четырех базовых наборов мер защиты информации, соответствующий установленному классу

защищенности информационной системы. Меры защиты информации, обозначенные знаком «+» в приложении № 2 включены в базовый набор мер защиты информации для соответствующего класса защищенности информационной системы. Меры защиты информации, не обозначенные знаком «+», к базовому набору мер не относятся, и могут применяться при последующих действиях по адаптации, уточнению, дополнению мер защиты информации, а также разработке компенсирующих мер защиты информации.

Базовый набор мер защиты информации, выбранный в соответствии с классом защищенности информационной системы, подлежит адаптации применительно к структурно-функциональным характеристикам и особенностям функционирования информационной системы, уточнению в зависимости от угроз безопасности информации и при необходимости дополнению мерами защиты информации, включенными в иные нормативные правовые акты, нормативные и методические документы по защите информации.

б) адаптация базового набора мер защиты информации

Вторым шагом является изменение изначально выбранного базового набора мер защиты информации в части его максимальной адаптации применительно к структуре, реализации и особенностям эксплуатации информационной системы.

При адаптации базового набора мер защиты информации учитываются:

цели (обеспечение конфиденциальности, целостности и (или) доступности информации) и задачи защиты информации в информационной системе;

перечень мероприятий проводимых оператором по обеспечению безопасности в рамках организации в целом;

применяемые информационные технологии и структурно-функциональные характеристики информационной системы.

Адаптация базового набора мер защиты информации, как правило, предусматривает исключение мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе.

В качестве примера адаптации можно рассмотреть исключение из базового набора мер защиты информации мер по защите среды виртуализации, в случае если в информационной системе не применяется технология виртуализации, или исключение из базового набора мер защиты информации мер по защите мобильных технических средств, если такие мобильные устройства не применяются или их применение запрещено.

в) уточнение адаптированного базового набора мер защиты информации

Уточнение адаптированного базового набора мер защиты информации проводится с учетом результатов оценки возможности адаптированного базового набора мер защиты информации адекватно блокировать (нейтрализовать) все угрозы безопасности информации, включенные в модель угроз безопасности информации, или снизить вероятность их реализации исходя из условий функционирования информационной системы.

Исходными данными при уточнении адаптированного базового набора мер защиты информации являются перечень угроз безопасности информации и их характеристики (потенциал, оснащенность, мотивация), включенные в модель угроз безопасности информации.

При уточнении адаптированного базового набора мер защиты информации для каждой угрозы безопасности информации, включенной в модель угроз, сопоставляется мера защиты информации из адаптированного базового набора мер защиты информации, обеспечивающая блокирование этой угрозы безопасности или снижающая вероятность ее реализации исходя из условий функционирования информационной системы. В случае, если адаптированный базовый набор мер защиты информации не обеспечивает блокирование (нейтрализацию) всех угроз безопасности информации в него дополнительно включаются меры защиты информации, приведенные в разделе 3 настоящего методического документа. При этом содержание данной меры защиты информации определяется с учетом класса защищенности информационной системы и потенциала нарушителя в соответствии с разделом 3 настоящего методического документа.

В качестве примера процедуры по уточнению адаптированного базового набора мер защиты информации можно рассмотреть дополнение адаптированных мер защиты информации в информационной системе 3 класса защищенности мерой по обеспечению доверенной загрузки в случае, если в модели угроз безопасности информации приведены угрозы, связанные с возможностью загрузки операционной системы с нештатного машинного носителя или нарушения целостности программной среды и (или) состава компонентов аппаратного обеспечения средств вычислительной техники в информационной системе.

Уточненный адаптированный базовый набор мер защиты информации подлежит реализации в информационной системе в соответствии с разделом 3 настоящего методического документа.

В подразделах «**требования к реализации меры защиты информации**» для каждой меры, приведенной в разделе 3 настоящего методического документа, указано требование к тому, каким образом и в каком объеме должна быть реализована каждая мера защиты информации. Требования к реализации мер защиты информации являются минимальными требованиями, выполнение которых должно быть обеспечено в информационной системе соответствующего класса защищенности, в случае если эта мера выбрана для

реализации в качестве уточненной адаптированной базовой меры защиты информации.

В зависимости от класса защищенности информационной системы минимальные требования к реализации уточненной адаптированной базовой меры защиты информации подлежат усилению для повышения уровня защищенности информации. Все возможные усиления мер защиты информации приведены в подразделах «**требования к усилению меры защиты информации**», приведенных в разделе 3 настоящего методического документа для каждой меры защиты информации. Усиления мер защиты информации применяются дополнительно к требованиям по реализации мер защиты информации, приведенным в подразделах «**требования к реализации меры защиты информации**».

Итоговое содержание каждой уточненной адаптированной базовой меры защиты информации, которое, как минимум, должно быть реализовано в информационной системе, приведено в таблице подраздела «**содержание базовой меры защиты информации**».

Усиления мер защиты информации, приведенные в подразделе «**требования к усилению меры защиты информации**» и не включенные в таблицу с содержанием базовой меры защиты информации в подразделе «**содержание базовой меры защиты информации**», применяется по решению обладателя информации, заказчика и (или) оператора для повышения уровня защищенности информации, содержащейся в информационной системе, или при адаптации, уточнении, дополнении мер защиты информации, а также при разработке компенсирующих мер защиты информации.

г) дополнение уточненного адаптированного базового набора мер защиты информации

Дополнение уточненного адаптированного базового набора мер защиты информации осуществляется с целью выполнения требований о защите информации, установленных иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных.

Дополнение уточненного адаптированного базового набора мер защиты информации может потребоваться в следующих случаях:

а) если федеральным законом, указом Президента Российской Федерации, постановлением Правительства Российской Федерации, нормативными актами органа государственной власти, органа местного самоуправления или организации, определяющими порядок создания и эксплуатации информационной системы, устанавливаются дополнительные требования к защите информации, выполнение которых не предусмотрено Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17;

б) политиками обеспечения информационной безопасности обладателя информации (заказчика), оператора и уполномоченного лица, разработанными по ГОСТ Р ИСО/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», предъявлены дополнительные требования к защите информации в информационной системе.

При дополнении уточненного адаптированного базового набора мер защиты информации возможны следующие действия:

1) может быть обосновано, что меры защиты информации, включенные в уточненный адаптированный базовый набор мер защиты информации, достаточны для выполнения дополнительных требований, установленных федеральным законом, указом Президента Российской Федерации, постановлением Правительства Российской Федерации, нормативными актами органа государственной власти, органа местного самоуправления или организации. В этом случае дополнение уточненного адаптированного базового набора мер защиты информации не требуется;

2) могут быть усилены (ужесточены) требования к некоторым мерам защиты информации, ранее включенным в уточненный адаптированный базовый набор мер защиты информации, до уровня, обеспечивающего выполнение дополнительных требований, установленных федеральным законом, указом Президента Российской Федерации, постановлением Правительства Российской Федерации, нормативными актами органа государственной власти, органа местного самоуправления или организации;

3) может быть дополнен уточненный адаптированный базовый набор мер защиты информации мерами защиты информации для выполнения дополнительных требований, установленных федеральным законом, указом Президента Российской Федерации, постановлением Правительства Российской Федерации, нормативными актами органа государственной власти, органа местного самоуправления или организации в случае, если такие меры не установлены Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17.

д) применение компенсирующих мер защиты информации

Сформированный набор мер защиты информации может содержать меры защиты информации, которые по каким-либо причинам (высокая стоимость, отсутствие апробированных технических реализаций, неприемлемо большие сроки реализации, отсутствие компетенции для эксплуатации и другие) делает невозможным или крайне затруднительным их реализацию в информационной системе в рамках ее системы защиты информации.

В таких случаях у заказчика, оператора и разработчика (проектировщика) есть возможность заменить соответствующие меры защиты информации на компенсирующие меры защиты информации.

В качестве исходных данных для разработки компенсирующих мер защиты информации, в первую очередь, необходимо рассматривать:

приложение № 2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17, и раздел 3 настоящего методического документа;

международные, национальные стандарты, стандарты организаций в области информационной безопасности;

результаты собственных разработок (научно-исследовательские и опытно-конструкторские работы).

При этом должно быть проведено обоснование применения компенсирующих мер защиты информации, включающее:

изложение причин исключения меры (мер) защиты информации;

сопоставление исключаемой меры (мер) защиты информации с блокируемой (нейтрализуемой) угрозой (угрозами) безопасности информации;

описание содержания компенсирующих мер защиты информации;

сравнительный анализ компенсирующих мер защиты информации с исключаемыми мерами защиты информации;

аргументацию, что предлагаемые компенсирующие меры защиты информации обеспечивают адекватное блокирование (нейтрализацию) угроз безопасности информации.

Разработанное обоснование должно быть представлено при проведении аттестационных испытаний. При аттестационных испытаниях с учетом представленного обоснования должны быть оценены достаточность и адекватность компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

3. СОДЕРЖАНИЕ МЕР ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

3.1. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ СУБЪЕКТОВ ДОСТУПА И ОБЪЕКТОВ ДОСТУПА (ИАФ)

ИАФ.1 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ, ЯВЛЯЮЩИХСЯ РАБОТНИКАМИ ОПЕРАТОРА

Требования к реализации ИАФ.1: В информационной системе должна обеспечиваться идентификация и аутентификация пользователей, являющихся работниками оператора.

При доступе в информационную систему должна осуществляться идентификация и аутентификация пользователей, являющихся работниками оператора (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

К внутренним пользователям в целях настоящего документа, относятся должностные лица оператора (пользователи, администраторы), выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств информационной системы в соответствии с должностными регламентами (инструкциями) утвержденными оператором и которым в информационной системе присвоены учетные записи.

В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица, привлекаемые на договорной основе для обеспечения функционирования информационной системы (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами оператора и которым в информационной системе также присвоены учетные записи.

Пользователи информационной системы должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с мерой защиты информации УПД.11.

Аутентификация пользователя осуществляется с использованием паролей, аппаратных средств, биометрических характеристик, иных средств или в случае многофакторной (двухфакторной) аутентификации – определенной комбинации указанных средств.

В информационной системе должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

Правила и процедуры идентификации и аутентификации пользователей регламентируются в организационно-распорядительных документах по защите информации.

Требования к усилению ИАФ.1:

1) в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами привилегированных учетных записей (администраторов):

а) с использованием сети связи общего пользования, в том числе сети Интернет;

б) без использования сети связи общего пользования;

2) в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами непривилегированных учетных записей (пользователей):

а) с использованием сети связи общего пользования, в том числе сети Интернет;

б) без использования сети связи общего пользования;

3) в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами привилегированных учетных записей (администраторов);

4) в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами непривилегированных учетных записей (пользователей);

5) в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация при доступе в систему с правами привилегированных учетных записей (администраторов), где один из факторов обеспечивается аппаратным устройством аутентификации, отделенным от информационной системы, к которой осуществляется доступ;

6) в информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация при доступе в систему с правами непривилегированных учетных записей (пользователей), где один из факторов обеспечивается устройством, отделенным от информационной системы, к которой осуществляется доступ;

7) в информационной системе должен использоваться механизм одноразовых паролей при аутентификации пользователей, осуществляющих удаленный или локальный доступ;

8) в информационной системе для аутентификации пользователей должно обеспечиваться применение в соответствии с законодательством Российской Федерации криптографических методов защиты информации.

Содержание базовой меры ИАФ.1:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ИАФ.1	+	+	+	+
Усиление ИАФ.1			1а, 2а, 3	1а, 2а, 3, 4

ИАФ.2 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ УСТРОЙСТВ, В ТОМ ЧИСЛЕ СТАЦИОНАРНЫХ, МОБИЛЬНЫХ И ПОРТАТИВНЫХ

Требования к реализации ИАФ.2: В информационной системе до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация и аутентификация устройств (технических средств).

Оператором должен быть определен перечень типов устройств, используемых в информационной системе и подлежащих идентификации и аутентификации до начала информационного взаимодействия.

Идентификация устройств в информационной системе обеспечивается по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства.

Аутентификация устройств в информационной системе обеспечивается с использованием соответствующих протоколов аутентификации или с применением в соответствии с законодательством Российской Федерации криптографических методов защиты информации.

Правила и процедуры идентификации и аутентификации устройств регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ИАФ.2:

1) в информационной системе должна обеспечиваться аутентификация устройств до начала информационного взаимодействия с ними:

а) взаимная аутентификация устройства и средства вычислительной техники (или другого взаимодействующего устройства);

б) аутентификация по уникальным встроенным средствам аутентификации.

Содержание базовой меры ИАФ.2:

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

ИАФ.3 УПРАВЛЕНИЕ ИДЕНТИФИКАТОРАМИ, В ТОМ ЧИСЛЕ СОЗДАНИЕ, ПРИСВОЕНИЕ, УНИЧТОЖЕНИЕ ИДЕНТИФИКАТОРОВ

Требования к реализации ИАФ.3: Оператором должны быть установлены и реализованы следующие функции управления идентификаторами пользователей и устройств в информационной системе:

определение должностного лица (администратора) оператора, ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств;

формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;

присвоение идентификатора пользователю и (или) устройству;

предотвращение повторного использования идентификатора пользователя и (или) устройства в течение установленного оператором периода времени;

блокирование идентификатора пользователя после установленного оператором времени неиспользования.

Правила и процедуры управления идентификаторами регламентируются в организационно-распорядительных документах оператора по защите информации.

Требование к усилению ИАФ.3:

1) оператором должно быть исключено повторное использование идентификатора пользователя в течение:

а) не менее одного года;

б) не менее трех лет;

в) в течение всего периода эксплуатации информационной системы;

2) оператором должно быть обеспечено блокирование идентификатора пользователя через период времени неиспользования:

а) не более 90 дней;

б) не более 45 дней;

3) оператором должно быть обеспечено использование различной аутентификационной информации (различных средств аутентификации) пользователя для входа в информационную систему и доступа к прикладному (специальному) программному обеспечению;

4) оператором должно быть исключено использование идентификатора пользователя информационной системы при создании учетной записи пользователя публичной электронной почты или иных публичных сервисов;

5) оператором должно быть обеспечено управление идентификаторами внешних пользователей, учетные записи которых используются для доступа к общедоступным ресурсам информационной системы.

Содержание базовой меры ИАФ.3:

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

Требования к реализации ИАФ.4: Оператором должны быть установлены и реализованы следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств в информационной системе:

определение должностного лица (администратора) оператора, ответственного за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;

изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации информационной системы;

выдача средств аутентификации пользователям;

генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);

установление характеристик пароля (при использовании в информационной системе механизмов аутентификации на основе пароля):

а) задание минимальной сложности пароля с определяемыми оператором требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;

б) задание минимального количества измененных символов при создании новых паролей;

в) задание максимального времени действия пароля;

г) задание минимального времени действия пароля;

д) запрет на использование пользователями определенного оператором числа последних использованных паролей при создании новых паролей;

блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;

назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);

обновление аутентификационной информации (замена средств аутентификации) с периодичностью, установленной оператором;

защита аутентификационной информации от неправомерных доступа к ней и модифицирования.

Правила и процедуры управления средствами аутентификации (аутентификационной информацией) регламентируются в организационно-распорядительных документах оператора по защите информации.

Требование к усилению ИАФ.4:

1) в случае использования в информационной системе механизмов аутентификации на основе пароля (иной последовательности символов, используемой для аутентификации) или применения пароля в качестве одного из факторов многофакторной аутентификации, его характеристики должны быть следующими:

а) длина пароля не менее шести символов, алфавит пароля не менее 30 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 3 до 15 минут, смена паролей не более чем через 180 дней;

б) длина пароля не менее шести символов, алфавит пароля не менее 60 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут, смена паролей не более чем через 120 дней;

в) длина пароля не менее шести символов, алфавит пароля не менее 70 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 8 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 10 до 30 минут, смена паролей не более чем через 90 дней;

г) длина пароля не менее восьми символов, алфавит пароля не менее 70 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 4 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 15 до 60 минут, смена паролей не более чем через 60 дней;

2) в информационной системе должно быть обеспечено использование автоматизированных средств для формирования аутентификационной информации (генераторов паролей) с требуемыми характеристиками стойкости (силы) механизма аутентификации и для оценки характеристик этих механизмов;

3) в информационной системе должно быть обеспечено использование серверов и (или) программного обеспечения аутентификации для единой аутентификации в компонентах информационной системы и компонентах программного обеспечения, предусматривающего собственную аутентификацию;

4) оператор должен обеспечить получение (запросить) у поставщика технических средств и программного обеспечения информационной системы аутентификационную информацию, заданную производителем этих технических средств и программного обеспечения и не указанную в эксплуатационной документации;

5) оператором должны быть определены меры по исключению возможности использования пользователями их идентификаторов и паролей в других информационных системах.

Содержание базовой меры ИАФ.4

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ИАФ.4	+	+	+	+
Усиление ИАФ.4	1а	1б	1в	1г

ИАФ.5 ЗАЩИТА ОБРАТНОЙ СВЯЗИ ПРИ ВВОДЕ АУТЕНТИФИКАЦИОННОЙ ИНФОРМАЦИИ

Требования к реализации ИАФ.5: В информационной системе должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

Защита обратной связи «система - субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками«*», «•» или иными знаками.

Требования к усилению ИАФ.5:

Не установлены.

Содержание базовой меры ИАФ.5:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ИАФ.5	+	+	+	+
Усиление ИАФ.5				

ИАФ.6 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ, НЕ ЯВЛЯЮЩИХСЯ РАБОТНИКАМИ ОПЕРАТОРА (ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ)

Требования к реализации ИАФ.6: В информационной системе должна осуществляться однозначная идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей), или процессов, запускаемых от имени этих пользователей.

К пользователям, не являющимся работникам оператора (внешним пользователям), относятся все пользователи информационной системы, не указанные в ИАФ.1 в качестве внутренних пользователей. Примером внешних пользователей являются граждане, на законных основаниях через сеть Интернет получающие доступ к информационным ресурсам портала Государственных услуг Российской Федерации «Электронного правительства» или официальным сайтам в сети Интернет органов государственной власти.

Пользователи информационной системы должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с мерой защиты информации УПД.11.

Идентификация и аутентификация внешних пользователей в целях предоставления государственных услуг осуществляется в том числе с использованием единой системы идентификации и аутентификации, созданной в соответствии с постановлением Правительства Российской Федерации от 28 ноября 2011 г. № 977.

Правила и процедуры идентификации и аутентификации пользователей регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ИАФ.6:

Не установлены.

Содержание базовой меры ИАФ.6:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ИАФ.6	+	+	+	+
Усиление ИАФ.6				

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

Требования к реализации ИАФ.7: В информационной системе должна осуществляться 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.

Требования к усилению ИАФ.7:

1) в информационной системе должна обеспечиваться аутентификация объектов файловой системы с использованием свидетельств подлинности информации (в том числе электронной подписи или иных свидетельств подлинности информации);

2) в информационной системе должна обеспечиваться аутентификация запускаемых и исполняемых модулей с использованием свидетельств подлинности модулей (в том числе цифровых сигнатур производителя или иных свидетельств подлинности модулей).

Содержание базовой меры ИАФ.7:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ИАФ.7				
Усиление ИАФ.7				

3.2. УПРАВЛЕНИЕ ДОСТУПОМ СУБЪЕКТОВ ДОСТУПА К ОБЪЕКТАМ ДОСТУПА (УПД)

УПД.1 УПРАВЛЕНИЕ (ЗАВЕДЕНИЕ, АКТИВАЦИЯ, БЛОКИРОВАНИЕ И УНИЧТОЖЕНИЕ) УЧЕТНЫМИ ЗАПИСЯМИ ПОЛЬЗОВАТЕЛЕЙ, В ТОМ ЧИСЛЕ ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ

Требования к реализации УПД.1: Оператором должны быть установлены и реализованы следующие функции управления учетными записями пользователей, в том числе внешних пользователей:

определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей);

объединение учетных записей в группы (при необходимости);

верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;

заведение, активация, блокирование и уничтожение учетных записей пользователей;

пересмотр и, при необходимости, корректировка учетных записей пользователей с периодичностью, определяемой оператором;

порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов;

оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;

уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;

предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами.

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

Правила и процедуры управления учетными записями пользователей регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.1:

1) оператором должны использоваться автоматизированные средства поддержки управления учетными записями пользователей;

2) в информационной системе должно осуществляться автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования;

3) в информационной системе должно осуществляться автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования:

а) более 90 дней;

б) более 45 дней;

4) в информационной системе должно осуществляться автоматическое блокирование учетных записей пользователей:

а) при превышении установленного оператором числа неуспешных попыток аутентификации пользователя;

б) при выявлении по результатам мониторинга (просмотра, анализа) журналов регистрации событий безопасности действий пользователей, которые отнесены оператором к событиям нарушения безопасности информации;

5) в информационной системе должен осуществляться автоматический контроль заведения, активации, блокирования и уничтожения учетных записей пользователей и оповещение администраторов о результатах автоматического контроля.

Содержание базовой меры УПД.1:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
УПД.1	+	+	+	+
Усиление УПД.1		1, 2	1, 2, 3а	1, 2, 3б

УПД.2 РЕАЛИЗАЦИЯ НЕОБХОДИМЫХ МЕТОДОВ УПРАВЛЕНИЯ ДОСТУПОМ (ДИСКРЕЦИОННЫЙ, МАНДАТНЫЙ, РОЛЕВОЙ ИЛИ ИНОЙ МЕТОД), ТИПОВ (ЧТЕНИЕ, ЗАПИСЬ, ВЫПОЛНЕНИЕ ИЛИ ИНОЙ ТИП) И ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА

Требования к реализации УПД.2: В информационной системе для управления доступом субъектов доступа к объектам доступа должны быть реализованы установленные оператором методы управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа.

Методы управления доступом реализуются в зависимости от особенностей функционирования информационной системы, с учетом угроз

безопасности информации и должны включать один или комбинацию следующих методов:

дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа;

ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности);

мандатный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе сопоставления классификационных меток каждого субъекта доступа и каждого объекта доступа, отражающих классификационные уровни субъектов доступа и объектов доступа, являющиеся комбинациями иерархических и неиерархических категорий.

Типы доступа должны включать операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению пользователем (группе пользователей) или запускаемому от его имени процессу при доступе к объектам доступа.

Правила разграничения доступа реализуются на основе установленных оператором списков доступа или матриц доступа и должны обеспечивать управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа.

Правила разграничения доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.2:

1) в информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов при входе в информационную систему;

2) в информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к техническим средствам, устройствам, внешним устройствам;

3) в информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к объектам, создаваемым общесистемным (общим) программным обеспечением;

4) в информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к объектам, создаваемым прикладным и специальным программным обеспечением.

Содержание базовой меры УПД.2:

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

Требования к реализации УПД.3: В информационной системе должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы, включающее:

фильтрацию информационных потоков в соответствии с правилами управления потоками, установленными оператором;

разрешение передачи информации в информационной системе только по маршруту, установленному оператором;

изменение (перенаправление) маршрута передачи информации в случаях, установленных оператором;

запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в случаях, установленных оператором.

Управление информационными потоками должно обеспечивать разрешенный (установленный оператором) маршрут прохождения информации между пользователями, устройствами, сегментами в рамках информационной системы, а также между информационными системами или при взаимодействии с сетью Интернет(или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации информационной системы, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации). Управление информационными потоками должно блокировать передачу защищаемой информации через сеть Интернет (или

другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из информационной системы и (или) входящие в информационную систему.

Правила и процедуры управления информационными потоками регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.3:

1) в информационной системе должно обеспечиваться управление информационными потоками на основе атрибутов (меток) безопасности, связанных с передаваемой информацией, источниками и получателями информации;

2) в информационной системе должно обеспечиваться динамическое управление информационными потоками, запрещающее и (или) разрешающее передачу информации на основе анализа изменения текущего состояния информационной системы или условий ее функционирования;

3) в информационной системе должен исключаться обход правил управления информационными потоками за счет преобразования передаваемой информации;

4) в информационной системе должен исключаться обход правил управления информационными потоками за счет встраивания одних данных в другие данные информационного потока;

5) в информационной системе должен обеспечиваться контроль соединений между техническими средствами (устройствами), используемыми для организации информационных потоков;

6) в информационной системе при передаче информации между сегментами информационной системы и (или) информационными системами разных классов защищенности должна обеспечиваться однонаправленная передача информации с использованием аппаратных средств;

7) в информационной системе должно обеспечиваться управление информационными потоками на основе структуры передаваемых данных (текст, таблицы, видео, аудиоинформация);

8) в информационной системе должно обеспечиваться управление информационными потоками на основе используемых сетевых протоколов;

9) в информационной системе должно обеспечиваться управление информационными потоками на основе типов (расширений) файлов и (или) имен файлов;

10) в информационной системе должна обеспечиваться возможность запрета, разрешения и изменения маршрута передачи информации только администраторами;

11) в информационной системе должно обеспечиваться разделение информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской информации;

12) в информационной системе должна обеспечиваться возможность автоматического блокирования передачи информации при выявлении в передаваемой информации вредоносных компьютерных программ;

13) в информационной системе должно осуществляться управление информационными потоками при передаче информации между информационными системами;

14) в информационной системе должна обеспечиваться возможность фильтрации информационных потоков на уровне прикладного программного обеспечения (приложений).

15) в информационной системе должна осуществляться накопление статистических данных, проверка и фильтрация сетевых пакетов по их содержимому (технология DPI);

16) наделение трафика конкретными параметрами (в частности включение уведомлений пользователей, исключение или замена элементов трафика) в зависимости от получателя информации.

Содержание базовой меры УПД.3:

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

УПД.4 РАЗДЕЛЕНИЕ ПОЛНОМОЧИЙ (РОЛЕЙ) ПОЛЬЗОВАТЕЛЕЙ, АДМИНИСТРАТОРОВ И ЛИЦ, ОБЕСПЕЧИВАЮЩИХ ФУНКЦИОНИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Требования к реализации УПД.4: Оператором должно быть обеспечено разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями (функциями), фиксирование в организационно-распорядительных документах по защите информации (документирование) полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей).

Доступ к объектам доступа с учетом разделения полномочий (ролей) обеспечивается в соответствии с УПД.2.

Требования к усилению УПД.4:

1) оператором должно быть обеспечено выполнение каждой роли по обработке информации, администрированию информационной системы, ее

системы защиты информации, контролю (мониторингу) за обеспечением уровня защищенности информации, обеспечению функционирования информационной системы отдельным должностным лицом;

2) оператором должно быть обеспечено исключение наделения одного должностного лица полномочиями (ролью) по обработке информации и полномочиями (ролью) по администрированию информационной системы и (или) ее системы защиты информации, контролю (мониторингу) за обеспечением уровня защищенности информации, обеспечению функционирования информационной системы;

3) оператором должно быть обеспечено исключение наделения одного должностного лица полномочиями (ролью) по контролю (мониторингу) за обеспечением уровня защищенности информации и полномочиями (ролью) по администрированию информационной системы и (или) ее системы защиты информации и обеспечению функционирования информационной системы;

4) оператором должно быть обеспечено исключение наделения одного должностного лица полномочиями (ролью) по администрированию системы защиты информации информационной системы и полномочиями (ролью) по обеспечению функционирования информационной системы;

5) оператором должен быть определен администратор, имеющий права по передаче полномочий по администрированию информационной системы и системы защиты информации другим лицам и осуществляющий контроль за использованием переданных полномочий (супервизор).

Содержание базовой меры УПД.4:

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

УПД.5 НАЗНАЧЕНИЕ МИНИМАЛЬНО НЕОБХОДИМЫХ ПРАВ И ПРИВИЛЕГИЙ ПОЛЬЗОВАТЕЛЯМ, АДМИНИСТРАТОРАМ И ЛИЦАМ, ОБЕСПЕЧИВАЮЩИМ ФУНКЦИОНИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Требования к реализации УПД.5: Оператором должно быть обеспечено назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями.

Оператором должны быть однозначно определены и зафиксированы в организационно-распорядительных документах по защите информации (задокументированы) роли и (или) должностные обязанности (функции), также объекты доступа, в отношении которых установлен наименьший уровень привилегий. Доступ к объектам доступа с учетом минимально необходимых прав и привилегий обеспечивается в соответствии с УПД.2.

Требования к усилению УПД.5:

1) оператором должно быть обеспечено предоставление прав и привилегий по доступу к функциям безопасности (параметрам настройки) средств защиты информации исключительно администратору, наделенному полномочиями по администрированию системы защиты информации (администратору безопасности);

2) запрет предоставления расширенных прав и привилегий внешним пользователям (пользователям, не являющимся внутренними пользователями).

Содержание базовой меры УПД.5:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
УПД.5		+	+	+
Усиление УПД.5				1

УПД.6 ОГРАНИЧЕНИЕ НЕУСПЕШНЫХ ПОПЫТОК ВХОДА В ИНФОРМАЦИОННУЮ СИСТЕМУ (ДОСТУПА К ИНФОРМАЦИОННОЙ СИСТЕМЕ)

Требования к реализации УПД.6: В информационной системе должно быть установлено и зафиксировано в организационно-распорядительных документах оператора по защите информации (задокументировано) ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) за период времени, установленный оператором, а также обеспечено блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к информационной системе).

Ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе)должно обеспечиваться в соответствии с ИАФ.4

Требования к усилению УПД.6:

1) в информационной системе обеспечивается автоматическое блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к информационной системе) за установленный период времени с возможностью разблокирования только администратором или иным лицом, имеющим соответствующие полномочия (роль);

2) в информационной системе обеспечивается автоматическое удаление информации с мобильного технического средства, входящего в состав информационной системы, при превышении допустимого числа неуспешных попыток входа в информационную систему (доступа к информационной системе) за установленный период времени, осуществляемых с мобильного устройства;

3) в информационной системе обеспечивается противодействие автоматизированному подбору паролей с использованием однократных кодов, требующих визуального распознавания (в том числе с использованием технологии CAPTCHA).

Содержание базовой меры УПД.6:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
УПД.6	+	+	+	+
Усиление УПД.6				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

Требования к реализации УПД.7: В информационной системе должно быть обеспечено предупреждение пользователя в виде сообщения («окна») при его входе в информационную систему (до процесса аутентификации) о том, что в информационной системе реализованы меры защиты информации, а также о том, что при работе в информационной системе пользователем должны быть соблюдены установленные оператором правила и ограничения на работу с информацией.

Вход в информационную систему и предоставление пользователю возможности работы в информационной системе осуществляются только после подтверждения пользователем ознакомления с предупреждением.

Требования к усилению УПД.7:
Не установлены.

Содержание базовой меры УПД.7:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
УПД.7				
Усиление УПД.7				

УПД.8 ОПОВЕЩЕНИЕ ПОЛЬЗОВАТЕЛЯ ПОСЛЕ УСПЕШНОГО ВХОДА В ИНФОРМАЦИОННУЮ СИСТЕМУ О ЕГО ПРЕДЫДУЩЕМ ВХОДЕ В ИНФОРМАЦИОННУЮ СИСТЕМУ

Требования к реализации УПД.8: В информационной системе должно быть обеспечено после успешного входа пользователя в информационную систему (завершения процесса аутентификации) оповещение этого пользователя о дате и времени предыдущего входа в информационную систему от имени этого пользователя.

Требования к усилению УПД.8:

1) в информационной системе обеспечивается оповещение пользователя после успешного входа в информационную систему о количестве неуспешных попыток входа в информационную систему (доступа к информационной системе), зафиксированных с момента последнего успешного входа в информационную систему;

2) в информационной системе обеспечивается оповещение пользователя после успешного входа в информационную систему о количестве успешных и (или) неуспешных попыток входа в информационную систему (доступа к информационной системе), зафиксированных за период времени не менее 7 дней;

3) в информационной системе обеспечивается оповещение пользователя после успешного входа в информационную систему об изменении сведений, относящихся к учетной записи пользователя (в том числе изменении прав доступа), произведенных за период времени не менее, чем с момента предыдущего успешного входа в информационную систему.

Содержание базовой меры УПД.8:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
УПД.8				
Усиление УПД.8				

УПД.9 ОГРАНИЧЕНИЕ ЧИСЛА ПАРАЛЛЕЛЬНЫХ СЕАНСОВ ДОСТУПА ДЛЯ КАЖДОЙ УЧЕТНОЙ ЗАПИСИ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Требования к реализации УПД.9: В информационной системе должно обеспечиваться ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы.

В информационной системе должна быть предусмотрена возможность задавать ограничения на число параллельных (одновременных) сеансов (сессий), основываясь на идентификаторах пользователей и (или) принадлежности к определенной роли.

Значение числа параллельных сеансов доступа может быть задано для информационной системы в целом, для отдельных сегментов информационной системы, для групп пользователей, отдельных пользователей или их комбинаций.

Ограничения числа параллельных сеансов доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.9:

1) в информационной системе для привилегированных учетных записей (администраторов) количество параллельных (одновременных) сеансов (сессий) от их имени с разных устройств (средств вычислительной техники) не должно превышать следующих значений:

а) не более 2;

б) не более 1;

2) в информационной системе в случае попытки входа под учетной записью пользователя или администратора, для которых достигнуто максимальное значение допустимых параллельных сеансов, при успешной аутентификации пользователя или администратора должно выдаваться сообщение о превышении числа параллельных сеансов доступа, месте (местах) их предыдущего входа (предыдущих входов) с активными сессиями и предложением отключения этой сессии (этих сессий);

3) в информационной системе должны быть предусмотрены программно-технические средства, позволяющие контролировать и отображать

администратору число активных параллельных (одновременных) сеансов (сессий) для каждой учетной записи пользователей;

4) в информационной системе должны быть предусмотрены программно-технические средства, позволяющие оповещать администратора о попытках превышения числа установленных допустимых активных параллельных (одновременных) сеансов (сессий) для каждой учетной записи пользователя.

Содержание базовой меры УПД.9:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
УПД.9				+
Усиление УПД.9				1а, 3

УПД.10 БЛОКИРОВАНИЕ СЕАНСА ДОСТУПА В ИНФОРМАЦИОННУЮ СИСТЕМУ ПОСЛЕ УСТАНОВЛЕННОГО ВРЕМЕНИ БЕЗДЕЙСТВИЯ (НЕАКТИВНОСТИ) ПОЛЬЗОВАТЕЛЯ ИЛИ ПО ЕГО ЗАПРОСУ

Требования к реализации УПД.10: В информационной системе должно обеспечиваться блокирование сеанса доступа пользователя после установленного оператором времени его бездействия (неактивности) в информационной системе или по запросу пользователя.

Блокирование сеанса доступа пользователя в информационную систему обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к информационной системе (без выхода из информационной системы).

Для заблокированного сеанса должно осуществляться блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

Блокирование сеанса доступа пользователя в информационную систему должно сохраняться до прохождения им повторной идентификации и аутентификации в соответствии с ИАФ.1.

Правила и процедуры блокирования сеансов доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.10:

1) в информационной системе обеспечивается блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя:

а) до 15 минут;

б) до 5 минут;

2) в информационной системе на устройстве отображения (мониторе) после блокировки сеанса не должна отображаться информация сеанса пользователя (в том числе использование «хранителя экрана», гашение экрана или иные способы);

3) в информационной системе обеспечивается завершение сеанса пользователя (выхода из системы) после превышения установленного оператором времени бездействия (неактивности) пользователя.

Содержание базовой меры УПД.10:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
УПД.10		+	+	+
Усиление УПД.10			1а, 2	1б,2

УПД.11 РАЗРЕШЕНИЕ (ЗАПРЕТ) ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ, РАЗРЕШЕННЫХ ДО ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

Требования к реализации УПД.11: Оператором должен быть установлен перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет действий пользователей, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации.

Разрешение действий пользователей до прохождения ими процедур идентификации и аутентификации осуществляется, в том числе, при предоставлении пользователям доступа к общедоступной информации (веб-сайтам, порталам, иным общедоступным ресурсам). Также администратору разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

Правила и процедуры определения действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.11:

Не установлены.

Содержание базовой мерыУПД.11:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
УПД.11	+	+	+	+
Усиление УПД.11				

УПД.12 ПОДДЕРЖКА И СОХРАНЕНИЕ АТРИБУТОВ БЕЗОПАСНОСТИ (МЕТОК БЕЗОПАСНОСТИ), СВЯЗАННЫХ С ИНФОРМАЦИЕЙ В ПРОЦЕССЕ ЕЕ ХРАНЕНИЯ И ОБРАБОТКИ

Требования к реализации УПД.12: В информационной системе должны обеспечиваться поддержка (обновление, назначение, изменение) и сохранение атрибутов безопасности (меток безопасности), установленных оператором, связанных с информацией в процессе ее хранения и обработки.

Атрибуты безопасности (метки безопасности) представляют собой свойства (характеристики) объектов и (или) субъектов доступа, которые используются для контроля доступа субъектов к объектам доступа и управления информационными потоками.

Правила и процедуры поддержки и сохранения атрибутов безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.12:

1) в информационной системе обеспечивается динамическое изменение атрибутов безопасности в соответствии с организационно-распорядительными документами по защите информации оператора в зависимости от процесса обработки информации (формирование, объединение, разделение информационных ресурсов);

2) в информационной системе допускается изменение атрибутов безопасности только авторизованными пользователям или процессами;

3) в информационной системе обеспечивается автоматизированный контроль связи атрибутов безопасности с информацией;

4) в информационной системе обеспечивается возможность отображения пользователям в удобочитаемом виде атрибутов безопасности (меток безопасности) для каждого из объектов доступа (отображение атрибутов безопасности на экране монитора и (или) при выводе информации на печать на принтере).

Содержание базовой меры УПД.12:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
УПД.12				
Усиление УПД.12				

УПД.13 РЕАЛИЗАЦИЯ ЗАЩИЩЕННОГО УДАЛЕННОГО ДОСТУПА СУБЪЕКТОВ ДОСТУПА К ОБЪЕКТАМ ДОСТУПА ЧЕРЕЗ ВНЕШНИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ

Требования к реализации УПД.13: Оператором должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа информационной системы через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа).

Защита удаленного доступа должна обеспечиваться при всех видах доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа) и включает:

установление (в том числе документальное) видов доступа, разрешенных для удаленного доступа к объектам доступа информационной системы;

ограничение на использование удаленного доступа в соответствии с задачами (функциями) информационной системы, для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа в соответствии с УПД.2;

предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа информационной системы;

контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой (передачи защищаемой информации).

Правила и процедуры применения удаленного доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.13:

1) в информационной системе для мониторинга и контроля удаленного доступа должны применяться автоматизированные средства (дополнительные программные или программно-технические средства);

2) в информационной системе используется ограниченное (минимально необходимое) количество точек подключения к информационной системе при организации удаленного доступа к объектам доступа информационной системы;

3) в информационной системе исключается удаленный доступ от имени привилегированных учетных записей (администраторов) для администрирования информационной системы и ее системы защиты информации;

4) в информационной системе при удаленном доступе обеспечивается применение в соответствии с законодательством Российской Федерации криптографических методов защиты информации;

5) в информационной системе обеспечивается мониторинг и контроль удаленного доступа на предмет выявления установления несанкционированного соединения технических средств (устройств) с информационной системой;

6) в информационной системе должен обеспечиваться запрет удаленного доступа с использованием сетевых технологий и протоколов, определенных оператором по результатам анализа защищенности в соответствии с АНЗ.1как небезопасных.

Содержание базовой меры УПД.13:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
УПД.13	+	+	+	+
Усиление УПД.13		2, 3	2, 3, 5	1, 2, 3, 5

УПД.14 РЕГЛАМЕНТАЦИЯ И КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ТЕХНОЛОГИЙ БЕСПРОВОДНОГО ДОСТУПА

Требования к реализации УПД.14: Оператором должны обеспечиваться регламентация и контроль использования в информационной системе технологий беспроводного доступа пользователей к объектам доступа (стандарты коротковолновой радиосвязи, спутниковой и пакетной радиосвязи), направленные на защиту информации в информационной системе.

Регламентация и контроль использования технологий беспроводного доступа должны включать:

ограничение на использование технологий беспроводного доступа (беспроводной передачи данных, беспроводного подключения оборудования к сети, беспроводного подключения устройств к средству вычислительной техники) в соответствии с задачами (функциями) информационной системы, для решения которых такой доступ необходим, и предоставление беспроводного доступа в соответствии с УПД.2;

предоставление технологий беспроводного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

мониторинг и контроль применения технологий беспроводного доступа на предмет выявления несанкционированного использования технологий беспроводного доступа к объектам доступа информационной системы;

контроль беспроводного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой.

Правила и процедуры применения технологий беспроводного доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.14:

1) в информационной системе обеспечивается аутентификация подключаемых с использованием технологий беспроводного доступа устройств в соответствии с ИАФ.2;

2) в информационной системе обеспечивается мониторинг точек беспроводного подключения устройств к информационной системе на предмет выявления несанкционированного беспроводного подключения устройств;

3) в информационной системе исключается возможность изменения пользователем точек беспроводного доступа информационной системы;

4) оператором одолжен быть предусмотрен запрет беспроводного доступа к информационной системе из-за пределов контролируемой зоны;

5) в информационной системе должен быть запрещен беспроводный доступ от имени привилегированных учетных записей (администраторов) для администрирования информационной системы и ее системы защиты информации;

6) в информационной системе исключается возможность изменения пользователем устройств и настроек беспроводного доступа;

7) оператором обеспечивается определение местонахождения несанкционированного беспроводного устройства;

8) оператором обеспечивается блокирование функционирования несанкционированного беспроводного устройства.

Содержание базовой меры УПД.14:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
УПД.14	+	+	+	+
Усиление УПД.14		1	1, 3	1, 3, 4, 5

УПД.15 РЕГЛАМЕНТАЦИЯ И КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ В ИНФОРМАЦИОННОЙ СИСТЕМЕ МОБИЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ

Требования к реализации УПД.15: Оператором должны обеспечиваться регламентация и контроль использования в информационной системе мобильных технических средств, направленные на защиту информации в информационной системе.

В качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства).

Регламентация и контроль использования мобильных технических средств должны включать:

установление (в том числе документальное) видов доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа), разрешенных для доступа к объектам доступа информационной системы с использованием мобильных технических средств, входящих в состав информационной системы;

использование в составе информационной системы для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации в соответствии с ЗИС.30;

ограничение на использование мобильных технических средств в соответствии с задачами (функциями) информационной системы, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств в соответствии с УПД.2;

мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа информационной системы;

запрет возможности запуска без команды пользователя в информационной системе программного обеспечения (программного кода), используемого для взаимодействия с мобильным техническим средством.

Правила и процедуры применения мобильных технических средств, включая процедуры выдачи и возврата мобильных технических средств, а также их передачи на техническое обслуживание (процедура должна обеспечивать удаление или недоступность информации), регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.15:

1) оператором обеспечивается запрет использования в информационной системе, не входящих в ее состав (находящихся в личном использовании) съемных машинных носителей информации;

2) оператором обеспечивается запрет использования в информационной системе съемных машинных носителей информации, для которых не определен владелец (пользователь, организация, ответственные за принятие мер защиты информации);

3) оператором обеспечивается (в соответствии с процедурами, зафиксированными в организационно-распорядительных документах) очистка машинного носителя информации мобильного технического средства, переустановка программного обеспечения и выполнение иных мер по защите информации мобильных технических средств, после их использования за пределами контролируемой зоны;

4) оператором обеспечивается предоставление доступа с использованием мобильных технических средств к объектам доступа информационной системы только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

5) в информационной системе обеспечивается запрет использования мобильных технических средств, на которые в информационной системе может быть осуществлена запись информации (перезаписываемых съемных машинных носителей информации).

Содержание базовой меры УПД.15:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
УПД.15	+	+	+	+
Усиление УПД.15			1, 2	1, 2

УПД.16 УПРАВЛЕНИЕ ВЗАИМОДЕЙСТВИЕМ С ИНФОРМАЦИОННЫМИ СИСТЕМАМИ СТОРОННИХ ОРГАНИЗАЦИЙ (ВНЕШНИЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ)

Требования к реализации УПД.16: Оператором должно быть обеспечено управление взаимодействием с внешними информационными системами, включающими информационные системы и вычислительные ресурсы (мощности) уполномоченных лиц, информационные системы, с которыми установлено информационное взаимодействие на основании заключенного договора (соглашения), а также с иными информационными системами, информационное взаимодействие с которыми необходимо для функционирования информационной системы.

Управление взаимодействием с внешними информационными системами должно включать:

предоставление доступа к информационной системе только авторизованным (уполномоченным) пользователям в соответствии с УПД.2;

определение типов прикладного программного обеспечения информационной системы, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних информационных систем;

определение системных учетных записей, используемых в рамках данного взаимодействия;

определение порядка предоставления доступа к информационной системе авторизованными (уполномоченным) пользователями из внешних информационных систем;

определение порядка обработки, хранения и передачи информации с использованием внешних информационных систем.

Управление взаимодействием с внешними информационными системами в целях межведомственного электронного взаимодействия, исполнения государственных и муниципальных функций, формирования базовых государственных информационных ресурсов осуществляется в том числе с использованием единой системы идентификации и аутентификации, созданной в соответствии с постановлением Правительства Российской Федерации от 28 ноября 2011 г. № 977.

Правила и процедуры управления взаимодействием с внешними информационными системами регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.16:

1) оператор предоставляет доступ к информационной системе авторизованным (уполномоченным) пользователям внешних информационных систем или разрешает обработку, хранение и передачу информации с использованием внешней информационной системы при выполнении следующих условий:

а) при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;

б) при наличии подтверждения выполнения во внешней информационной системе предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

Содержание базовой меры УПД.16:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
УПД.16	+	+	+	+
Усиление УПД.16	1а	1а, 1б	1а, 1б	1а, 1б

УПД.17 ОБЕСПЕЧЕНИЕ ДОВЕРЕННОЙ ЗАГРУЗКИ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Требования к реализации УПД.17: В информационной системе должно обеспечиваться исключение несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники информационной системы на этапе его загрузки.

Доверенная загрузка должна обеспечивать:

блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы;

контроль доступа пользователей к процессу загрузки операционной системы;

контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники.

В информационной системе применяется доверенная загрузка на разных уровнях (уровня базовой системы ввода-вывода, уровня платы расширения и уровня загрузочной записи).

Правила и процедуры обеспечения доверенной загрузки средств вычислительной техники регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению УПД.17:

1) в информационной системе должна осуществляться доверенная загрузка уровня базовой системы ввода-вывода или уровня платы расширения;

2) в информационной системе должна осуществляться доверенная загрузка уровня базовой системы ввода-вывода или уровня платы расширения, реализованные на основе программно-аппаратного модуля;

3) в информационной системе должна осуществляться доверенная загрузка программного обеспечения телекоммуникационного оборудования;

Содержание базовой мерыУПД.17:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
УПД.17			+	+
Усиление УПД.17			1	2

3.3 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

Требования к реализации ОПС.1: Оператором должны быть реализованы следующие функции по управлению запуском (обращениями) компонентов программного обеспечения:

определение перечня (списка) компонентов программного обеспечения (файлов, объектов баз данных, хранимых процедур и иных компонентов),запускаемых автоматически при загрузке операционной системы средства вычислительной техники;

разрешение запуска компонентов программного обеспечения, включенных в перечень (список) программного обеспечения, запускаемого автоматически при загрузке операционной системы средства вычислительной техники;

ограничение запуска компонентов программного обеспечения от имени администраторов безопасности (например, разрешение такого запуска только для программного обеспечения средств защиты информации: сенсоры систем обнаружения вторжений, агенты систем мониторинга событий информационной безопасности, средства антивирусной защиты);

настройка параметров запуска компонентов программного обеспечения от имени учетной записи администратора безопасности таким образом, чтобы текущий пользователь средства вычислительной техники не мог получить через данные компоненты доступ к объектам доступа, на доступ к которым у него нет прав в соответствии с УПД.2;

контроль за запуском компонентов программного обеспечения, обеспечивающий выявление компонентов программного обеспечения, не включенных в перечень (список) компонентов, запускаемых автоматически при загрузке операционной системы средства вычислительной техники.

Правила и процедуры управления запуском программного обеспечения (в том числе списки программного обеспечения, ограничения запуска, параметры запуска компонентов программного обеспечения) регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОПС.1:

1) в информационной системе обеспечивается разрешение запуска только тех программных компонентов, которые явно разрешены администратором безопасности;

2) в информационной системе обеспечивается использование средств автоматизированного контроля перечня (списка)компонентов программного

обеспечения, запускаемого автоматически при загрузке операционной системы средства вычислительной техники;

3) в информационной системе обеспечивается использование автоматизированных механизмов управления запуском (обращениями) компонентов программного обеспечения;

4) в информационной системе обеспечивается управление удаленным запуском компонентов программного обеспечения (например, запрет запуска компонентов программного обеспечения на одном средстве вычислительной техники командой с другого средства вычислительной техники);

5) в информационной системе обеспечивается управление временем запуска и завершения работы компонентов программного обеспечения (например, ограничение запуска только в течение рабочего дня);

6) в информационной системе обеспечивается контроль целостности (состояния)запускаемых компонентов программного обеспечения (файлов (в том числе конфигурационных), объектов баз данных, подключаемых библиотек и др.) в соответствии с ОЦЛ.1;

7) в информационной системе обеспечивается контроль обновления запускаемых компонентов программного обеспечения;

8) в информационной системе обеспечивается регистрация событий, связанных с контролем состояния и обновлением запускаемых компонентов программного обеспечения;

9) в информационной системе обеспечивается запрет (блокирование) запуска определенных оператором компонентов программного обеспечения, не прошедших аутентификацию в соответствии с ИАФ.7.

Содержание базовой меры ОПС.1:

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

Требования к реализации ОПС.2: Оператором должны быть реализованы следующие функции по управлению установкой (инсталляцией) компонентов программного обеспечения информационной системы:

определение компонентов программного обеспечения (состава и конфигурации), подлежащих установке в информационной системе после загрузки операционной системы;

настройка параметров установки компонентов программного обеспечения, обеспечивающая исключение установки (если осуществимо) компонентов программного обеспечения, использование которых не требуется для реализации информационной технологии информационной системы (например, при запуске установщика можно выбрать или не выбрать определенные опции и, тем самым, разрешить или запретить установку соответствующих компонентов программного обеспечения);

выбор конфигурации устанавливаемых компонентов программного обеспечения (в том числе конфигурации, предусматривающие включение в домен, или не включение в домен);

контроль за установкой компонентов программного обеспечения (состав компонентов, параметры установки, конфигурация компонентов);

определение и применение параметров настройки компонентов программного обеспечения, включая программные компоненты средств защиты информации, обеспечивающих реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации.

Правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения (в том числе управления составом и конфигурацией подлежащих установке компонентов программного обеспечения, параметрами установки, параметрами настройки компонентов программного обеспечения) регламентируются в организационно-распорядительных документах оператора по защите информации с учетом эксплуатационной документации.

Требования к усилению ОПС.2:

1) в информационной системе должно обеспечиваться использование средств автоматизации для применения и контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации;

2) в информационной системе должны быть реализованы автоматизированные механизмы реагирования на несанкционированное изменение параметров настройки компонентов программного обеспечения, влияющих на безопасность информации, предусматривающие блокирование доступа к средству вычислительной техники и (или) информации, автоматическое восстановление параметров настройки или другие действия, препятствующие несанкционированному доступу к информации, который может быть получен вследствие несанкционированного изменения параметров настройки;

3) в информационной системе должно обеспечиваться использование средств автоматизации для инсталляции и централизованного управления

процессами инсталляции, в том числе с применением пакетов соответствующих дистрибутивов программного обеспечения.

Содержание базовой меры ОПС.2:

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

ОПС.3 УСТАНОВКА (ИНСТАЛЛЯЦИЯ) ТОЛЬКО РАЗРЕШЕННОГО К ИСПОЛЬЗОВАНИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И (ИЛИ) ЕГО КОМПОНЕНТОВ

Требования к реализации ОПС.3: Оператором должна быть обеспечена установка (инсталляция) только разрешенного к использованию в информационной системе программного обеспечения и (или) его компонентов.

Установка (инсталляция) в информационной системе программного обеспечения (вида, типа, класса программного обеспечения) и (или) его компонентов осуществляется с учетом перечня программного обеспечения и (или) его компонентов, разрешенных оператором к установке («белый список»), и (или) перечнем программного обеспечения и (или) его компонентов, запрещенных оператором к установке («черный список»). Указанные перечни программного обеспечения и (или) его компонентов разрабатываются оператором для информационной системы в целом или для всех ее сегментов или устройств в отдельности и фиксируются в организационно-распорядительной документации оператора по защите информации (документируются).

Установка (инсталляция) в информационной системе программного обеспечения и (или) его компонентов должна осуществляться только от имени администратора в соответствии с УПД.5.

Оператором должен обеспечиваться периодический контроль установленного (инсталлированного) в информационной системе программного обеспечения на предмет соответствия его перечню программного обеспечения, разрешенному к установке в информационной системе в соответствии с АНЗ.4, а также на предмет отсутствия программного обеспечения, запрещенного оператором к установке.

Требования к усилению ОПС.3:

Не установлены.

Содержание базовой меры ОПС.3:

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

ОПС.4 УПРАВЛЕНИЕ ВРЕМЕННЫМИ ФАЙЛАМИ, В ТОМ ЧИСЛЕ ЗАПРЕТ, РАЗРЕШЕНИЕ, ПЕРЕНАПРАВЛЕНИЕ ЗАПИСИ, УДАЛЕНИЕ ВРЕМЕННЫХ ФАЙЛОВ

Требования к реализации ОПС.4: В информационной системе должно осуществляться управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов.

Управление временными файлами должно обеспечивать перехват записи временной информации в файлы на системном (загрузочном) разделе машинного носителя информации средства вычислительной техники и ее перенаправление в оперативную память и (или) в другой раздел машинного носителя информации с последующей очисткой (стиранием).

Оператором должен быть определен и зафиксирован в организационно-распорядительной документации по защите информации (задокументирован) порядок очистки (стирания) временных файлов.

Требования к усилению ОПС.4:

1) в информационной системе должны осуществляться:

а) контроль доступа к временным файлам;

б) удаление временных файлов по завершении сеанса работы с ними.

Содержание базовой меры ОПС.4:

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

3.4. ЗАЩИТА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ (ЗНИ)

ЗНИ.1 УЧЕТ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

Требования к реализации ЗНИ.1: Оператором должен быть обеспечен учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации.

Учету подлежат:

съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

Учет съемных машинных носителей информации ведется в журналах учета машинных носителей информации.

Учет встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в журналах материально-технического учета в составе соответствующих технических средств. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

Регистрационные или иные номера подлежат занесению в журналы учета машинных носителей информации или журналы материально-технического учета с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации.

Раздельному учету в журналах учета подлежат съемные (в том числе портативные) перезаписываемые машинные носители информации (флэш-накопители, съемные жесткие диски).

Требования к усилению ЗНИ.1:

1) оператором обеспечивается маркировка машинных носителей информации (технических средств), дополнительно включающая:

а) информацию о возможности использования машинного носителя информации вне информационной системы;

б) информацию о возможности использования машинного носителя информации за пределами контролируемой зоны (конкретных помещений);

в) атрибуты безопасности, указывающие на возможность использования этих машинных носителей информации для обработки (хранения) соответствующих видов информации;

2) оператором обеспечивается маркировка машинных носителей информации (технических средств), дополнительно включающая неотторгаемую цифровую метку носителя информации для обеспечения возможности распознавания (идентификации) носителя в системах управления доступом;

3) оператором обеспечиваться маркировка машинных носителей информации (технических средств), дополнительно включающая использование механизмов распознавания (идентификации) носителя информации по его уникальным физическим характеристикам.

Содержание базовой меры ЗНИ.1:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗНИ.1	+	+	+	+
Усиление ЗНИ.1			1а	1а, 1б

ЗНИ.2 УПРАВЛЕНИЕ ДОСТУПОМ К МАШИННЫМ НОСИТЕЛЯМ ИНФОРМАЦИИ

Требования к реализации ЗНИ.2: Оператором должны быть реализованы следующие функции по управлению доступом к машинным носителям информации, используемым в информационной системе:

определение должностных лиц, имеющих физический доступ к машинным носителям информации, а именно к следующим:

съемным машинным носителям информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

портативным вычислительным устройствам, имеющим встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

машинным носителям информации, стационарно устанавливаемым в корпус средств вычислительной техники (например, накопители на жестких дисках);

предоставление физического доступа к машинным носителям информации только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций);

Правила и процедуры доступа к машинным носителям информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗНИ.2:

1) применение автоматизированной системы контроля физического доступа в помещения, в которых осуществляется хранение машинных носителей информации;

2) опечатывание корпуса средства вычислительной техники, в котором стационарно установлен машинный носитель информации;

3) в информационной системе должно обеспечиваться применение программных (программно-технических) автоматизированных средств управления физическим доступом к машинным носителям информации;

4) контроль физического доступа лиц к машинным носителям информации в соответствии с атрибутами безопасности, установленными для этих носителей.

Содержание базовой меры ЗНИ.2:

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

ЗНИ.3 КОНТРОЛЬ ПЕРЕМЕЩЕНИЯ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ ЗА ПРЕДЕЛЫ КОНТРОЛИРУЕМОЙ ЗОНЫ

Требования к реализации ЗНИ.3: Оператором должен обеспечиваться контроль перемещения используемых в информационной системе машинных носителей информации за пределы контролируемой зоны. При контроле перемещения машинных носителей информации должны осуществляться:

определение должностных лиц, имеющих права на перемещение машинных носителей информации за пределы контролируемой зоны;

предоставление права на перемещение машинных носителей информации за пределы контролируемой зоны только тем лицам, которым оно необходимо для выполнения своих должностных обязанностей (функции);

учет перемещаемых машинных носителей информации в соответствии с ЗНИ.1;

периодическая проверка наличия машинных носителей информации.

Правила и процедуры контроля перемещения машинных носителей информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗНИ.3:

1) оператором информационной системы определяются задачи (виды деятельности, функции), для решения которых необходимо перемещение машинных носителей информации за пределы контролируемой зоны;

2) применение в соответствии с законодательством Российской Федерации криптографических методов защиты информации, хранимой на носителе, при перемещении машинных носителей информации за пределы контролируемой зоны;

3) оператором определяется должностное лицо, ответственное за перемещение машинных носителей информации;

4) оператором информационной системы осуществляется периодическая проверка машинных носителей информации после их возврата в пределы контролируемой зоны.

Содержание базовой меры ЗНИ.3:

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

ЗНИ.4 ИСКЛЮЧЕНИЕ ВОЗМОЖНОСТИ НЕСАНКЦИОНИРОВАННОГО ОЗНАКОМЛЕНИЯ С СОДЕРЖАНИЕМ ИНФОРМАЦИИ, ХРАНЯЩЕЙСЯ НА МАШИННЫХ НОСИТЕЛЯХ, И (ИЛИ) ИСПОЛЬЗОВАНИЯ НОСИТЕЛЕЙ ИНФОРМАЦИИ В ИНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Требования к реализации ЗНИ.4: Оператором должно обеспечиваться исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах.

Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах должно предусматривать:

определение типов машинных носителей информации, подлежащих хранению в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище машинных носителей информации);

физический контроль и хранение машинных носителей информации в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище машинных носителей информации);

защита машинных носителей информации до уничтожения (стирания) с них данных и остаточной информации (информации, которую можно восстановить после удаления с помощью нештатных средств и методов) с использованием средств стирания данных и остаточной информации.

Правила и процедуры управления, направленные на исключение несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах, регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗНИ.4:

1) оператором должны применяться средства контроля съемных машинных носителей информации;

2) оператором должны применяться в соответствии с законодательством Российской Федерации криптографические методы защиты информации, хранящейся на машинных носителях;

3) оператором должен быть определен перечь машинных носителей информации, подлежащих хранению в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище машинных носителей информации).

Содержание базовой меры ЗНИ.4:

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

ЗНИ.5 КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ ИНТЕРФЕЙСОВ ВВОДА (ВЫВОДА)

Требования к реализации ЗНИ.5: В информационной системе должен осуществляться контроль использования интерфейсов ввода (вывода).

Контроль использования (разрешение или запрет) интерфейсов ввода (вывода) должен предусматривать:

определение оператором интерфейсов средств вычислительной техники, которые могут использоваться для ввода (вывода) информации, разрешенных и (или) запрещенных к использованию в информационной системе;

определение оператором категорий пользователей, которым предоставлен доступ к разрешенным к использованию интерфейсов ввода (вывода);

принятие мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода);

контроль доступа пользователей к разрешенным к использованию интерфейсов ввода (вывода).

В качестве мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода), могут применяться:

опечатывание интерфейсов ввода (вывода);

использование механических запирающих устройств;

удаление драйверов, обеспечивающих работу интерфейсов ввода (вывода);

применение средств защиты информации, обеспечивающих контроль использования интерфейсов ввода (вывода).

Правила и процедуры контроля использования интерфейсов ввода (вывода) регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗНИ.5:

1) в информационной системе должна быть обеспечена регистрация использования интерфейсов ввода (вывода) в соответствии с РСБ.3;

2) оператором обеспечивается конструктивное (физическое) исключение из средства вычислительной техники запрещенных к использованию интерфейсов ввода (вывода);

3) оператором информационной системы обеспечивается программное отключение запрещенных к использованию интерфейсов ввода (вывода).

Содержание базовой меры ЗНИ.5:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗНИ.5			+	+
Усиление ЗНИ.5				1

ЗНИ.6 КОНТРОЛЬ ВВОДА (ВЫВОДА) ИНФОРМАЦИИ НА МАШИННЫЕ НОСИТЕЛИ ИНФОРМАЦИИ

Требования к реализации ЗНИ.6: В информационной системе должен осуществляться контроль ввода (вывода) информации на машинные носители информации.

Контроль ввода (вывода) информации на машинные носители информации должен предусматривать:

определение оператором типов носителей информации, ввод (вывод) информации на которые подлежит контролю;

определение оператором категорий пользователей, которым предоставлены полномочия по вводу (выводу) информации на машинные носители в соответствии с УПД.2;

запрет действий по вводу (выводу) информации для пользователей, не имеющих полномочий на ввод (вывод) информации на машинные носители информации, и на носители информации, на которые запрещен ввод (вывод) информации;

регистрация действий пользователей и событий по вводу (выводу) информации на машинные носители информации в соответствии с РСБ.3.

Правила и процедуры контроля ввода (вывода) информации на машинные носители информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗНИ.6:

1) в информационной системе должна создаваться копия информации, записываемой пользователями на съемные машинные носители информации (теневое копирование);

2) оператором должны применяться средства контроля подключения съемных машинных носителей информации.

Содержание базовой меры ЗНИ.6:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗНИ.6				
Усиление ЗНИ.6				

ЗНИ.7 КОНТРОЛЬ ПОДКЛЮЧЕНИЯ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

Требования к реализации ЗНИ.7: В информационной системе должен обеспечиваться контроль подключения машинных носителей информации.

Контроль подключения машинных носителей информации должен предусматривать:

определение оператором типов носителей информации, подключение которых к информационной системе разрешено в соответствии с УПД.2;

определение оператором категорий пользователей, которым предоставлены полномочия по подключению носителей к информационной системе в соответствии с УПД.2;

запрет подключения носителей информации, подключение которых к информационной системе не разрешено;

регистрация действий пользователей и событий по подключению к информационной системе носителей в соответствии с РСБ.3.

Правила и процедуры контроля подключения машинных носителей информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗНИ.7:

1) оператором должен обеспечиваться контроль подключения машинных носителей информации с использованием средств контроля подключения съемных машинных носителей информации, позволяющих устанавливать разрешенные и (или) запрещенные типы и (или) конкретные съемные машинные носители информации для различных категорий пользователей;

2) запрет подключения к информационной системе носителей пользователями, не имеющими полномочий на подключение носителей.

Содержание базовой меры ЗНИ.7:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗНИ.7				
Усиление ЗНИ.7				

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)

Требования к реализации ЗНИ.8: Оператором должно обеспечиваться уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации.

Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации.

Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации.

Процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации должны быть разработаны оператором и включены в организационно-распорядительные документы по защите информации.

Требования к усилению ЗНИ.8:

1) оператором должны быть обеспечены регистрация и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации;

2) оператором должны проводиться периодическая проверка процедур и тестирование средств стирания информации и контроля удаления информации;

3) оператором перед подключением к информационной системе должно быть обеспечено уничтожение (стирание) информации с носителей информации после их приобретения и при первичном подключении к информационной системе, при использовании в иных информационных системах, при передаче для постоянного использования от одного пользователя другому пользователю, после возвращения из ремонта, а также в иных случаях, определяемых оператором;

4) оператором должно быть обеспечено уничтожение машинных носителей информации, которые не подлежат очистке (неперезаписываемые машинные носители информации, такие как оптические диски типа CD-R);

5) оператором должны применяться следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации:

а) удаление файлов штатными средствами операционной системы и (или) форматирование машинного носителя информации штатными средствами операционной системы;

б) перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаление записи о файлах, обнуление журнала файловой системы или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием;

в) очистка всего физического пространства машинного носителя информации, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя;

г) полная многократная перезапись машинного носителя информации специальными битовыми последовательностями, зависящими от типа накопителя и используемого метода кодирования информации, затем очистка всего физического пространства накопителя, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя;

д) размагничивание машинного носителя информации;

е) физическое уничтожение машинного носителя информации (в том числе сжигание, измельчение, плавление, расщепление, распыление и другое).

Содержание базовой меры ЗНИ.8:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗНИ.8	+	+	+	+
Усиление ЗНИ.8	5а	1, 5б	1, 5в	1, 2, 3, 5г

3.5. РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ (РСБ)

3.5.1. РСБ.1 ОПРЕДЕЛЕНИЕ СОБЫТИЙ БЕЗОПАСНОСТИ, ПОДЛЕЖАЩИХ РЕГИСТРАЦИИ, И СРОКОВ ИХ ХРАНЕНИЯ

Требования к реализации РСБ.1: Оператором должны быть определены события безопасности в информационной системе, подлежащие регистрации, и сроки их хранения.

События безопасности, подлежащие регистрации в информационной системе, должны определяться с учетом способов реализации угроз безопасности для информационной системы. К событиям безопасности, подлежащим регистрации в информационной системе, должны быть отнесены любые проявления состояния информационной системы и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов информационной системы, нарушения процедур, установленных организационно-распорядительными документами по защите информации оператора, а также на нарушение штатного функционирования средств защиты информации.

События безопасности, подлежащие регистрации в информационной системе, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в информационной системе. Подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации в информационной системе.

Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется оператором исходя из возможностей реализации угроз безопасности информации и фиксируется в организационно-распорядительных документах по защите информации (документируется).

В информационной системе как минимум подлежат регистрации следующие события:

вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы;

подключение машинных носителей информации и вывод информации на носители информации;

запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;

попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;

попытки удаленного доступа.

Состав и содержание информации о событиях безопасности, подлежащих регистрации, определяются в соответствии с РСБ.2.

Требования к усилению РСБ.1:

1) оператором должен обеспечиваться пересмотр перечня событий безопасности, подлежащих регистрации, не менее чем один раз в год, а также по результатам контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

2) оператором в перечень событий безопасности, подлежащих регистрации, должны быть включены события, связанные с действиями от имени привилегированных учетных записей (администраторов);

3) оператором в перечень событий безопасности, подлежащих регистрации, должны быть включены события, связанные с изменением привилегий учетных записей;

4) оператором должен быть обеспечен срок хранения информации о зарегистрированных событиях безопасности не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации, при этом:

а) осуществляется хранение только записей о выявленных событиях безопасности;

б) осуществляется хранение записей о выявленных событиях безопасности и записей системных журналов, которые послужили основанием для регистрации события безопасности;

в) осуществляется хранение журналов приложений, которые послужили основанием для регистрации события безопасности;

г) осуществляется хранение всех записей системных журналов и событий безопасности;

д) осуществляется хранение всех записей журналов приложений.

Содержание базовой меры РСБ.1:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
РСБ.1	+	+	+	+
Усиление РСБ.1			1,3, 4а	1, 2, 3, 4б

РСБ.2 ОПРЕДЕЛЕНИЕ СОСТАВА И СОДЕРЖАНИЯ ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ, ПОДЛЕЖАЩИХ РЕГИСТРАЦИИ

Требования к реализации РСБ.2: В информационной системе должны быть определены состав и содержание информации о событиях безопасности, подлежащих регистрации.

Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и

времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

При регистрации входа (выхода) субъектов доступа в информационную систему и загрузки (останова) операционной системы состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

При регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

При регистрации попыток удаленного доступа к информационной системе состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

Состав и содержание информации о событиях безопасности, подлежащих регистрации, отражаются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению РСБ.2:

1) в информационной системе обеспечивается запись дополнительной информации о событиях безопасности, включающую:

а) полнотекстовую запись привилегированных команд (команд, управляющих системными функциями);

б) запись сетевых потоков (дампов), связанных с событием безопасности;

2) в информационной системе обеспечивается централизованное управление записями регистрации событий безопасности в рамках сегментов информационной системы, определяемых оператором, и (или) информационной системы в целом;

3) в информационной системе обеспечивается индивидуальная регистрация пользователей групповых учетных записей*;

4) в информационной системе обеспечивается регистрация информации о месте (в частности сетевой адрес, географическая привязка и (или) другая информация), с которого осуществляется вход субъектов доступа в информационную систему;

5) в информационной системе состав и содержание регистрационных записей при регистрации запуска процессов (приложений) должны включать следующие сведения:

а) параметров запуска процесса (приложения);

б) продолжительность работы;

в) объекты доступа, к которым осуществлялось обращение процесса (приложения);

г) использованные процессом (приложением) устройства;

6) в информационной системе обеспечивается запись следующей информации, связанной с доступом к объектам доступа (в частности к файлам):

а) тип доступа (в том числе чтение, исполнение, запись и (или) иные типы);

б) изменение атрибутов объектов доступа(права доступа, контрольные суммы, размер, содержание, путь, тип и (или) иные атрибуты);

в) продолжительность доступа.

Содержание базовой меры РСБ.2:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
РСБ.2	+	+	+	+
Усиление РСБ.2			1а	1а

* Локальные и доменные группы пользователей.

РСБ.3 СБОР, ЗАПИСЬ И ХРАНЕНИЕ ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ В ТЕЧЕНИЕ УСТАНОВЛЕННОГО ВРЕМЕНИ ХРАНЕНИЯ

Требования к реализации РСБ.3: В информационной системе должны осуществляться сбор, запись и хранение информации о событиях безопасности в течение установленного оператором времени хранения информации о событиях безопасности.

Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать:

возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности определенных в соответствии с РСБ.1;

генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с РСБ.1 с составом и содержанием информации, определенными в соответствии с РСБ.2;

хранение информации о событиях безопасности в течение времени, установленного в соответствии с РСБ.1.

Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с РСБ.1, составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с РСБ.2, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности в соответствии с РСБ.1.

Правила и процедуры сбора, записи и хранения информации о событиях безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению РСБ.3:

1) в информационной системе должно быть обеспечено централизованное автоматизированное управление сбором, записью и хранением информации о событиях безопасности;

2) в информационной системе обеспечивается объединение информации из записей регистрации событий безопасности, полученной от разных технических средств (устройств), программного обеспечения информационной системы, в единый логический или физический журнал аудита с корреляцией информации по времени для своевременного выявления инцидентов и реагирования на них;

3) в информационной системе обеспечивается объединение информации из записей регистрации событий безопасности, полученной от разных технических средств (устройств), программного обеспечения информационной системы, в единый логический или физический журнал аудита с корреляцией информации по событиям безопасности для своевременного выявления инцидентов и реагирования на них в масштабах оператора;

4) в информационной системе обеспечивается хранение записей системных журналов и записей о событиях безопасности в обособленном хранилище, физически отделенном от технических средств, входящих в состав информационной системы.

Содержание базовой меры РСБ.3:

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

Требования к реализации РСБ.4: В информационной системе должно осуществляться 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.

Реагирование на сбои при регистрации событий безопасности должно предусматривать:

предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;

реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационной системы, запись поверх устаревших хранимых записей событий безопасности.

Правила и процедуры реагирования на сбои при регистрации событий безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению РСБ.4:

1) в информационной системе обеспечивается выдача предупреждения администратору при заполнении установленной оператором части (процент или фактическое значение) объема памяти для хранения информации о событиях безопасности.

2) в информационной системе обеспечивается выдача предупреждения администратору в масштабе времени, близком к реальному, при наступлении критичных сбоев в механизмах сбора информации, определенных оператором;

3) в информационной системе обеспечивается запрет обработки информации в случае аппаратных или программных ошибок, сбоев в механизмах сбора информации или достижения предела или переполнения объема (емкости) памяти.

Содержание базовой меры РСБ.4:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
РСБ.4	+	+	+	+
Усиление РСБ.4				1а, 2

РСБ.5 МОНИТОРИНГ (ПРОСМОТР, АНАЛИЗ) РЕЗУЛЬТАТОВ РЕГИСТРАЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ И РЕАГИРОВАНИЕ НА НИХ

Требования к реализации РСБ.5: Оператором должен осуществляться мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться для всех событий, подлежащих регистрации в соответствии с РСБ.1, и с периодичностью, установленной оператором, и обеспечивающей своевременное выявление признаков инцидентов безопасности в информационной системе.

В случае выявление признаков инцидентов безопасности в информационной системе осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

Правила и процедуры мониторинга результатов регистрации событий безопасности и реагирования на них регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению РСБ.5:

1) в информационной системе должны обеспечиваться интеграция результатов мониторинга (просмотра и анализа) записей регистрации (аудита) из разных источников (журналов, хранилищ информации о событиях безопасности) и их корреляция с целью выявления инцидентов безопасности и реагирования на них;

2) в информационной системе обеспечивается интеграция процессов мониторинга (просмотра, анализа) результатов регистрации событий безопасности с результатами анализа уязвимостей, проводимого в соответствии

с АНЗ.1, и результатами обнаружения вторжений, проводимого в соответствии с СОВ.1 с целью усиления возможностей по выявлению признаков инцидентов безопасности;

3) в информационной системе обеспечивается полнотекстовый анализ привилегированных команд;

4) оператором обеспечивается анализ записанных сетевых потоков (дампов).

Содержание базовой меры РСБ.5:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
РСБ.5	+	+	+	+
Усиление РСБ.5				1

РСБ.6 ГЕНЕРИРОВАНИЕ ВРЕМЕННЫХ МЕТОК И (ИЛИ) СИНХРОНИЗАЦИЯ СИСТЕМНОГО ВРЕМЕНИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Требования к реализации РСБ.6: В информационной системе должно осуществляться генерирование надежных меток времени и (или) синхронизация системного времени.

Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в информационной системе достигается посредством применения внутренних системных часов информационной системы.

Требования к усилению РСБ.6:

1) оператором информационной системы должен быть определен источник надежных меток времени; в информационной системе должна выполняться синхронизация системного времени с периодичностью, определенной оператором.

Содержание базовой меры РСБ.6:

Меры защиты информации	Класс защищенности информационной системы			
	4	3	2	1
РСБ.6	+	+	+	+
Усиление РСБ.6				1

РСБ.7 ЗАЩИТА ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ

Требования к реализации РСБ.7: В информационной системе должна обеспечиваться защита информации о событиях безопасности.

Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в соответствии с настоящим методическим документом, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам.

Правила и процедуры защиты информации о событиях безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению РСБ.7:

1) в информационной системе обеспечивается резервное копирование записей регистрации (аудита);

2) в информационной системе обеспечивается резервное копирование записей регистрации (аудита) на носители однократной записи (неперезаписываемые носители информации);

3) в информационной системе для обеспечения целостности информации о зарегистрированных событиях безопасности должны применяться в соответствии с законодательством Российской Федерации криптографические методы;

4) оператор предоставляет доступ к записям регистрации событий безопасности (аудита) ограниченному кругу администраторов.

Содержание базовой меры РСБ.7:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
РСБ.7	+	+	+	+
Усиление РСБ.7			1	1

РСБ.8 ОБЕСПЕЧЕНИЕ ВОЗМОЖНОСТИ ПРОСМОТРА И АНАЛИЗА ИНФОРМАЦИИ О ДЕЙСТВИЯХ ОТДЕЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Требования к реализации РСБ.8: В информационной системе должна иметься возможность просмотра и анализа информации о действиях отдельных пользователей в информационной системе.

Сведения о действиях отдельных пользователей в информационной системе должны предоставляться уполномоченным должностным лицам для просмотра и анализа с целью расследования причин возникновения инцидентов в информационной системе в соответствии с законодательством Российской Федерации.

Правила и процедуры просмотра и анализа информации о действиях отдельных пользователей регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению РСБ.8:

1) в информационной системе должна быть обеспечена возможность автоматизированной обработки записей регистрации (аудита) событий безопасности на основе критериев избирательности.

Содержание базовой меры РСБ.8:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
РСБ.8				
Усиление РСБ.8				

3.6. АНТИВИРУСНАЯ ЗАЩИТА (АВЗ)

АВЗ.1 РЕАЛИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ

Требования к реализации АВЗ.1: Оператором должна обеспечиваться антивирусная защита информационной системы, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Реализация антивирусной защиты должна предусматривать:

применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), мобильных технических средствах и иных точках доступа в информационную систему, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы);

установку, конфигурирование и управление средствами антивирусной защиты;

предоставление доступа средствам антивирусной защиты к объектам информационной системы, которые должны быть подвергнуты проверке средством антивирусной защиты;

проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов);

проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов;

оповещение администраторов безопасности в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов);

определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).

Правила и процедуры антивирусной защиты информационной системы регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению АВЗ.1:

1) в информационной системе должно обеспечиваться предоставление прав по управлению (администрированию) средствами антивирусной защиты администратору безопасности;

2) в информационной системе должно обеспечиваться централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий программного обеспечения средств антивирусной защиты) средствами антивирусной защиты, установленными на компонентах информационной системы (серверах, автоматизированных рабочих местах);

3) оператором должен обеспечиваться запрет использования съемных машинных носителей информации, которые могут являться источниками вредоносных компьютерных программ (вирусов);

4) в информационной системе должно обеспечиваться использование на разных уровнях информационной системы средств антивирусной защиты разных производителей;

5) в информационной системе должны обеспечиваться проверка работоспособности, актуальность базы данных признаков компьютерных вирусов и версии программного обеспечения средств антивирусной защиты;

6) в информационной системе должна обеспечиваться проверка объектов файловой системы средством антивирусной защиты до загрузки операционной системы;

7) в информационной системе должна обеспечиваться регистрация событий о неуспешном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);

8) оператором должна обеспечиваться антивирусная защита на этапе инициализации микропрограммного обеспечения средства вычислительной техники.

Содержание базовой меры АВЗ.1:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
АВЗ.1	+	+	+	+
Усиление АВЗ.1		1	1, 2	1, 2

АВЗ.2 ОБНОВЛЕНИЕ БАЗЫ ДАННЫХ ПРИЗНАКОВ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ (ВИРУСОВ)

Требования к реализации АВЗ.2: Оператором должно быть обеспечено обновление базы данных признаков вредоносных компьютерных программ (вирусов).

Обновление базы данных признаков вредоносных компьютерных программ (вирусов) должно предусматривать:

получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);

получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов);

контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

Правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов) регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению АВЗ.2:

1) в информационной системе должно обеспечиваться централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов);

2) в информационной системе должно обеспечиваться автоматическое обновление базы данных признаков вредоносных компьютерных программ (вирусов) на всех компонентах информационной системы;

3) в информационной системе должен обеспечиваться запрет изменений настроек системы обновления базы данных признаков вредоносных компьютерных программ (вирусов) на автоматизированных рабочих местах и серверах;

4) в информационной системе должна обеспечиваться возможность возврата (отката) к предыдущим обновлениям базы данных признаков вредоносных компьютерных программ (вирусов).

Содержание базовой меры АВЗ.2:

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

3.7. ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ (СОВ)

СОВ.1 ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ

Требования к реализации СОВ.1: Оператором должно обеспечиваться обнаружение (предотвращение) вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней, с использованием систем обнаружения вторжений.

Применяемые системы обнаружения вторжений должны включать компоненты регистрации событий безопасности (датчики), компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы) и базу решающих правил, содержащую информацию о характерных признаках компьютерных атак.

Обнаружение (предотвращение) вторжений должно осуществляться на внешней границе информационной системы (системы обнаружения вторжений уровня сети) и (или) на внутренних узлах (системы обнаружения вторжений уровня узла) сегментов информационной системы (автоматизированных рабочих местах, серверах и иных узлах), определяемых оператором.

Права по управлению (администрированию) системами обнаружения вторжений должны предоставляться только уполномоченным должностным лицам.

Системы обнаружения вторжений должны обеспечивать реагирование на обнаруженные и распознанные компьютерные атаки с учетом особенностей функционирования информационных систем.

Правила и процедуры обнаружения (предотвращения) вторжений (компьютерных атак) регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению СОВ.1:

1) оператором обеспечивается применение систем обнаружения вторжений уровня сети, обеспечивающих сбор и анализ информации об информационных потоках, передаваемых в рамках сегмента (сегментов) информационной системы;

2) в информационной системе обеспечивается централизованное управление (администрирование) компонентами системы обнаружения вторжений, установленными в различных сегментах информационной системы;

3) обнаружение и реагирование (уведомление администратора безопасности, блокирование трафика и иные действия по реагированию) на компьютерные атаки в масштабе времени, близком к реальному;

4) защита информации, собранной и сгенерированной системой обнаружения вторжений, от несанкционированного доступа, модификации и удаления;

5) оператором информационной системы обеспечивается применение систем обнаружения вторжений уровня узла на автоматизированных рабочих местах и серверах информационной системы;

6) оператором информационной системы обеспечивается применение систем обнаружения вторжений на прикладном уровне базовой эталонной модели взаимосвязи открытых систем.

Содержание базовой меры СОВ.1:

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

СОВ.2 ОБНОВЛЕНИЕ БАЗЫ РЕШАЮЩИХ ПРАВИЛ

Требования к реализации СОВ.2: Оператором должно обеспечиваться обновление базы решающих правил системы обнаружения вторжений, применяемой в информационной системе.

Обновление базы решающих правил системы обнаружения вторжений должно предусматривать:

получение уведомлений о необходимости обновлений и непосредственном обновлении базы решающих правил;

получение из доверенных источников и установку обновлений базы решающих правил;

контроль целостности обновлений базы решающих правил.

Правила и процедуры обновления базы решающих правил регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению СОВ.2:

1) в информационной системе должно обеспечиваться централизованное управление обновлением базы решающих правил системы обнаружения вторжений;

2) в информационной системе должна обеспечиваться возможность редактирования базы решающих правил (добавление и (или) исключение решающих правил) со стороны уполномоченных должностных лиц (администраторов) для предотвращения определенных оператором компьютерных атак и (или) сокращения нагрузки на информационную систему, а также минимизации ложных срабатываний системы обнаружения вторжений;

3) оператором информационной системы устанавливается порядок редактирования базы решающих правил. В случае редактирования базы

решающих правил запись об этом событии с указанием произведенных изменений фиксируется в соответствующем журнале регистрации событий безопасности.

Содержание базовой меры СОВ.2:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
СОВ.2			+	+
Усиление СОВ.2				1, 2, 3

3.8. КОНТРОЛЬ (АНАЛИЗ) ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ (АНЗ)

АНЗ.1 ВЫЯВЛЕНИЕ, АНАЛИЗ И УСТРАНЕНИЕ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Требования к реализации АНЗ.1: Оператором должны осуществляться выявление (поиск), анализ и устранение уязвимостей в информационной системе.

При выявлении (поиске), анализе и устранении уязвимостей в информационной системе должны проводиться:

выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;

разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;

анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;

устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;

информирование должностных лиц оператора (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей.

Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации информационной системы. На этапе эксплуатации поиск и анализ уязвимостей проводится с периодичностью, установленной оператором. При этом в обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в информационной системе.

В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических

средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

Оператором должны осуществляться получение из доверенных источников и установка обновлений базы признаков уязвимостей.

Правила и процедуры выявления, анализа и устранения уязвимостей регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению АН3.1:

1) оператором обеспечивается использование для выявления (поиска) уязвимостей средств анализа (контроля) защищенности (сканеров безопасности), имеющих стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования информационной системы на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей;

2) оператор должен уточнять перечень сканируемых в информационной системе уязвимостей с установленной им периодичностью, а также после появления информации о новых уязвимостях;

3) оператором определяется информация об информационной системе, которая может стать известной нарушителям и использована ими для эксплуатации уязвимостей (в том числе уязвимостей «нулевого дня» - уязвимостей, описание которых отсутствует в базах данных разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств), и принимаются меры по снижению (исключению) последствий от эксплуатации нарушителями неустранимых уязвимостей;

4) оператором предоставляется доступ только администраторам к функциям выявления (поиска) уязвимостей (предоставление такой возможности только администраторам безопасности);

5) оператором применяются автоматизированные средства для сравнения результатов сканирования уязвимостей в разные периоды времени для анализа изменения количества и классов (типов) уязвимостей в информационной системе;

6) оператором применяются автоматизированные средства для обнаружения в информационной системе неразрешенного программного обеспечения (компонентов программного обеспечения) и уведомления об этом уполномоченных должностных лиц (администратора безопасности);

7) оператором проводится анализ журналов регистрации событий безопасности (журнала аудита) в целях определения, были ли выявленные

уязвимости ранее использованы в информационной системе для нарушения безопасности информации;

8) оператором обеспечивается проведение выявления уязвимостей «нулевого дня», о которых стало известно, но информация о которых не включена в сканеры уязвимостей;

9) оператором обеспечивается проведение выявления новых уязвимостей, информация о которых не опубликована в общедоступных источниках;

10) оператором должно осуществляться выявление (поиск) уязвимостей в информационной системе с использованием учетных записей на сканируемых ресурсах;

11) оператором должно использоваться тестирование информационной системы на проникновение.

Содержание базовой меры АНЗ.1:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
АНЗ.1		+	+	+
Усиление АНЗ.1		1, 4	1, 2,4	1, 2, 4, 7

АНЗ.2 КОНТРОЛЬ УСТАНОВКИ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ВКЛЮЧАЯ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Требования к реализации АНЗ.2: Оператором должен осуществляться контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

Оператором должно осуществляться получение из доверенных источников и установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в информационной системе и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

Контроль установки обновлений проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации и фиксируется в соответствующих журналах.

При контроле установки обновлений осуществляются проверки установки обновлений баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты в соответствии с АВЗ.2, баз решающих правил систем обнаружения вторжений в соответствии с СОВ.2, баз признаков уязвимостей средств анализа защищенности и иных баз данных, необходимых для реализации функций безопасности средств защиты информации.

Правила и процедуры контроля установки обновлений программного обеспечения регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению АНЗ.2:

1) оператором должна осуществляться проверка корректности функционирования обновлений в тестовой среде с обязательным оформлением результатов проверки в соответствующем журнале;

2) оператором обеспечивается регламентация и контроль обновлений программного обеспечения базовой системы ввода-вывода (иного микропрограммного обеспечения).

Содержание базовой меры АНЗ.2:

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

АНЗ.3 КОНТРОЛЬ РАБОТОСПОСОБНОСТИ, ПАРАМЕТРОВ НАСТРОЙКИ И ПРАВИЛЬНОСТИ ФУНКЦИОНИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Требования к реализации АНЗ.3: Оператором должен проводиться контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.

При контроле работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации осуществляется:

контроль работоспособности (неотключения) программного обеспечения и средств защиты информации;

проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации, объем и содержание которой определяется оператором;

контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;

восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.

Требования к усилению АНЗ.3:

1) в информационной системе должны обеспечиваться регистрация событий и оповещение (сигнализация, индикация) администратора безопасности о событиях, связанных с нарушением работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации;

2) оператором в случае обнаружения нарушений работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации должен обеспечиваться перевод информационной системы, сегмента или компонента информационной системы в режим ограничения обработки информации и (или) запрет обработки информации в информационной системе, сегменте или компоненте информационной системы до устранения нарушений;

3) оператором должны использоваться автоматизированные средства, обеспечивающие инвентаризацию параметров настройки программного обеспечения и средств защиты информации и восстановление параметров настройки программного обеспечения и средств защиты информации;

4) в информационной системе должно использоваться программное обеспечение, прошедшее контроль отсутствия недекларированных возможностей и отсутствия влияния на корректность работы средств защиты информации.

Содержание базовой меры АНЗ.3:

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

АНЗ.4 КОНТРОЛЬ СОСТАВА ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Требования к реализации АНЗ.4: Оператором должен проводиться контроль состава технических средств, программного обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация).

При контроле состава технических средств, программного обеспечения и средств защиты информации осуществляется:

контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации информационной системы и принятие мер, направленных на устранение выявленных недостатков;

контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;

контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

Контроль состава технических средств, программного обеспечения и средств защиты информации проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.

Требования к усилению АНЗ.4:

1) в информационной системе должна обеспечиваться регистрация событий безопасности, связанных с изменением состава технических средств, программного обеспечения и средств защиты информации;

2) оператором должны использоваться автоматизированные средства, обеспечивающие инвентаризацию технических средств, программного обеспечения и средств защиты информации.

Содержание базовой меры АНЗ.4:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
АНЗ.4		+	+	+
Усиление АНЗ.4			1	1, 2

АН3.5 КОНТРОЛЬ ПРАВИЛ ГЕНЕРАЦИИ И СМЕНЫ ПАРОЛЕЙ ПОЛЬЗОВАТЕЛЕЙ, ЗАВЕДЕНИЯ И УДАЛЕНИЯ УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ, РЕАЛИЗАЦИИ ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПОМ, ПОЛНОМОЧИЙ ПОЛЬЗОВАТЕЛЕЙ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Требования к реализации АН3.5: Оператором должен проводиться контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе.

При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе осуществляется:

контроль правил генерации и смены паролей пользователей в соответствии с ИАФ.1 и ИАФ.4;

контроль заведения и удаления учетных записей пользователей в соответствии с УПД.1;

контроль реализации правил разграничения доступом в соответствии с УПД.2;

контроль реализации полномочий пользователей в соответствии с УПД.4 и УПД.5;

контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей, предусмотренных организационно-распорядительными документами по защите информации оператора;

устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.

Требования к усилению АН3.5:

1) в информационной системе должна обеспечиваться регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступом и полномочий пользователей;

2) оператором должны использоваться автоматизированные средства, обеспечивающие контроль правил генерации и смены паролей пользователей,

учетных записей пользователей, правил разграничения доступом и полномочий пользователей.

Содержание базовой меры АНЗ.5:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
АНЗ.5		+	+	+
Усиление АНЗ.5			1	1

3.9. ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ И ИНФОРМАЦИИ (ОЦЛ)

ОЦЛ.1 КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ВКЛЮЧАЯ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Требования к реализации ОЦЛ.1: В информационной системе должен осуществляться контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.

Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации, должен предусматривать:

контроль целостности программного обеспечения средств защиты информации, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов средств защиты информации в процессе загрузки и (или) динамически в процессе работы информационной системы;

контроль целостности компонентов программного обеспечения (за исключением средств защиты информации), определяемого оператором исходя из возможности реализации угроз безопасности информации, по наличию имен (идентификаторов) компонентов программного обеспечения и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы информационной системы;

контроль применения средств разработки и отладки программ в составе программного обеспечения информационной системы;

тестирование с периодичностью установленной оператором функций безопасности средств защиты информации, в том числе с помощью тест-программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств, в соответствии с АНЗ.1 и АНЗ.2;

обеспечение физической защиты технических средств информационной системы в соответствии с ЗТС.2 и ЗТС.3.

В случае если функциональные возможности информационной системы должны предусматривать применение в составе ее программного обеспечения средств разработки и отладки программ, оператором обеспечивается выполнение процедур контроля целостности программного обеспечения после завершения каждого процесса функционирования средств разработки и отладки программ.

Правила и процедуры контроля целостности программного обеспечения регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОЦЛ.1:

1) в информационной системе контроль целостности средств защиты информации должен осуществляться по контрольным суммам всех

компонентов средств защиты информации, как в процессе загрузки, так и динамически в процессе работы системы;

2) в информационной системе должен обеспечиваться контроль целостности средств защиты информации с использованием криптографических методов в соответствии с законодательством Российской Федерации, всех компонентов средств защиты информации, как в процессе загрузки, так и динамически в процессе работы системы;

3) оператором исключается возможность использования средств разработки и отладки программ во время обработки и (или) хранения информации в целях обеспечения целостности программной среды;

4) оператором обеспечивается выделение рабочих мест с установленными средствами разработки и отладки программ в отдельный сегмент (тестовую среду);

5) в информационной системе должна обеспечиваться блокировка запуска программного обеспечения и (или) блокировка сегмента (компонента) информационной системы (автоматизированного рабочего места, сервера) в случае обнаружения фактов нарушения целостности.

Содержание базовой меры ОЦЛ.1:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ОЦЛ.1			+	+
Усиление ОЦЛ.1			1,3	1,3

ОЦЛ.2 КОНТРОЛЬ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В БАЗАХ ДАННЫХ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Требования к реализации ОЦЛ.2: В информационной системе должен осуществляться контроль целостности информации, содержащейся в базах данных информационной системы.

Контроль целостности информации, содержащейся в базах данных информационной системы, должен предусматривать:

контроль целостности с периодичностью, установленной оператором, структуры базы данных по наличию имен (идентификаторов) и (или) по контрольным суммам программных компонент базы данных в процессе загрузки и (или) динамически в процессе работы информационной системы;

контроль целостности с периодичностью, установленной оператором, объектов баз данных, определяемых оператором, по контрольным суммам и (или) с использованием криптографических методов в соответствии с законодательством Российской Федерации в процессе загрузки и (или) динамически в процессе работы информационной системы;

обеспечение физической защиты технических средств информационной системы, на которых установлена база данных, в соответствии с ЗТС.2 и ЗТС.3.

Правила и процедуры контроля целостности информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОЦЛ.2:

1) в информационной системе должны выполняться процедуры контроля целостности информации, содержащейся в базе данных, перед каждым запуском программного обеспечения доступа к базе данных;

2) в информационной системе должен обеспечиваться контроль целостности исполняемых модулей, хранящихся в базах данных (например, хранимые процедуры, триггеры);

3) в информационной системе должна обеспечиваться блокировка запуска системы управления базы данных и (или) блокировка сегмента (компонента) информационной системы (автоматизированного рабочего места, сервера) в случае обнаружения фактов нарушения целостности;

4) контроль целостности структуры базы данных и контроль целостности информации, хранящейся в базе данных, с применением специальных программных автоматизированных средств контроля целостности.

Содержание базовой меры ОЦЛ.2:

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

ОЦЛ.3 ОБЕСПЕЧЕНИЕ ВОЗМОЖНОСТИ ВОССТАНОВЛЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ВКЛЮЧАЯ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, ПРИ ВОЗНИКНОВЕНИИ НЕШТАТНЫХ СИТУАЦИЙ

Требования к реализации ОЦЛ.3: Оператором должна быть предусмотрена возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

Для обеспечения возможности восстановления программного обеспечения в информационной системе должны быть приняты соответствующие планы по действиям персонала (администраторов безопасности, пользователей) при возникновении нештатных ситуаций.

Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций должна предусматривать:

восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;

восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации;

возврат информационной системы в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей информационной системы, определенных оператором, позволяющих решать задачи по обработке информации.

Оператором применяются компенсирующие меры защиты информации в случаях, когда восстановление работоспособности системы защиты информации невозможно.

Правила и процедуры восстановления (в том числе планы по действиям персонала порядок применения компенсирующих мер) отражаются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОЦЛ.3:

1) оператором обеспечивается восстановление отдельных функциональных возможностей информационной системы с применением резервированного программного обеспечения зеркальной информационной системы (сегмента информационной системы, технического средства, устройства) в соответствии с ОДТ.2 и ОДТ.4.

Содержание базовой меры ОЦЛ.3:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ОЦЛ.3	+	+	+	+
Усиление ОЦЛ.3				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)

Требования к реализации ОЦЛ.4: Оператором должно обеспечиваться обнаружение и реагирование на поступление незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама).

Защита от спама реализуется на точках входа в информационную систему (выхода) информационных потоков (межсетевые экраны, почтовые серверы, Web-серверы, прокси-серверы и серверы удаленного доступа), а также на автоматизированных рабочих местах, серверах и (или) мобильных технических средствах, подключенных к сетям связи общего пользования, для обнаружения и реагирования на поступление по электронной почте незапрашиваемых электронных сообщений (писем, документов) или в приложениях к электронным письмам.

Защита от спама обеспечивается применением специализированных средств защиты, реализующих следующие механизмы защиты:

фильтрация по содержимому электронных сообщений (писем, документов) с использованием критериев, позволяющих относить сообщения к спаму сигнатурным и (или) эвристическим методами;

фильтрация на основе информации об отправителе электронного сообщения (в том числе с использованием «черных» списков(запрещенные отправители) и (или) «белых» списков (разрешенные отправители).

Оператором должно осуществляться обновление базы «черных» («белых») списков и контроль целостности базы «черных» («белых») списков.

Правила и процедуры обнаружения и реагирования на поступление незапрашиваемой информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОЦЛ.4:

1) оператором обеспечивается централизованное управление средствами защиты от спама;

2) в информационной системе должна обеспечиваться фильтрация на основе информации об отправителе электронного сообщения с использованием эвристических методов (например, «серые» списки серверов электронной почты, распознавание автоматически генерируемых имен отправителей и другие);

3) в информационной системе должна обеспечиваться аутентификация отправителей электронных сообщений в соответствии с ИАФ.1, ИАФ.6, ИАФ.7;

4) в информационной системе должна обеспечиваться аутентификация серверов электронной почты(в том числе в соответствии с ИАФ.2, ИАФ.7);

5) в информационной системе должен обеспечиваться контроль поступления в информационную систему информационных сообщений и документов на основе контентного анализа.

Содержание базовой меры ОЦЛ.4:

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

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

Требования к реализации ОЦЛ.5: В информационной системе должен осуществляться 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.

Контроль содержания информации, передаваемой из информационной системы, должен предусматривать:

выявление фактов неправомерной передачи защищаемой информации из информационной системы через различные типы сетевых соединений, включая сети связи общего пользования и реагирование на них;

выявление фактов неправомерной записи защищаемой информации на неучтенные съемные машинные носители информации и реагирование на них;

выявление фактов неправомерного вывода на печать документов, содержащих защищаемую информацию и реагирование на них;

выявление фактов неправомерного копирования защищаемой информации в прикладное программное обеспечение из буфера обмена и реагирование на них;

контроль хранения защищаемой информации на серверах и автоматизированных рабочих местах;

выявление фактов хранения информации на общих сетевых ресурсах (общие папки, системы документооборота, базы данных, почтовые архивы и иные ресурсы).

Контроль содержания информации, передаваемой из информационной системы, осуществляется по цифровым отпечаткам информации, по регулярным выражениям и (или) по атрибутам безопасности (меткам безопасности) файлов, а также с помощью иных методов.

Правила и процедуры контроля содержания передаваемой информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОЦЛ.5:

1) в информационной системе должно осуществляться хранение всей передаваемой из информационной системы информации и (или) информации с недопустимым к передаче из информационной системы содержанием, в течение времени, определяемого оператором;

2) в информационной системе должна осуществляться блокировка передачи из информационной системы информации с недопустимым содержанием.

Содержание базовой меры ОЦЛ.5:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ОЦЛ.5				
Усиление ОЦЛ.5				

ОЦЛ.6 ОГРАНИЧЕНИЕ ПРАВ ПОЛЬЗОВАТЕЛЕЙ ПО ВВОДУ ИНФОРМАЦИИ В ИНФОРМАЦИОННУЮ СИСТЕМУ

Требования к реализации ОЦЛ.6: В информационной системе должно осуществляться ограничение прав пользователей по вводу информации в информационную систему.

Ограничение прав пользователей по вводу информации предусматривает ограничение по вводу в определенные типы объектов доступа (объекты файловой системы, объекты баз данных, объекты прикладного и специального программного обеспечения) информации исходя из задач и полномочий, решаемых пользователем в информационной системе.

Ограничения прав пользователей по вводу информации в информационную систему должны фиксироваться в организационно-распорядительных документах по защите информации (документироваться) и реализовываться в соответствии с УПД.4 и УПД.5.

Требования к усилению ОЦЛ.6:

1) в информационной системе обеспечивается исключение возможности ввода пользователями информации в информационную систему, вследствие

реализации ограничительных интерфейсов по вводу информации только через специальные формы прикладного программного обеспечения.

Содержание базовой меры ОЦЛ.6:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ОЦЛ.6				+
Усиление ОЦЛ.6				

ОЦЛ.7 КОНТРОЛЬ ТОЧНОСТИ, ПОЛНОТЫ И ПРАВИЛЬНОСТИ ДАННЫХ, ВВОДИМЫХ В ИНФОРМАЦИОННУЮ СИСТЕМУ

Требования к реализации ОЦЛ.7: В информационной системе должен осуществляться контроль точности, полноты и правильности данных, вводимых в информационную систему.

Контроль точности, полноты и правильности данных, вводимых в информационную систему, обеспечивается путем установления и проверки соблюдения форматов ввода данных, синтаксических, семантических и (или) иных правил ввода информации в информационную систему (допустимые наборы символов, размерность, область числовых значений, допустимые значения, количество символов) для подтверждения того, что ввод информации соответствует заданному оператором формату и содержанию.

Вводимые данные должны проверяться на наличие конструкций, которые могут быть интерпретированы программно-техническими средствами информационной системы как исполняемые команды.

Требования к усилению ОЦЛ.7:

Не установлены.

Содержание базовой меры ОЦЛ.7:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ОЦЛ.7				
Усиление ОЦЛ.7				

ОЦЛ.8 КОНТРОЛЬ ОШИБОЧНЫХ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ ПО ВВОДУ И (ИЛИ) ПЕРЕДАЧЕ ИНФОРМАЦИИ И ПРЕДУПРЕЖДЕНИЕ ПОЛЬЗОВАТЕЛЕЙ ОБ ОШИБОЧНЫХ ДЕЙСТВИЯХ

Требования к реализации ОЦЛ.8: В информационной системе должен осуществляться контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях.

Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях должен предусматривать:

определение оператором типов ошибочных действий пользователей, которые потенциально могут привести к нарушению безопасности информации в информационной системе;

генерирование сообщений для пользователей об их ошибочных действиях и о возможности нарушения безопасности информации в информационной системе для корректировки действий пользователей;

регистрация информации об ошибочных действиях пользователей, которые могут привести к нарушению безопасности информации в информационной системе, в журналах регистрации событий безопасности в соответствии с РСБ.3;

предоставление доступа к сообщениям об ошибочных действиях пользователей только администраторам.

Требования к усилению ОЦЛ.8:

Не установлены.

Содержание базовой меры ОЦЛ.8:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ОЦЛ.8				
Усиление ОЦЛ.8				

3.10. ОБЕСПЕЧЕНИЕ ДОСТУПНОСТИ ИНФОРМАЦИИ (ОДТ)

ОДТ.1 ИСПОЛЬЗОВАНИЕ ОТКАЗОУСТОЙЧИВЫХ ТЕХНИЧЕСКИХ СРЕДСТВ

Требования к реализации ОДТ.1: Оператором должно обеспечиваться использование отказоустойчивых технических средств, предусматривающее:

определение сегментов информационной системы, в которых должны применяться отказоустойчивые технические средства, обладающие свойствами сохранять свою работоспособность после отказа одного или нескольких их составных частей, и перечня таких средств исходя из требуемых условий обеспечения непрерывности функционирования информационной системы и доступности информации, установленных оператором;

определение предельных (пороговых) значений характеристик (коэффициента) готовности, показывающего, какую долю времени от общего времени работы информационной системы техническое средство (техническое решение) находится в рабочем состоянии, и характеристик надежности (требуемое значение вероятности отказа в единицу времени) исходя из требуемых условий обеспечения непрерывности функционирования информационной системы и доступности информации, установленных оператором;

применение в информационной системе технических средств с установленными оператором характеристиками (коэффициентом) готовности и надежности, обеспечивающих требуемые условия непрерывности функционирования информационной системы и доступности информации;

контроль с установленной оператором периодичностью за значениями характеристик (коэффициентов) готовности и надежности технических средств и реагирование на ухудшение значений данных характеристик (инициализация плана восстановления работоспособности и иные методы реагирования);

замена технических средств, характеристики (коэффициенты) готовности и надежности которых достигли предельного значения.

Оператором должно быть обеспечено определение требуемых характеристик (коэффициентов) надежности и готовности в соответствии с национальными стандартами.

Требования к усилению ОДТ.1:

1) оператор выводит из эксплуатации техническое средство путем передачи его функций другому (резервному) техническому средству до достижения первым предельных (пороговых) значений характеристик (коэффициентов) готовности и (или) надежности;

2) в информационной системе реализуется автоматическое оповещение (сигнализация) о достижения техническим средством предельных (пороговых) значений характеристик (коэффициентов) готовности и надежности (степень достижения предельных значений определяется оператором);

3) в информационной системе реализуется автоматическое оповещение (сигнализация) о достижения техническим средством предельных (пороговых) значений характеристик загрузки.

Содержание базовой меры ОДТ.1:

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

ОДТ.2 РЕЗЕРВИРОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ, СРЕДСТВ ОБЕСПЕЧЕНИЯ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Требования к реализации ОДТ.2: Оператором должно обеспечиваться резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы, предусматривающее:

определение сегментов информационной системы, в которых должно осуществляться резервирование технических средств, программного обеспечения, каналов передачи информации и средств обеспечения функционирования, а также перечня резервируемых средств исходя из требуемых условий обеспечения непрерывности функционирования информационной системы и доступности информации, установленных оператором;

применение резервных (дублирующих) технических средств, программного обеспечения, каналов передачи информации и (или) средств обеспечения функционирования информационной системы, обеспечивающих требуемые условия непрерывности функционирования информационной системы и доступности информации;

ввод в действие резервного технического средства, программного обеспечения, канала передачи информации или средства обеспечения функционирования при нарушении требуемых условий непрерывности функционирования информационной системы и доступности информации.

Резервирование технических средств в зависимости от требуемых условий обеспечения непрерывности функционирования информационной системы и доступности информации включает ненагруженное («холодное») и (или) нагруженное («горячее»)резервирование.

При резервировании программного обеспечения осуществляется создание резервных копий общесистемного, специального и прикладного программного обеспечения, а также программного обеспечения средств защиты информации,

необходимых для обеспечения требуемых условий непрерывности функционирования информационной системы и доступности информации.

Резервирование каналов передачи информации включает:

резервирование каналов связи, обеспечивающее снижение вероятности отказа в доступе к информационной системе;

наличие у основных и альтернативных поставщиков телекоммуникационных услуг (провайдеров) информационной системы планов по восстановлению связи при авариях и сбоях, с указанием времени восстановления.

Резервирование средств обеспечения функционирования информационной системы включает:

использование кратковременных резервных источников питания для обеспечения правильного (корректного) завершения работы сегмента информационной системы (технического средства, устройства) в случае отключения основного источника питания;

использование долговременных резервных источников питания в случае длительного отключения основного источника питания и необходимости продолжения выполнения сегментом информационной системы (техническим средством, устройством) установленных функциональных (задач);

определение перечня энергозависимых технических средств, которым необходимо обеспечить наличие резервных источников питания (кратковременных и долговременных).

Правила и процедуры резервирования регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОДТ.2:

1) в информационной системе должно обеспечиваться резервирование автоматизированных рабочих мест, на которых обрабатывается информация (совокупности технических средств, установленного программного обеспечения, средств защиты информации и параметров настройки), в том числе предусматривающее:

пространственное (географическое) отделение резервных автоматизированных рабочих мест от основных мест обработки информации, с учетом возможных угроз нарушения доступности информации;

конфигурацию резервных мест обработки информации, предусматривающую минимально требуемые эксплуатационные возможности рабочего места;

разработку оператором процедур обеспечения требуемых условий обеспечения непрерывности функционирования информационной системы и доступности информации в случае нарушения функционирования (сбоев, аварий) резервных мест обработки информации;

ограничение времени обработки информации на резервном рабочем месте до времени восстановления функционирования основного рабочего места;

2) в информационной системе должно обеспечиваться предоставление резервных каналов связи от альтернативных поставщиков телекоммуникационных услуг (провайдеров), отличных от поставщиков (провайдеров) основных каналов связи;

3) в информационной системе должно обеспечиваться использование резервных каналов связи, проходящих по трассам отличным, от трасс прохождения основных каналов связи;

4) в информационной системе должно обеспечиваться использование резервных (отделенных от основных) телекоммуникационных сервисов, обеспечивающих доступность информации, до восстановления доступности основных телекоммуникационных сервисов поставщиком телекоммуникационных услуг (провайдером).

Содержание базовой меры ОДТ.2:

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

ОДТ.3 КОНТРОЛЬ БЕЗОТКАЗНОГО ФУНКЦИОНИРОВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ, ОБНАРУЖЕНИЕ И ЛОКАЛИЗАЦИЯ ОТКАЗОВ ФУНКЦИОНИРОВАНИЯ, ПРИНЯТИЕ МЕР ПО ВОССТАНОВЛЕНИЮ ОТКАЗАВШИХ СРЕДСТВ И ИХ ТЕСТИРОВАНИЕ

Требования к реализации ОДТ.3: Оператором должен осуществляться контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.

Контроль безотказного функционирования проводится в отношении серверного и телекоммуникационного оборудования, каналов связи, средств обеспечения функционирования информационной системы путем периодической проверки работоспособности в соответствии с эксплуатационной документацией (в том числе путем посылки тестовых сообщений и принятия «ответов», визуального контроля, контроля трафика, контроля «поведения» системы или иными методами).

При обнаружении отказов функционирования осуществляется их локализация и принятие мер по восстановлению отказавших средств в соответствии с ОЦЛ.3, их тестирование в соответствии с эксплуатационной документацией, а также регистрация событий, связанных с отказами функционирования, в соответствующих журналах.

Требования к усилению ОДТ.3:

1) в информационной системе должна быть обеспечена сигнализация (уведомление) о неисправностях, сбоях и отказах в функционировании программно-технических средств информационной системы;

2) оператором должна обеспечиваться регистрация сбоев и отказов в функционировании технических средств информационной системы;

3) в информационной системе должны применяться программные средства мониторинга технического состояния информационной системы, осуществляющие мониторинг отказов программных и программно-технических средств в соответствии с перечнем, определенным оператором.

Базовый набор ОДТ.3:

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

ОДТ.4 ПЕРИОДИЧЕСКОЕ РЕЗЕРВНОЕ КОПИРОВАНИЕ ИНФОРМАЦИИ НА РЕЗЕРВНЫЕ МАШИННЫЕ НОСИТЕЛИ ИНФОРМАЦИИ

Требования к реализации ОДТ.4: Оператором должно обеспечиваться периодическое резервное копирование информации на резервные машинные носители информации, предусматривающее:

резервное копирование информации на резервные машинные носители информации с установленной оператором периодичностью;

разработку перечня информации (типов информации), подлежащей периодическому резервному копированию на резервные машинные носители информации;

регистрацию событий, связанных с резервным копированием информации на резервные машинные носители информации;

принятие мер для защиты резервируемой информации, обеспечивающих ее конфиденциальность, целостность и доступность.

Правила и процедуры резервного копирования информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОДТ.4:

1) оператором должна осуществляться с установленной им периодичностью проверка работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из

резервных копий (периодичность проверки работоспособности определяется оператором);

2) оператором должно осуществляться хранение (размещение) резервных копий информации на отдельных (размещенных вне информационной системы) средствах хранения резервных копий и в помещениях, специально предназначенных для хранения резервных копий информации, которые исключают воздействие внешних факторов на хранимую информацию;

3) оператором должно осуществляться резервное копирование информации на зеркальную информационную систему (сегмент информационной системы, техническое средство, устройство);

4) оператором должна обеспечиваться соответствующая пропускная способность каналов связи, используемых для передачи резервных копий в процессе их создания или восстановления информации, для достижения требуемых условий обеспечения непрерывности функционирования информационной системы и доступности информации;

5) оператором должно осуществляться пространственное (географическое) разнесение мест хранения носителей резервных копий информации и мест расположения оригиналов этой информации.

Содержание базовой меры ОДТ.4:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ОДТ.4			+	+
Усиление ОДТ.4			1, 2	1, 3

ОДТ.5 ОБЕСПЕЧЕНИЕ ВОЗМОЖНОСТИ ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ С РЕЗЕРВНЫХ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ (РЕЗЕРВНЫХ КОПИЙ) В ТЕЧЕНИЕ УСТАНОВЛЕННОГО ВРЕМЕННОГО ИНТЕРВАЛА

Требования к реализации ОДТ.5: Оператором должна быть обеспечена возможность восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала.

Восстановление информации с резервных машинных носителей информации (резервных копий) должно предусматривать:

определение времени, в течение которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования информационной системы и доступности информации;

восстановление информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала;

регистрация событий, связанных восстановлением информации с резервных машинных носителей информации.

Правила и процедуры восстановления информации с резервных машинных носителей информации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОДТ.5:

1) оператором должна обеспечиваться возможность восстановления информации с учетом нагруженного («горячего») резервирования технических средств в соответствии с ОДТ.2;

2) в информационной системе должно осуществляться предоставление пользователям резервных мест обработки информации в соответствии с ОДТ.2 до восстановления из резервных копий информации и обеспечения ее доступности на основных местах обработки информации.

Содержание базовой меры ОДТ.5:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ОДТ.5			+	+
Усиление ОДТ.5				1

ОДТ.6 КЛАСТЕРИЗАЦИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ И (ИЛИ) ЕЕ СЕГМЕНТОВ

Требования к реализации ОДТ.6: В информационной системе должно обеспечиваться выделение групп однотипных узлов, объединенных каналами передачи информации и рассматриваемых как единый программно-технический ресурс, информационной системы в целом и (или) отдельных ее сегментов (серверов приложений, файловых серверов, серверов баз данных, средств защиты информации и иных сегментов) для обеспечения доступности информации, сервисов и механизмов защиты информации.

Требования к усилению ОДТ.6:

1) в информационной системе должна осуществляться кластеризация серверов контроллеров доменов, серверов резервного копирования, серверов управления и мониторинга состояния информационной системы, серверов виртуальной инфраструктуры и иных основных устройств и программного обеспечения системного уровня;

2) в информационной системе должна осуществляться кластеризация серверов приложений, файловых серверов, серверов баз данных, почтовых серверов и иных устройств и программного обеспечения прикладного уровня;

3) в информационной системе должна осуществляться кластеризация средств защиты информации (в случаях, когда это технически возможно), включая средства межсетевого экранирования, средства защиты каналов передачи информации.

Содержание базовой меры ОДТ.6:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ОДТ.6				
Усиление ОДТ.6				

ОДТ.7 КОНТРОЛЬ СОСТОЯНИЯ И КАЧЕСТВА ПРЕДОСТАВЛЕНИЯ УПОЛНОМОЧЕННЫМ ЛИЦОМ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ (МОЩНОСТЕЙ), В ТОМ ЧИСЛЕ ПО ПЕРЕДАЧЕ ИНФОРМАЦИИ

Требования к реализации ОДТ.7: Оператором должен осуществляться контроль состояния и качества предоставления уполномоченным лицом (провайдером) вычислительных ресурсов (мощностей), в том числе по передаче информации, предусматривающий:

контроль выполнения уполномоченным лицом требований о защите информации, установленных законодательством Российской Федерации и условиями договора (соглашения), на основании которого уполномоченное лицо обрабатывает информацию или предоставляет вычислительные ресурсы (мощности);

мониторинг состояния и качества предоставления уполномоченным лицом (провайдером) вычислительных ресурсов (мощностей);

мониторинг состояния и качества предоставления уполномоченным лицом (провайдером)услуг по передаче информации.

Условия, права и обязанности, содержание и порядок контроля должны определяться в договоре (соглашении), заключаемом между оператором и уполномоченным лицом на предоставление вычислительных ресурсов (мощностей) или передачу информации с использованием информационно-телекоммуникационных сетей связи.

Требования к усилению ОДТ.7:

1) между оператором и поставщиком услуг (телекоммуникационных, вычислительных) должно заключаться соглашение об уровне услуг, содержащее описание услуг, прав и обязанностей сторон и согласованный

уровень качества предоставляемых услуг в соответствии с законодательством Российской Федерации.

Содержание базовой меры ОДТ.7:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ОДТ.7			+	+
Усиление ОДТ.7				

3.11. ЗАЩИТА СРЕДЫ ВИРТУАЛИЗАЦИИ (ЗСВ)

ЗСВ.1 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ СУБЪЕКТОВ ДОСТУПА И ОБЪЕКТОВ ДОСТУПА В ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЕ, В ТОМ ЧИСЛЕ АДМИНИСТРАТОРОВ УПРАВЛЕНИЯ СРЕДСТВАМИ ВИРТУАЛИЗАЦИИ

Требования к реализации ЗСВ.1: В информационной системе должны обеспечиваться идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации, в соответствии с ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6 и ИАФ.7.

Виртуальная инфраструктура включает среду виртуализации (программное обеспечение, служебные данные компонентов виртуальной инфраструктуры) и аппаратное обеспечение (аппаратные средства, необходимые для функционирования среды виртуализации, в том числе средства резервного копирования и защиты информации).

В качестве компонентов виртуальной инфраструктуры необходимо, как минимум, рассматривать серверное оборудование, аппаратное обеспечение консолей управления, оборудование хранения данных, сетевое оборудование, гипервизор, хостовую операционную систему (если применимо), виртуальные машины, программную среду виртуальных машин (в том числе их операционные системы и программное обеспечение), виртуальное аппаратное обеспечение, виртуализированное программное обеспечение (виртуальные машины с предустановленным программным обеспечением, предназначенным для выполнения определенных функций в виртуальной инфраструктуре), программное обеспечение управления виртуальной инфраструктурой (в том числе гипервизором, настройками виртуальных машин, миграцией виртуальных машин, балансировкой нагрузки), служебные данные компонентов виртуальной инфраструктуры (настройки и иные служебные данные), средства резервного копирования компонентов среды виртуализации и средства защиты информации, используемые в рамках виртуальных машин и виртуальной инфраструктуры в целом.

В качестве объектов доступа в виртуальной инфраструктуре необходимо, как минимум, рассматривать программное обеспечение управления виртуальной инфраструктурой, гипервизор, хостовую операционную систему (если применимо), виртуальные машины, программную среду виртуальных машин (в том числе их операционные системы и программное обеспечение), виртуальные контейнеры (зоны), виртуализированное программное обеспечение (виртуальные машины с предустановленным программным обеспечением, предназначенная для выполнения определенных функций в виртуальной инфраструктуре), средства защиты информации, используемые в рамках виртуальных машин и виртуальной инфраструктуры в целом.

При реализации мер по идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре должны обеспечиваться:

идентификация и аутентификация администраторов управления средствами виртуализации;

идентификация и аутентификация субъектов доступа при их локальном и удалённом обращении к объектам доступа в виртуальной инфраструктуре;

блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

защита аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерных доступа к ней, уничтожения или модифицирования;

защита аутентификационной информации в процессе ее ввода для аутентификации в виртуальной инфраструктуре от возможного использования лицами, не имеющими на это полномочий;

идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления параметрами аппаратного обеспечения виртуальной инфраструктуры.

Внутри развернутых на базе виртуальной инфраструктуры виртуальных машин должна быть также обеспечена реализация мер по идентификации и аутентификации субъектов и объектов доступа в соответствии с ИАФ.1 – ИАФ.7.

Требования к усилению ЗСВ.1:

1) в информационной системе должны обеспечиваться взаимная идентификация и аутентификация пользователя и сервера виртуализации (виртуальных машин) при удалённом доступе.

Содержание базовой меры ЗСВ.1:

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

ЗСВ.2 УПРАВЛЕНИЕ ДОСТУПОМ СУБЪЕКТОВ ДОСТУПА К ОБЪЕКТАМ ДОСТУПА В ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЕ, В ТОМ ЧИСЛЕ ВНУТРИ ВИРТУАЛЬНЫХ МАШИН

Требования к реализации ЗСВ.2: В информационной системе должно обеспечиваться управление доступом субъектов доступа к объектам доступа, в

том числе внутри виртуальных машин, в соответствии с УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.9, УПД.10, УПД.11, УПД.12, УПД.13.

При реализации мер по управлению доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре должны обеспечиваться:

контроль доступа субъектов доступа к средствам управления компонентами виртуальной инфраструктуры;

контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения, виртуальных машин, файлам-образам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды;

управление доступом к виртуальному аппаратному обеспечению информационной системы, являющимся объектом доступа;

контроль запуска виртуальных машин на основе заданных оператором правил (режима запуска, типа используемого носителя и иных правил).

Кроме того, меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать:

разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к объектам доступа, расположенным внутри виртуальных машин, в соответствии с правилами разграничения доступа пользователей данных виртуальных машин (потребителей облачных услуг);

разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к ресурсам информационной системы, размещенным за пределами виртуальных машин, в соответствии с правилами разграничения доступа принятыми в информационной системе в целом.

Требования к усилению ЗСВ.2:

1) в информационной системе должен обеспечиваться доступ к операциям, выполняемым с помощью средств управления виртуальными машинами, в том числе к операциям создания, запуска, останова, создания копий, удаления виртуальных машин, который должен быть разрешен только администраторам виртуальной инфраструктуры;

2) в информационной системе должен обеспечиваться доступ к конфигурации виртуальных машин только администраторам виртуальной инфраструктуры;

3) администратор виртуальной инфраструктуры определяет ограничения по изменению состава устройств виртуальных машин, объема используемой оперативной памяти, подключаемых виртуальных и физических носителей информации;

4) в информационной системе должен обеспечиваться контроль доступа субъектов доступа к изолированному адресному пространству в памяти гипервизора, в памяти хостовой операционной системы, виртуальных машин и (или) иных объектов доступа.

Содержание базовой меры ЗСВ.2:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗСВ.2	+	+	+	+
Усиление ЗСВ.2		1, 2	1, 2	1, 2

ЗСВ.3 РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ В ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЕ

Требования к реализации ЗСВ.3: В информационной системе должна обеспечиваться регистрация событий безопасности в виртуальной инфраструктуре в соответствии с РСБ.1, РСБ.2, РСБ.3, РСБ.4 и РСБ.5.

При реализации мер по регистрации событий безопасности в виртуальной инфраструктуре дополнительно к событиям, установленным в РСБ.1, должны подлежать регистрации следующие события:

запуск (завершение) работы компонентов виртуальной инфраструктуры;

доступ субъектов доступа к компонентам виртуальной инфраструктуры;

изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения;

изменения правил разграничения доступа к компонентам виртуальной инфраструктуры.

При регистрации запуска (завершения) работы компонентов виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время запуска (завершения) работы гипервизора и виртуальных машин, хостовой операционной системы, программ и процессов в виртуальных машинах, результат запуска (завершения) работы указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке запуска (завершения) работы указанных компонентов виртуальной инфраструктуры.

При регистрации входа (выхода) субъектов доступа в компоненты виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время доступа субъектов доступа к гипервизору и виртуальной машине, к хостовой операционной системе, результат попытки доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры.

При изменении в составе и конфигурации компонентов виртуальной инфраструктуры во время запуска, функционирования и в период её аппаратного отключения состав и содержание информации, подлежащей

регистрации, должны включать дату и время изменения в составе и конфигурации виртуальных машин, виртуального аппаратного обеспечения, виртуализированного программного обеспечения, виртуального аппаратного обеспечения в гипервизоре и в виртуальных машинах, в хостовой операционной системе, виртуальном сетевом оборудовании, результат попытки изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры.

При изменении правил разграничения доступа к компонентам виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время изменения правил разграничения доступа к виртуальному и физическому аппаратному обеспечению, к файлам-образам виртуализированного программного обеспечения и виртуальных машин, к файлам-образам, используемым для обеспечения работы виртуальных файловых систем, к виртуальному сетевому оборудованию, к защищаемой информации, хранимой и обрабатываемой в гипервизоре и виртуальных машинах, в хостовой операционной системе, результат попытки изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры.

Требования к усилению ЗСВ.3:

1) в информационной системе должен обеспечиваться централизованный сбор, хранение и анализ информации о зарегистрированных событиях безопасности виртуальной инфраструктуры;

2) в информационной системе при регистрации запуска (завершения) работы компонентов виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время запуска (завершения) программ и процессов в гипервизоре и хостовой операционной системе;

3) в информационной системе должна обеспечиваться регистрация событий безопасности, связанных с перемещением и размещением виртуальных машин.

Содержание базовой меры ЗСВ.3:

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

ЗСВ.4 УПРАВЛЕНИЕ (ФИЛЬТРАЦИЯ, МАРШРУТИЗАЦИЯ, КОНТРОЛЬ СОЕДИНЕНИЯ, ОДНОНАПРАВЛЕННАЯ ПЕРЕДАЧА) ПОТОКАМИ ИНФОРМАЦИИ МЕЖДУ КОМПОНЕНТАМИ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ, А ТАКЖЕ ПО ПЕРИМЕТРУ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

Требования к реализации ЗСВ.4: В информационной системе должно осуществляться управление потоками информации между компонентами виртуальной инфраструктуры и по периметру виртуальной инфраструктуры в соответствии с УПД.3, ЗИС.3.

При реализации мер по управлению потоками информации между компонентами виртуальной инфраструктуры должны обеспечиваться:

фильтрация сетевого трафика между компонентами виртуальной инфраструктуры, в том числе между внешними по отношению к серверу виртуализации сетями и внутренними по отношению к серверу виртуализации сетями, в том числе при организации сетевого обмена с сетями связи общего пользования;

обеспечение доверенных канала, маршрута внутри виртуальной инфраструктуры между администратором, пользователем и средствами защиты информации (функциями безопасности);

контроль передачи служебных информационных сообщений, передаваемых в виртуальных сетях гипервизора, хостовой операционной системы, по составу, объёму и иным характеристикам;

отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры гипервизора, хостовой операционной системы, виртуальной вычислительной сети;

обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;

обеспечение изоляции потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры (гипервизором, хостовой операционной системой) и сетевых потоков виртуальной вычислительной сети;

семантический и статистический анализ сетевого трафика виртуальной вычислительной сети.

Требования к усилению ЗСВ.4:

1) в информационной системе, построенной с применением технологии виртуализации, должна быть обеспечена единая точка подключения к виртуальной инфраструктуре (при необходимости резервирования каналов связи, точка подключения должна рассматриваться как комплексное решение, включающее в себя средства взаимодействия с основным и резервными каналами связи);

2) в информационной системе должна обеспечиваться фильтрация сетевого трафика от (к) каждой гостевой операционной системы, в виртуальных сетях гипервизора и для каждой виртуальной машины;

3) в информационной системе должен обеспечиваться запрет прямого (с использованием механизмов, встроенных в средства виртуализации) взаимодействия виртуальных машин между собой; для служебных данных должен обеспечиваться контроль прямого взаимодействия виртуальных машин между собой;

4) в информационной системе в соответствии с законодательством Российской Федерации применяются криптографические методы защиты информации конфиденциального характера, передаваемой по виртуальным и физическим каналам связи гипервизора, хостовой операционной системы;

5) в информационной системе при реализации мер по управлению потоками информации между компонентами виртуальной инфраструктуры должны обеспечиваться семантический и статистический анализ сетевого трафика;

6) в информационной системе должно обеспечиваться определение перечня протоколов и портов (включая динамически выделяемые порты), необходимых для работы приложений и сервисов в рамках виртуальной инфраструктуры;

7) в информационной системе должно обеспечиваться определение перечня протоколов и портов (включая динамически выделяемые порты), необходимых для работы приложений и сервисов между виртуальной инфраструктурой и сетями, являющимися внешними по отношению к виртуальной инфраструктуре.

Содержание базовой меры ЗСВ.4:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗСВ.4			+	+
Усиление ЗСВ.4				1, 2

ЗСВ.5 ДОВЕРЕННАЯ ЗАГРУЗКА СЕРВЕРОВ ВИРТУАЛИЗАЦИИ, ВИРТУАЛЬНОЙ МАШИНЫ (КОНТЕЙНЕРА), СЕРВЕРОВ УПРАВЛЕНИЯ ВИРТУАЛИЗАЦИЕЙ

Требования к реализации ЗСВ.5: В информационной системе должна обеспечиваться доверенная загрузка серверов виртуализации, виртуальных машин (контейнеров) и серверов управления виртуализацией в соответствии с УПД.17.

Доверенная загрузка должна обеспечивать блокирование попыток несанкционированной загрузки гипервизора, хостовой и гостевых операционных систем.

Доверенная загрузка гипервизоров обеспечивается с использованием средств доверенной загрузки функционирующих на серверах виртуализации.

Доверенная загрузка виртуальных машин (контейнеров) обеспечивается с использованием многокомпонентных средств доверенной загрузки, отдельные компоненты которых функционируют в гипервизорах.

Требования к усилению ЗСВ.5:

1) должна обеспечиваться доверенная загрузка автоматизированных рабочих мест администраторов управления средствами виртуализации.

Содержание базовой меры ЗСВ.5:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗСВ.5				
Усиление ЗСВ.5				

ЗСВ.6 УПРАВЛЕНИЕ ПЕРЕМЕЩЕНИЕМ ВИРТУАЛЬНЫХ МАШИН (КОНТЕЙНЕРОВ) И ОБРАБАТЫВАЕМЫХ НА НИХ ДАННЫХ

Требования к реализации ЗСВ.6: Оператором должно обеспечиваться управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.

При управлении перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных должны обеспечиваться:

регламентирование порядка перемещения (определение ответственных за организацию процесса, объектов перемещения, ресурсов инфраструктуры, задействованных в перемещении, а также способов перемещения);

управление размещением и перемещением файлов-образов виртуальных машин (контейнеров) между носителями (системами хранения данных);

управление размещением и перемещением исполняемых виртуальных машин (контейнеров) между серверами виртуализации;

управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных).

Управление перемещением виртуальных машин (контейнеров) должно предусматривать:

полный запрет перемещения виртуальных машин (контейнеров);

ограничение перемещения виртуальных машин (контейнеров) в пределах информационной системы (сегмента информационной системы);

ограничение перемещения виртуальных машин (контейнеров) между сегментами информационной системы.

Требования к усилению ЗСВ.6:

1) оператором должно обеспечиваться перемещение виртуальных машин (контейнеров) и обрабатываемых на них данных в пределах информационной системы только на контролируемые им (или уполномоченным лицом) технические средства (сервера виртуализации, носители, системы хранения данных);

2) оператором должна осуществляться обработка отказов перемещения виртуальных машин (контейнеров) и обрабатываемых на них данных;

3) в информационной системе должны использоваться механизмы централизованного управления перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных;

4) в информационной системе должна быть обеспечена непрерывность регистрации событий безопасности в виртуальных машинах (контейнерах) в процессе перемещения;

5) в информационной системе должна осуществляться очистка освобождаемых областей памяти на серверах виртуализации, носителях, системах хранения данных при перемещении виртуальных машин (контейнеров) и обрабатываемых на них данных.

Содержание базовой меры ЗСВ.6:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗСВ.6			+	+
Усиление ЗСВ.6			1	1, 2

ЗСВ.7 КОНТРОЛЬ ЦЕЛОСТНОСТИ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ И ЕЕ КОНФИГУРАЦИЙ

Требования к реализации ЗСВ.7: В информационной системе должен обеспечиваться контроль целостности компонентов виртуальной инфраструктуры в соответствии с ОЦЛ.1.

При реализации мер по контролю целостности компонентов виртуальной инфраструктуры должны обеспечиваться:

контроль целостности компонентов, критически важных для функционирования хостовой операционной системы, гипервизора, гостевых операционных систем и (или) обеспечения безопасности обрабатываемой в них

информации (загрузчика, системных файлов, библиотек операционной системы и иных компонентов);

контроль целостности состава и конфигурации виртуального оборудования;

контроль целостности файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин;

контроль целостности файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем (контроль файлов-образов должен проводиться во время, когда файлы-образы не задействованы).

В информационной системе должен обеспечиваться контроль целостности резервных копий виртуальных машин (контейнеров).

Требования к усилению ЗСВ.7:

1) в информационной системе должен обеспечиваться контроль целостности базовой системы ввода-вывода вычислительных серверов и консолей управления виртуальной инфраструктуры;

2) в информационной системе должен обеспечиваться контроль целостности микропрограмм и служебных данных элементов аппаратной части виртуальной инфраструктуры (в том числе загрузочных записей машинных носителей информации);

3) в информационной системе должен обеспечиваться контроль состава аппаратной части компонентов виртуальной инфраструктуры;

4) в информационной системе должен обеспечиваться контроль целостности программного обеспечения облачных клиентов.

Содержание базовой меры ЗСВ.7:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗСВ.7			+	+
Усиление ЗСВ.7			3	1, 3

ЗСВ.8 РЕЗЕРВНОЕ КОПИРОВАНИЕ ДАННЫХ, РЕЗЕРВИРОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ, А ТАКЖЕ КАНАЛОВ СВЯЗИ ВНУТРИ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

Требования к реализации ЗСВ.8: В информационной системе должны обеспечиваться резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры и каналов

связи внутри виртуальной инфраструктуры в соответствии с ОДТ.2, ОДТ.4, ОДТ.5.

При реализации мер по резервному копированию данных, резервированию технических средств, программного обеспечения виртуальной инфраструктуры должны обеспечиваться:

определение мест хранения резервных копий виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре;

резервное копирование виртуальных машин (контейнеров);

резервное копирование данных, обрабатываемых в виртуальной инфраструктуре;

резервирование программного обеспечения виртуальной инфраструктуры;

резервирование каналов связи, используемых в виртуальной инфраструктуре;

периодическая проверка резервных копий и возможности восстановления виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре с использованием резервных копий.

Требования к усилению ЗСВ.8:

1) в информационной системе должно выполняться резервное копирование конфигурации виртуальной инфраструктуры;

2) в информационной системе должно выполняться резервное копирование программного обеспечения серверов управления виртуализацией, автоматизированного рабочего места администратора управления средствами виртуализации;

3) в информационной системе должно выполняться резервирование дистрибутивов средств построения виртуальной инфраструктуры (в том числе средств управления виртуальной инфраструктурой);

4) в информационной системе должно обеспечиваться резервирование технических средств для серверов виртуализации, серверов управления виртуализацией, автоматизированного рабочего места администратора управления средствами виртуализации;

5) в информационной системе должно обеспечиваться резервирование технических средств систем хранения данных и их компонент, используемых в виртуальной инфраструктуре;

6) в информационной системе должно обеспечиваться резервирование технических средств активного (коммутационного) и пассивного оборудования каналов связи, используемых в виртуальной инфраструктуре;

7) в информационной системе должно обеспечиваться применение технологий распределенного хранения информации и восстановления информации после сбоев для обеспечения отказоустойчивости виртуальной инфраструктуры.

Содержание базовой меры ЗСВ.8:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗСВ.8			+	+
Усиление ЗСВ.8				1, 2, 3

ЗСВ.9 РЕАЛИЗАЦИЯ И УПРАВЛЕНИЕ АНТИВИРУСНОЙ ЗАЩИТОЙ В ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЕ

Требования к реализации ЗСВ.9: В информационной системе должны обеспечиваться реализация и управление антивирусной защитой в виртуальной инфраструктуре в соответствии с АВЗ.1, АВЗ.2.

При реализации соответствующих мер должны обеспечиваться:

проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов;

проверка наличия вредоносных программ в гостевой операционной системе, в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов.

Требования к усилению ЗСВ.9:

1) в информационной системе должно обеспечиваться разграничение доступа к управлению средствами антивирусной защиты;

2) в информационной системе должен обеспечиваться контроль функционирования средств антивирусной защиты в виртуальной инфраструктуре, в том числе маршрутизация потоков информации в виртуальной инфраструктуре через средство антивирусной защиты;

3) в информационной системе должна обеспечиваться реализация технологии обновления программного обеспечения и баз данных признаков компьютерных вирусов средств антивирусной защиты, предусматривающая однократную передачу обновлений на сервер виртуальной инфраструктуры для их последующего применения в виртуальных машинах;

4) в информационной системе должна обеспечиваться проверка наличия вредоносных программ (вирусов) в гипервизоре;

5) в информационной системе должна обеспечиваться проверка наличия вредоносных программ в файлах конфигурации виртуального оборудования;

6) в информационной системе должна обеспечиваться проверка наличия вредоносных программ в файлах-образах виртуализированного программного обеспечения и виртуальных машин.

Содержание базовой меры ЗСВ.9:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗСВ.9		+	+	+
Усиление ЗСВ.9			1	1

ЗСВ.10 РАЗБИЕНИЕ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ НА СЕГМЕНТЫ (СЕГМЕНТИРОВАНИЕ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ) ДЛЯ ОБРАБОТКИ ИНФОРМАЦИИ ОТДЕЛЬНЫМ ПОЛЬЗОВАТЕЛЕМ И (ИЛИ) ГРУППОЙ ПОЛЬЗОВАТЕЛЕЙ

Требования к реализации ЗСВ.10: В информационной системе должно обеспечиваться разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей в соответствии с ЗИС.17.

Требования к усилению ЗСВ.10:

1) в информационной системе должно обеспечиваться логическое сегментирование виртуальной инфраструктуры, предусматривающее выделение группы виртуальных машин, хранилищ информации и информационных потоков, предназначенных для решения выделенных (обособленных) задач;

2) в информационной системе должно обеспечиваться выделение в отдельный сегмент (отдельные сегменты) серверов управления виртуализацией (автоматизированного рабочего места администратора управления средствами виртуализации);

3) в информационной системе должно обеспечиваться физическое сегментирование виртуальной инфраструктуры для решения выделенных (обособленных) задач.

Содержание базовой меры ЗСВ.10:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗСВ.10			+	+
Усиление ЗСВ.10				2

3.12. ЗАЩИТА ТЕХНИЧЕСКИХ СРЕДСТВ (ЗТС)

ЗТС.1 ЗАЩИТА ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ, ОТ ЕЕ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Требования к реализации ЗТС.1: Оператором должна обеспечиваться защита информации, обрабатываемой техническими средствами, от ее утечки за счет побочных электромагнитных излучений и наводок.

Защита информации от утечки по техническим каналам должна осуществляться в соответствии со Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30 августа 2002 г. № 282, а также иными методическими документами ФСТЭК России по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, от утечки по техническим каналам.

Требования к усилению ЗТС.1:
Не установлены.

Содержание базовой меры ЗТС.1:

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

ЗТС.2 ОРГАНИЗАЦИЯ КОНТРОЛИРУЕМОЙ ЗОНЫ, В ПРЕДЕЛАХ КОТОРОЙ ПОСТОЯННО РАЗМЕЩАЮТСЯ СТАЦИОНАРНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА, ОБРАБАТЫВАЮЩИЕ ИНФОРМАЦИЮ, И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ, А ТАКЖЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ФУНКЦИОНИРОВАНИЯ

Требования к реализации ЗТС.2: Оператором должна обеспечиваться контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

Контролируемая зона включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание работников (сотрудников) оператора и лиц, не имеющих постоянного допуска на объекты информационной системы (не являющихся работниками оператора), а также транспортных, технических и иных материальных средств.

Границами контролируемой зоны могут являться периметр охраняемой территории, ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории. Границы контролируемой зоны устанавливаются в организационно-распорядительных документах по защите информации.

Для одной информационной системы (ее сегментов) может быть организовано несколько контролируемых зон.

Требования к усилению ЗТС.2:

Не установлены.

Содержание базовой меры ЗТС.2:

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

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

Требования к реализации ЗТС.3: Оператором должны обеспечиваться 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.

Контроль и управление физическим доступом должны предусматривать:

определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;

санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;

учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

Правила и процедуры контроля и управления физическим доступом регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗТС.3:

1) оператором должны применяться автоматизированные системы контроля и управления доступом (СКУД), обеспечивающие контроль и учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены с учетом ГОСТ Р 51241-2008;

2) оператором должны применяться средства видеонаблюдения, обеспечивающие регистрацию доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;

3) оператором обеспечивается интеграция системы контроля и управления доступом (СКУД) со средствами идентификации и аутентификации пользователей в информационной системе в соответствии с ИАФ.1, ИАФ.6 и средствами управления доступом в соответствии с УПД.2, УПД.10.

Содержание базовой меры ЗТС.3:

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

ЗТС.4 РАЗМЕЩЕНИЕ УСТРОЙСТВ ВЫВОДА (ОТОБРАЖЕНИЯ) ИНФОРМАЦИИ, ИСКЛЮЧАЮЩЕЕ ЕЕ НЕСАНКЦИОНИРОВАННЫЙ ПРОСМОТР

Требования к реализации ЗТС.4: Оператором должно осуществляться размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

В качестве устройств вывода (отображения) информации в информационной системе следует рассматривать экраны мониторов автоматизированных рабочих мест пользователей, мониторы консолей управления технических средств (серверов, телекоммуникационного оборудования и иных технических средств), видеопанели, видеостены и другие средства визуального отображения защищаемой информации, печатающие

устройства (принтеры, плоттеры и иные устройства), аудиоустройства, многофункциональные устройства.

Размещение устройств вывода (отображения, печати) информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Не следует размещать устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.

Требования к усилению ЗТС.4:

1) оператором обеспечивается установка на окна помещений информационной системы средств, ограничивающих возможность визуального ознакомления с защищаемой информацией извне помещений (жалюзи, плотные шторы и иные средства), если в этих помещениях размещены устройства вывода информации на печать и (или) осуществляется отображение информации на видеоустройства.

Содержание базовой меры ЗТС.4:

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

ЗТС.5 ЗАЩИТА ОТ ВНЕШНИХ ВОЗДЕЙСТВИЙ (ВОЗДЕЙСТВИЙ ОКРУЖАЮЩЕЙ СРЕДЫ, НЕСТАБИЛЬНОСТИ ЭЛЕКТРОСНАБЖЕНИЯ, КОНДИЦИОНИРОВАНИЯ И ИНЫХ ВНЕШНИХ ФАКТОРОВ)

Требования к реализации ЗТС.5: Оператором должна осуществляться защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов).

Защита от внешних воздействий в соответствии с требованиями законодательства Российской Федерации (национальных стандартов, технических регламентов) должна предусматривать:

выполнение норм и правил пожарной безопасности;

выполнение норм и правил устройства и технической эксплуатации электроустановок, а также соблюдение параметров электропитания и заземления технических средств;

обеспечение необходимых для эксплуатации технических средств температурно-влажностного режима и условий по степени запыленности воздуха.

Требования к усилению ЗТС.5:
Не установлены.

Содержание базовой меры ЗТС.5:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗТС.5				+
Усиление ЗТС.5				

3.13. ЗАЩИТА ИНФОРМАЦИОННОЙ СИСТЕМЫ, ЕЕ СРЕДСТВ И 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

Требования к реализации ЗИС.1: В информационной системе должно быть обеспечено разделение функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации(функций безопасности) и функциональных возможностей пользователей по обработке информации.

Функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации включают функции по управлению базами данных, прикладным программным обеспечением, телекоммуникационным оборудованием, рабочими станциями, серверами, средствами защиты информации и иные функции, требующие высоких привилегий.

Разделение функциональных возможностей обеспечивается на физическом и (или) логическом уровне путем выделения части программно-технических средств информационной системы, реализующих функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации, в отдельный домен, использования различных автоматизированных рабочих мест и серверов, различных типов операционных систем, разных способов аутентификации, различных сетевых адресов, выделенных каналов управления и (или) комбинаций данных способов, а также иными методами.

Требования к усилению ЗИС.1:

1) в информационной системе должно обеспечиваться исключение отображения функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации в интерфейсе пользователя;

2) в информационной системе должно обеспечиваться выделение автоматизированных рабочих мест для администраторов информационной системы;

3) в информационной системе должно обеспечиваться выделение автоматизированных рабочих мест для администраторов безопасности;

4) оператором должно обеспечиваться исключение возможности управления (администрирования) информационной системой, управления (администрирования) системой защиты информации из-за пределов контролируемой зоны.

Содержание базовой меры ЗИС.1:

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

ЗИС.2 ПРЕДОТВРАЩЕНИЕ ЗАДЕРЖКИ ИЛИ ПРЕРЫВАНИЯ ВЫПОЛНЕНИЯ ПРОЦЕССОВ С ВЫСОКИМ ПРИОРИТЕТОМ СО СТОРОНЫ ПРОЦЕССОВ С НИЗКИМ ПРИОРИТЕТОМ

Требования к реализации ЗИС.2: В информационной системе должно обеспечиваться предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов (служб, сервисов) с низким приоритетом, предусматривающее:

определение приоритетов процессов (служб, сервисов) для пользователей и (или) групп пользователей и (или) ролей в информационной системе;

выполнение процессов (служб, сервисов) в информационной системе с учетом их приоритета (в первую очередь должны выполняться процессы с более высоким приоритетом);

исключение задержки и (или) вмешательства в выполнение процессов (служб, сервисов) с более высоким приоритетом со стороны процессов (служб, сервисов) с более низким приоритетом.

Требования к усилению ЗИС.2:

1) в информационной системе должно обеспечиваться исключение возможности несанкционированного изменения приоритетов выполнения процессов.

Содержание базовой меры ЗИС.2:

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

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

Требования к реализации ЗИС.3: Оператором должна быть обеспечена защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны.

Защита информации обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации или иными методами.

Требования к усилению ЗИС.3:

1) оператор обеспечивает защиту от модификации и навязывания (ввода ложной информации) видеоинформации (звуковой информации) путем ее маркирования и контроля (в том числе с использованием цифровых водяных знаков) в различных точках тракта ее формирования и распространения;

2) оператор обеспечивает защиту от модификации и навязывания (ввода ложной информации) передаваемой видеоинформации путем выявления и удаления скрытых вставок.

Содержание базовой меры ЗИС.3:

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

ЗИС.4 ОБЕСПЕЧЕНИЕ ДОВЕРЕННЫХ КАНАЛА, МАРШРУТА МЕЖДУ АДМИНИСТРАТОРОМ, ПОЛЬЗОВАТЕЛЕМ И СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ (ФУНКЦИЯМИ БЕЗОПАСНОСТИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ)

Требования к реализации ЗИС.4: В информационной системе должны обеспечиваться доверенные маршруты передачи данных между администратором (пользователем) и средствами защиты информации (функциями безопасности средств защиты информации), определяемыми оператором.

Оператором должен быть определен перечень целей (функций) передачи данных, для которых требуется доверенный канал (маршрут).

Доверенный канал между пользователем и средствами защиты информации должен обеспечиваться при удаленном и локальном доступе в информационную систему.

Требования к усилению ЗИС.4:
Не установлены.

Содержание базовой меры ЗИС.4:

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

ЗИС.5 ЗАПРЕТ НЕСАНКЦИОНИРОВАННОЙ УДАЛЕННОЙ АКТИВАЦИИ ВИДЕОКАМЕР, МИКРОФОНОВ И ИНЫХ ПЕРИФЕРИЙНЫХ УСТРОЙСТВ, КОТОРЫЕ МОГУТ АКТИВИРОВАТЬСЯ УДАЛЕННО, И ОПОВЕЩЕНИЕ ПОЛЬЗОВАТЕЛЕЙ ОБ АКТИВАЦИИ ТАКИХ УСТРОЙСТВ

Требования к реализации ЗИС.5: В информационной системе должны осуществляться запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств, в том числе путем сигнализации, индикации.

Запрет несанкционированной удаленной активации должен осуществляться в отношении всех периферийных устройств ввода (вывода) информации, которые имеют возможность управления (запуска, включения, выключения) через компоненты программного обеспечение, установленные на рабочем месте пользователя, коммуникационных сервисов сторонних лиц (провайдеров) (ICQ, Skype и иные сервисы).

Запрет несанкционированной удаленной активации должен осуществляться через физическое исключение такой возможности и (или) путем управления программным обеспечением.

В исключительных случаях для решения установленных оператором отдельных задач, решаемых информационной системой, допускается возможность удаленной активации периферийных устройств. При этом должно быть обеспечено определение и фиксирование в организационно-распорядительных документах по защите информации (документирование) перечня периферийных устройств, для которых допускается возможность удаленной активации и обеспечен контроль за активацией таких устройств.

Требования к усилению ЗИС.5:

1) в информационной системе должна обеспечиваться возможность физического отключения периферийных устройств (например, отключение при

организации и проведении совещаний в помещениях, где размещены видеокамеры и микрофоны);

2) в информационной системе должна обеспечиваться возможность блокирования входящего и исходящего трафика от пользователей систем, предоставляющих внешние сервисы (например, системы видеоконференцсвязи), в которых конфигурации (настройки) сервисов для конечных пользователей устанавливаются провайдерами или самими пользователями;

3) оператором обеспечивается удаление (отключение) из информационной системы (отдельных сегментов, например, расположенных в защищаемых и выделенных помещениях) периферийных устройств, перечень которых определяется оператором;

4) оператором обеспечивается запись и хранение в течение установленного времени информации, переданной (полученной) периферийными устройствами ввода (вывода) информации при разрешенной удаленной активации периферийных устройств ввода (вывода) информации.

Содержание базовой меры ЗИС.5:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.5	+	+	+	+
Усиление ЗИС.5			1	1,2

ЗИС.6 ПЕРЕДАЧА И КОНТРОЛЬ ЦЕЛОСТНОСТИ АТРИБУТОВ БЕЗОПАСНОСТИ (МЕТОК БЕЗОПАСНОСТИ), СВЯЗАННЫХ С ИНФОРМАЦИЕЙ, ПРИ ОБМЕНЕ ИНФОРМАЦИЕЙ С ИНЫМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

Требования к реализации ЗИС.6: В информационной системе должна осуществляться передача, сопоставление (сравнение) атрибутов безопасности (меток безопасности) с информацией, которой она обменивается с иными (внешними) информационными системами.

Атрибуты безопасности могут сопоставляться с информацией, содержащейся в информационной системе, в явном или скрытом виде.

Меры по передаче и контролю целостности (сопоставлению, сравнению) атрибутов безопасности (меток безопасности) реализуются в соответствии с УПД.12.

Требования к усилению ЗИС.6:

1) в информационной системе должен обеспечиваться контроль целостности атрибутов безопасности (меток безопасности).

Содержание базовой меры ЗИС.6:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.6				
Усиление ЗИС.6				

ЗИС.7 КОНТРОЛЬ САНКЦИОНИРОВАННОГО И ИСКЛЮЧЕНИЕ НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ МОБИЛЬНОГО КОДА, В ТОМ ЧИСЛЕ РЕГИСТРАЦИЯ СОБЫТИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ МОБИЛЬНОГО КОДА, ИХ АНАЛИЗ И РЕАГИРОВАНИЕ НА НАРУШЕНИЯ, СВЯЗАННЫЕ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ МОБИЛЬНОГО КОДА

Требования к реализации ЗИС.7: Оператором должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий мобильного кода (активного контента) в информационной системе, в том числе регистрация событий, связанных с использованием технологии мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологии мобильного кода. Технология мобильного кода включает, в том числе использование Java, JavaScript, ActiveX, PDF, Postscript, Flash-анимация и VBScript и иных технологий.

При контроле использования технологий мобильного кода должно быть обеспечено:

определение перечня мобильного кода и технологий мобильного кода разрешенных и (или) запрещенных для использования в информационной системе;

определение разрешенных мест распространения (серверы информационной системы) и использования мобильного кода (автоматизированные рабочие места, мобильные технические средства информационной системы) и функций информационной системы, для которых необходимо применение технологии мобильного кода;

регистрация и анализ событий, связанных с разработкой, приобретением или внедрением технологии мобильного кода;

исключение возможности использования запрещенного мобильного кода в информационной системе, а также внедрение мобильного кода в местах, не разрешенных для его установки.

Правила и процедуры контроля использования технологий мобильного кода регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗИС.7:

1) в информационной системе должны быть реализованы механизмы обнаружения и анализа мобильного кода для выявления фактов несанкционированного использования мобильного кода и выполнения действий по реагированию (оповещение администраторов, изоляция мобильного кода (перемещение в карантин), блокирование мобильного кода, удаление мобильного кода) и иные действия, определяемые оператором;

2) в информационной системе должен осуществляться запрет загрузки и выполнения запрещенного мобильного кода;

3) в информационной системе для приложений, определяемых оператором, должен осуществляться запрет автоматического выполнения разрешенного мобильного кода (уведомление пользователя о получении мобильного кода и запрос разрешения на запуск или иные действия определяемые оператором);

4) в информационной системе должен осуществляться контроль подлинности источника мобильного кода и контроль целостности мобильного кода.

Содержание базовой меры ЗИС.7:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.7			+	+
Усиление ЗИС.7			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

Требования к реализации ЗИС.8: Оператором должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий передачи речи в информационной системе, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи. При контроле использования технологий передачи речи должно быть обеспечено:

определение перечня технологий (сервисов) передачи речи разрешенных и (или) запрещенных для использования в информационной системе;

определение субъектов доступа (категорий пользователей), которым разрешены разработка, приобретение или внедрение технологий передачи речи в соответствии с установленными ролями;

реализация параметров настройки, исключающих возможность удаленной конфигурации устройств передачи речи;

регистрация и анализ событий, связанных с разработкой, приобретением и внедрением технологий передачи речи;

исключение возможности использования запрещенной технологии передачи речи в информационной системе, а также разработки, приобретения и внедрения технологий передачи речи субъектам доступа (пользователям), которым не разрешено ее использование.

Технология передачи речи включает, в том числе, передачу речи через Интернет (в частности VoIP).

Правила и процедуры контроля использования технологий передачи речи регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗИС.8:

Не установлены.

Содержание базовой меры ЗИС.8:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.8			+	+
Усиление ЗИС.8				

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

Требования к реализации ЗИС.9: Оператором должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий передачи видеоинформации в информационной системе, в том числе регистрация событий, связанных с использованием технологий передачи видеоинформации, их анализ и реагирование на нарушения, связанные с использованием технологий передачи видеоинформации. При контроле использования технологий передачи видеоинформации должно быть обеспечено:

определение перечня технологий (сервисов) передачи видеоинформации разрешенных и (или) запрещенных для использования в информационной системе;

определение субъектов доступа (категорий пользователей), которым разрешены разработка, приобретение или внедрение технологий передачи видеоинформации в соответствии с установленными ролями;

реализация параметров настройки, исключающих возможность удаленной конфигурации устройств передачи видеоинформации;

регистрация и анализ событий, связанных с разработкой, приобретением и внедрением технологий передачи видеоинформации;

исключение возможности использования запрещенной технологии передачи видеоинформации в информационной системе, а также разработки, приобретения и внедрения технологий передачи видеоинформации субъектов доступа (пользователям), которым не разрешено ее использование.

Технология передачи видеоинформации включает, в том числе, применение технологий видеоконференцсвязи.

Правила и процедуры контроля передачи видеоинформации регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗИС.9:

Не установлены.

Содержание базовой меры ЗИС.9:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.9			+	+
Усиление ЗИС.9				

ЗИС.10 ПОДТВЕРЖДЕНИЕ ПРОИСХОЖДЕНИЯ ИСТОЧНИКА ИНФОРМАЦИИ, ПОЛУЧАЕМОЙ В ПРОЦЕССЕ ОПРЕДЕЛЕНИЯ СЕТЕВЫХ АДРЕСОВ ПО СЕТЕВЫМ ИМЕНАМ ИЛИ ОПРЕДЕЛЕНИЯ СЕТЕВЫХ ИМЕН ПО СЕТЕВЫМ АДРЕСАМ

Требования к реализации ЗИС.10: В информационной системе должна обеспечиваться возможность подтверждения происхождения источника и целостности информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам, в том числе с использованием DNS-серверов. При подтверждении происхождения источника должны обеспечиваться:

аутентификация в соответствии с ИАФ.7 и (или) ИАФ.2 сервера, являющегося источником ответов на запросы (сервер доменных имен или DNS-сервер) по определению сетевых адресов (IP-адресов) по сетевым именам (доменные имена);

аутентификация в соответствии с ИАФ.7 и (или) ИАФ.2 сервера, являющегося источником ответов на запросы (кэширующийDNS-сервер) по определению сетевых имен (доменных имен) по сетевым адресам (IP-адресам).

Требования к усилению ЗИС.10:

1) в информационной системе должен осуществляться процесс верификации цепочки доверия между основным (корневым) и подчиненными (дочерними) доменами (например, с использованием записей ресурсов в системе доменных имен, сопоставляющих сетевое имя и сетевой адрес средств вычислительной техники и технических средств).

Содержание базовой меры ЗИС.10:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.10				
Усиление ЗИС.10				

ЗИС.11 ОБЕСПЕЧЕНИЕ ПОДЛИННОСТИ СЕТЕВЫХ СОЕДИНЕНИЙ (СЕАНСОВ ВЗАИМОДЕЙСТВИЯ), В ТОМ ЧИСЛЕ ДЛЯ ЗАЩИТЫ ОТ ПОДМЕНЫ СЕТЕВЫХ УСТРОЙСТВ И СЕРВИСОВ

Требования к реализации ЗИС.11: В информационной системе должно осуществляться обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (защита от атак типа «человек посередине»).

Для подтверждения подлинности сторон сетевого соединения (сеанса взаимодействия) и защиты сетевых устройств и сервисов от подмены должна осуществляться их аутентификация в соответствии с ИАФ.2 и ЗИС.10.

Контроль целостности передаваемой информации должен включать проверку целостности передаваемых пакетов (в частности в соответствии с ЗИС.3).

Требования к усилению ЗИС.11:

1) в информационной системе должно обеспечиваться признание идентификатора сеанса связи недействительным после окончания сетевого соединения;

2) в информационной системе должна осуществляться регистрация установления и разрыва сетевых соединений (сеансов взаимодействия) в целях выявления возможных инцидентов (событий безопасности);

3) в информационной системе должна осуществляться генерация и присвоение уникальных идентификаторов (одноразовых) для каждого сетевого соединения (сеанса взаимодействия) и контроль их подлинности

(восприниматься должны только идентификаторы, сгенерированные информационной системой);

4) в информационной системе должно обеспечиваться обнаружение попыток повторного использования идентификаторов сетевых соединений и реагирование на эти попытки;

5) в информационной системе должна осуществляться защита от подбора идентификаторов, присваиваемых будущим сетевым соединениям (сеансам взаимодействия).

Содержание базовой меры ЗИС.11:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.11			+	+
Усиление ЗИС.11				1

ЗИС.12 ИСКЛЮЧЕНИЕ ВОЗМОЖНОСТИ ОТРИЦАНИЯ ПОЛЬЗОВАТЕЛЕМ ФАКТА ОТПРАВКИ ИНФОРМАЦИИ ДРУГОМУ ПОЛЬЗОВАТЕЛЮ

Требования к реализации ЗИС.12: Оператором должно обеспечиваться исключение возможности отрицания пользователем факта отправки информации другому пользователю.

Для исключения возможности отрицания пользователем факта отправки информации другому пользователю должны осуществляться:

определение объектов или типов информации, для которых требуется обеспечение неотказуемости отправки (например, сообщения электронной почты);

обеспечение целостности информации при ее подготовке к передаче и непосредственной ее передаче по каналам связи в соответствии с ЗИС.3;

регистрация событий, связанных с отправкой информации другому пользователю в соответствии с РСБ.2.

Требования к усилению ЗИС.12:

1) в информационной системе должна обеспечиваться генерация свидетельства отправления информации (например, электронной подписи);

2) в информационной системе должна обеспечиваться связь атрибутов отправителя информации в соответствии с учетом ИАФ.1 и ИАФ.6 с полями отправляемой информации (текстом сообщения);

3) в информационной системе должна быть обеспечена возможность верификации (проверки) свидетельства отправления информации;

4) в информационной системе должна быть обеспечена возможность записи и защищенного хранения в течение установленного оператором времени информации, отправленной пользователем другому пользователю.

Содержание базовой мерыЗИС.12:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.12			+	+
Усиление ЗИС.12				

ЗИС.13 ИСКЛЮЧЕНИЕ ВОЗМОЖНОСТИ ОТРИЦАНИЯ ПОЛЬЗОВАТЕЛЕМ ФАКТА ПОЛУЧЕНИЯ ИНФОРМАЦИИ ОТ ДРУГОГО ПОЛЬЗОВАТЕЛЯ

Требования к реализации ЗИС.13: Оператором должно обеспечиваться исключение возможности отрицания пользователем факта получения информации от другого пользователя.

Для исключения возможности отрицания пользователем факта получения информации должны осуществляться:

определение объектов или типов информации, для которых требуется обеспечение неотказуемости получения (сообщения электронной почты);

обеспечение целостности полученной информации в соответствии с ЗИС.3;

регистрация событий, связанных с получением информации от другого пользователя в соответствии с РСБ.2.

Требования к усилению ЗИС.13:

1) в информационной системе должна обеспечиваться генерация свидетельства получения информации (запрос подтверждения получения или электронная подпись);

2) в информационной системе должна быть обеспечена связь атрибутов получателя информации в соответствии с ИАФ.1 и ИАФ.6 с полями отправляемой информации (текстом сообщения);

3) в информационной системе должна быть обеспечена возможность верификации (проверки) свидетельства получения информации;

4) в информационной системе должна быть обеспечена возможность записи и защищенного хранения в течение установленного оператором времени информации, полученной пользователем от другого пользователя.

Содержание базовой меры ЗИС.13:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.13			+	+
Усиление ЗИС.13				

ЗИС.14 ИСПОЛЬЗОВАНИЕ УСТРОЙСТВ ТЕРМИНАЛЬНОГО ДОСТУПА ДЛЯ ОБРАБОТКИ ИНФОРМАЦИИ

Требования к реализации ЗИС.14: Оператором для обработки информации в информационной системе должны применяться устройства терминального доступа, обладающие минимальными функциональными возможностями по обработке и хранению информации.

Применение устройств терминального доступа должно быть направлено на сосредоточение основных функций по обработке и хранению информации на серверах (в центрах обработки данных), уменьшение состава мер защиты информации, реализуемых на каждой рабочей станции, и перенос их реализации на серверы.

К таким устройствам относятся, в том числе, бездисковые рабочие станции, при использовании которых информация текущей сессии хранится в оперативной памяти или на защищенном съемном машинном носителе информации, устройства, поддерживающие технологию виртуального рабочего стола, и иные устройства.

Требования к усилению ЗИС.14:

Не установлены.

Содержание базовой меры ЗИС.14:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.14				
Усиление ЗИС.14				

ЗИС.15 ЗАЩИТА АРХИВНЫХ ФАЙЛОВ, ПАРАМЕТРОВ НАСТРОЙКИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНЫХ ДАННЫХ, НЕ ПОДЛЕЖАЩИХ ИЗМЕНЕНИЮ В ПРОЦЕССЕ ОБРАБОТКИ ИНФОРМАЦИИ

Требования к реализации ЗИС.15: В информационной системе должна обеспечиваться защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных данных, не подлежащих изменению в процессе обработки информации.

Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации, обеспечивается принятием мер защиты информации, определенных оператором в соответствии с настоящим методическим документом, направленных на обеспечение их конфиденциальности и целостности.

Защита данных, не подлежащих изменению в процессе обработки информации, обеспечивается в отношении информации, хранящейся на жестких магнитных дисках, дисковых накопителях и иных накопителях в информационной системе.

Требования к усилению ЗИС.15:

1) оператором для обеспечения конфиденциальности и целостности архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации, в соответствии с законодательством Российской Федерации применяются криптографические (шифровальные) средства защиты информации (данных);

2) использование неперезаписываемых носителей или носителей с защищенной областью памяти для размещения (хранения) параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации.

Содержание базовой меры ЗИС.15:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.15			+	+
Усиление ЗИС.15				

ЗИС.16 ВЫЯВЛЕНИЕ, АНАЛИЗ И БЛОКИРОВАНИЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ СКРЫТЫХ КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ В ОБХОД РЕАЛИЗОВАННЫХ МЕР ЗАЩИТЫ ИНФОРМАЦИИ ИЛИ ВНУТРИ РАЗРЕШЕННЫХ СЕТЕВЫХ ПРОТОКОЛОВ

Требования к реализации ЗИС.16: Оператором должны выполняться мероприятия по выявлению и анализу скрытых каналов передачи информации для определения параметров передачи информации, которые могут использоваться для скрытого хранения информации и скрытой передачи информации за пределы информационной системы.

Выявление, анализ и блокирование скрытых каналов передачи информации выполняется с учетом национальных стандартов:

ГОСТ Р 53113-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения;

ГОСТ Р 53113.2-2009 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.

Выявление и анализ скрытых каналов передачи информации осуществляется на этапах разработки и реализации системы защиты информации.

Требования к усилению ЗИС.16:

Не установлены.

Содержание базовой меры ЗИС.16:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.16				
Усиление ЗИС.16				

ЗИС.17 РАЗБИЕНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА СЕГМЕНТЫ (СЕГМЕНТИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ) И ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРИМЕТРОВ СЕГМЕНТОВ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Требования к реализации ЗИС.17: Оператором должно осуществляться разбиение информационной системы на сегменты (сегментирование

информационной системы) и обеспечиваться защита периметров сегментов информационной системы.

Сегментирование информационной системы проводится с целью построения многоуровневой (эшелонированной) системы защиты информации путем построения сегментов на различных физических доменах или средах. Принципы сегментирования информационной системы определяются оператором с учетом функциональных и технологических особенностей процесса обработки информации и анализа угроз безопасности информации и должны заключаться в снижении вероятности реализации угроз и (или) их локализации в рамках одного сегмента.

Сегментирование информационной системы также может проводиться с целью разделения информационной системы на сегменты, имеющие различные классы защищенности информационной системы.

При сегментировании информационной системы должна быть обеспечена защита периметров сегментов информационной системы в соответствии с УПД.3 и ЗИС.23.

Требования к усилению ЗИС.17:

1) оператором осуществляется выделение сегментов информационной системы для размещения общедоступной (публичной) информации:

а) путем выделения отдельных физических сетевых интерфейсов коммуникационного оборудования и (или) средств защиты периметра;

б) путем физической изоляции сегментов информационной системы для размещения общедоступной (публичной) информации.

Содержание базовой меры ЗИС.17:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.17			+	+
Усиление ЗИС.17				

ЗИС.18 ОБЕСПЕЧЕНИЕ ЗАГРУЗКИ И ИСПОЛНЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ, ДОСТУПНЫХ ТОЛЬКО ДЛЯ ЧТЕНИЯ, И КОНТРОЛЬ ЦЕЛОСТНОСТИ ДАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Требования к реализации ЗИС.18: В информационной системе должно обеспечиваться:

выделение в составе операционной системы и прикладного программного обеспечения частей, немодифицируемых в процессе загрузки и выполнения, и размещение их на машинных носителях информации, доступных только для чтения;

загрузка и выполнение на средствах вычислительной техники, определяемых оператором, операционной системы с машинных носителей информации, доступных только для чтения;

загрузка и выполнение на средствах вычислительной техники прикладного программного обеспечения, определяемого оператором, с машинных носителей информации, доступных только для чтения.

В качестве машинных носителей информации, доступных только для чтения, рассматриваются, в том числе, оптические носители CD-R/DVD-R или иные аппаратные машинные носители информации, возможность перезаписи на которые исключена технологически.

Требования к усилению ЗИС.18:

1) в сегментах (компонентах) информационной системы, определяемых оператором, применяются неперезаписываемые (защищенные от записи) машинные носители информации, устойчивые к сбоям в программном обеспечении информационной системы и отключению питания;

2) оператором должен осуществляться контроль целостности программного обеспечения, записанного на машинные носители информации, доступные только для чтения, в соответствии с ОЦЛ.1.

Содержание базовой меры ЗИС.18:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.18				
Усиление ЗИС.18				

ЗИС.19 ИЗОЛЯЦИЯ ПРОЦЕССОВ (ВЫПОЛНЕНИЕ ПРОГРАММ) В ВЫДЕЛЕННОЙ ОБЛАСТИ ПАМЯТИ

Требования к реализации ЗИС.19: В информационной системе должна осуществляться изоляция процессов (выполнение программ) в выделенной области памяти.

Изоляция процессов (выполнение программ) в выделенной области памяти должна обеспечивать недоступность областей памяти, используемых процессами (программами) выполняемыми от имени одного пользователя (учетной записи), для процессов (программ), исполняемых от имени другого пользователя (учетной записи).

Изоляция процессов (выполнение программ) в выделенной области памяти реализуется в средствах вычислительной техники, определенных оператором, и как минимум должна включать изоляцию процессов, связанных с выполнением функций безопасности средств защиты информации.

Требования к усилению ЗИС.19:
Не установлены.

Содержание базовой меры ЗИС.19:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.19				
Усиление ЗИС.19				

ЗИС.20 ЗАЩИТА БЕСПРОВОДНЫХ СОЕДИНЕНИЙ, ПРИМЕНЯЕМЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Требования к реализации ЗИС.20: Оператором должна быть обеспечена защита беспроводных соединений, применяемых в информационной системе. Защита беспроводных соединений включает:

ограничение на использование в информационной системе беспроводных соединений (в частности 802.11xWi-Fi, 802.15.1 Bluetooth, 802.22WRAN, IrDA и иных беспроводных соединений) в соответствии с задачами (функциями) информационной системы, для решения которых такие соединения необходимы;

предоставление доступа к параметрам(изменению параметров) настройки беспроводных соединений только администраторам информационной системы;

обеспечение возможности реализации беспроводных соединений только через контролируемые интерфейсы (в том числе, путем применения средств защиты информации);

регистрация и анализ событий, связанных с использованием беспроводных соединений, в том числе для выявления попыток несанкционированного подключения к информационной системе через беспроводные соединения.

При обеспечении защиты беспроводных соединений в зависимости от их типов должны реализовываться меры по идентификации и аутентификации в соответствии с ИАФ.1, ИАФ.2 и ИАФ.6.

При невозможности исключения установления беспроводных соединений из-за пределов контролируемой зоны должны приниматься меры защищенного удаленного доступа в соответствии с УПД.13 и ЗИС.3.

Правила и процедуры применения беспроводных соединений регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗИС.20:

1) оператором для защиты беспроводных соединений в соответствии с законодательством Российской Федерации должны применяться средства криптографической защиты информации;

2) в информационной системе должны применяться программно-технические средства обнаружения, анализа и блокирования несанкционированного использования беспроводных технологий и подключений к информационной системе;

3) оператором должно обеспечиваться блокирование несанкционированных беспроводных подключений к информационной системе;

4) оператором должна быть исключена возможность установления беспроводных соединений из-за пределов контролируемой зоны.

Содержание базовой меры ЗИС.20:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.20		+	+	+
Усиление ЗИС.20				

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

Требования к реализации ЗИС.21: В информационной системе должен быть исключен доступ пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства, ресурсы файловой системы и иные общие для пользователей ресурсы информационной системы.

Исключение доступа к информации через общие для пользователей ресурсы должно обеспечивать запрет доступа текущему пользователю (учетной записи) или текущему процессу к системным ресурсам (реестрам, оперативной памяти, внешним запоминающим устройствам) при их повторном использовании, в которых хранится информация другого (предыдущего) пользователя.

Требования к усилению ЗИС.21:

1) в информационной системе должна быть исключена возможность использованияв качестве общих для пользователей ресурсов информационной системы, которые используются как интерфейс (память, однонаправленные

интерфейсы (устройства) и сетевые карты) взаимодействия (связи) с системами, имеющими другие классы защищенности.

Содержание базовой меры ЗИС.21:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.21				+
Усиление ЗИС.21				

ЗИС.22 ЗАЩИТА ИНФОРМАЦИОННОЙ СИСТЕМЫ ОТ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, НАПРАВЛЕННЫХ НА ОТКАЗ В ОБСЛУЖИВАНИИ ЭТОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Требования к реализации ЗИС.22: В информационной системе должна обеспечиваться защита от угроз безопасности информации, направленных на отказ в обслуживании этой системы.

Оператором должен быть определен перечень угроз (типов угроз) безопасности информации, направленных на отказ в обслуживании.

Защита от угроз безопасности информации, направленных на отказ в обслуживании, осуществляется посредством реализации в информационной системе мер защиты информационной системы в соответствии с ЗИС.23 и повышенными характеристиками производительности телекоммуникационного оборудования и каналов передачи совместно с резервированием информации и технических средств, программного обеспечения, каналов передачи информации в соответствии с ОДТ.2, ОДТ.4 и ОДТ.5.

Требования к усилению ЗИС.22:

1) в информационной системе обеспечивается ограничение возможностей пользователей по реализации угроз безопасности информации, направленных на отказ в обслуживании, в отношении отдельных сегментов информационной системы и других информационных систем;

2) в информационной системе обеспечивается управление характеристиками производительности телекоммуникационного оборудования и каналов передачи информации в зависимости от интенсивности реализации угроз безопасности информации, направленных на отказ в обслуживании;

3) оператором в установленном порядке обеспечивается использование услуг сторонних организаций (провайдеров) по «очистке» входящего трафика (для сброса потока пакетов, используемых нарушителем для реализации угроз безопасности, направленных на отказ в обслуживании этой информационной системы);

4) оператором обеспечивается применение средств защиты информации, предназначенных для нейтрализации угроз безопасности, направленных на отказ в обслуживании;

5) в информационной системе меры защиты от угроз безопасности информации, направленных на отказ в обслуживании, должны обеспечить возможность защиты от соответствующих атак на информационную систему без воздействия на трафик сети (подсети), в которой функционирует информационная система;

6) оператором обеспечивается возможность взаимодействия по вопросам защиты информации от угроз, направленных на отказ в обслуживании, со специальными системами уполномоченных органов с учетом требований по защите информации.

Содержание базовой меры ЗИС.22:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.22			+	+
Усиление ЗИС.22				

ЗИС.23 ЗАЩИТА ПЕРИМЕТРА (ФИЗИЧЕСКИХ И (ИЛИ) ЛОГИЧЕСКИХ ГРАНИЦ) ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРИ ЕЕ ВЗАИМОДЕЙСТВИИ С ИНЫМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ И ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫМИ СЕТЯМИ

Требования к реализации ЗИС.23: В информационной системе должна осуществляться защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, предусматривающая:

управление (контроль) входящими в информационную систему и исходящими из информационной системы информационными потоками на физической и (или) логической границе информационной системы (сегментов информационной системы);

обеспечение взаимодействия информационной системы и (или) ее сегментов с иными информационными системами и сетями только через сетевые интерфейсы, которые обеспечивают управление (контроль) информационными потоками с использованием средств защиты информации (управляемые (контролируемые) сетевые интерфейсы), установленных на физическом и (или) логическом периметре информационной системы или ее отдельных сегментов (маршрутизаторов, межсетевых экранов, коммутаторов,

прокси-серверов, шлюзов безопасности, средств построения виртуальных частных сетей и иных средств защиты информации).

Правила и процедуры защиты периметра информационной системы регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ЗИС.23:

1) в информационной системе должна быть обеспечена возможность размещения публичных общедоступных ресурсов (в частности общедоступный веб-сервер), взаимодействующих с информационной системой через отдельные физические управляемые (контролируемые) сетевые интерфейсы;

2) в информационной системе должно быть обеспечено предоставление доступа во внутренние сегменты информационной системы (демилитаризованную зону) из внешних информационных систем и сетей только через средства защиты периметра (за исключением внутренних сегментов, которые специально выделены для такого взаимодействия);

3) оператор должен ограничить количество точек доступа в информационную систему из внешних информационных систем и сетей до минимально необходимого числа для решения постановленных задач, а также обеспечивающего постоянный и всесторонний контроль входящих и исходящих информационных потоков;

4) оператором в информационной системе:

а) должен применяться отдельный физический управляемый (контролируемый) сетевой интерфейс для каждого внешнего телекоммуникационного сервиса;

б) должны быть установлены правила управления информационными потоками для каждого физического управляемого (контролируемого) сетевого интерфейса;

в) должна обеспечиваться защита информации при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны (при необходимости), путем применения организационно-технических мер или криптографических методов в соответствии с законодательством Российской Федерации;

г) должно обеспечиваться обоснование и документирование всех исключений из правил управления информационными потоками, связанных с решением определенных задач в информационной системе, и определение продолжительности потребности таких исключений;

д) должно обеспечиваться удаление введенных исключений из правил управления информационными потоками после истечения установленного времени;

5) в информационной системе должен быть исключен выход (вход) через управляемые (контролируемые) сетевые интерфейсы информационных потоков по умолчанию (реализация принципа «запрещено все, что не разрешено»);

6) оператором обеспечивается запрет передачи информации за пределы периметра информационной системы при отказе (сбое) функционирования средств защиты периметра;

7) в информационной системе должна быть исключена возможность информационного взаимодействия мобильных и иных технических средств (устройств) с внешними информационными системами и информационно-телекоммуникационным сетям в процессе их удаленного подключения к защищаемой информационной системе с использованием средств построения виртуальных частных сетей;

8) в информационной системе обеспечивается сетевое соединение внутренних сегментов информационной системы (отдельных средств вычислительных техники), определенных оператором, с установленными им внешними информационными системами и сетями через прокси-серверы, размещенные совместно со средствами защиты периметра, обеспечивающие логирование (отслеживание) TCP-сессий, блокирование конкретных URL, доменных имен, IP-адресов и другим параметрам запросов к внешним информационным ресурсам;

9) в информационной системе исключается возможность выхода через управляемые (контролируемые) сетевые интерфейсы информационных потоков, содержащих вредоносное программное обеспечение (вирусы) или признаки компьютерных атак представляющих угрозу внешним информационным системам и сетям;

10) в информационной системе исключается возможность утечки информации через управляемые (контролируемые) сетевые интерфейсы путем точного соблюдения форматов протоколов, контроля использования стеганографии, отключения внешних сетевых интерфейсов, разборки и сборки пакетов данных, контроля отклонения типа и объема информационного потока от установленного профиля;

11) в информационной системе должна быть обеспечена проверка адреса источника информационного потока и адреса получателя информационного потока с целью подтверждения того, что информационное взаимодействие между этими адресами разрешено;

12) в информационной системе обеспечивается защита периметра с использованием шлюза безопасности на уровне узлов (хостов) для серверов, рабочих станций и мобильных технических средств;

13) в информационной системе обеспечивается сокрытие сетевых адресов используемых для управления средствами защиты периметра, информация о которых может быть получена через технологии определения устройств в сети (в частности систему доменных имен);

14) оператором обеспечивается отделение через отдельный физический управляемый (контролируемый) сетевой интерфейс функций безопасности и управления (администрирования) информационной системы, определенных оператором, от других (внутренних) компонентов информационной системы;

15) оператором обеспечивается исключение возможности несанкционированного физического сетевого подключения к управляемым

(контролируемым) сетевым интерфейсам (сетевым интерфейсам средств защиты периметра);

16) в информационной системе для контроля (анализа) защищенности доступ администраторов обеспечивается через выделенный отдельный физический управляемый (контролируемый) сетевой интерфейс;

17) оператором применяются автоматизированные средства, обеспечивающие строгое соблюдение формата сетевых протоколов на уровне приложений (проверка пакетов на предмет соблюдения спецификаций протокола на уровне приложений);

18) в информационной системе обеспечивается корректное завершение ее функционирования в случае нарушения функционирования (сбоя, отказов) средств защиты периметра;

19) в информационной системе при необходимости предоставлять доступ к ресурсам информационной системы должна быть организована демилитаризованная зона, содержащая доступные ресурсы.

20) в информационной системе должна быть обеспечена возможность размещения публичных общедоступных ресурсов (например, общедоступный веб-сервер), взаимодействующих с информационной системой через отдельные физические управляемые (контролируемые) сетевые интерфейсы.

Содержание базовой меры ЗИС.23:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.23			+	+
Усиление ЗИС.23			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

Требования к реализации ЗИС.24: В информационной системе должно осуществляться завершение сетевых соединений (например, открепление пары порт/адрес (TCP/IP)) по их завершении и (или) по истечении заданного оператором временного интервала неактивности сетевого соединения.

Требования к усилению ЗИС.24:

Не установлены.

Содержание базовой меры ЗИС.24:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.24			+	+
Усиление ЗИС.24				

ЗИС.25 ИСПОЛЬЗОВАНИЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ИЛИ ЕЕ СЕГМЕНТАХ РАЗЛИЧНЫХ ТИПОВ ОБЩЕСИСТЕМНОГО, ПРИКЛАДНОГО И СПЕЦИАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (СОЗДАНИЕ ГЕТЕРОГЕННОЙ СРЕДЫ)

Требования к реализации ЗИС.25: Проектировщиком при создании информационной должны применяться различные типы общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды).

Гетерогенная среда создается путем применения различных типов информационных технологий с целью ограничения возможностей потенциальных нарушителей по реализации угроз безопасности информации (по несанкционированному доступу к информации, внедрению вредоносного программного обеспечения (компьютерных вирусов) и по организации вторжений (проведению компьютерных атак)).

Создание гетерогенной среды может достигаться в частности применением на серверах информационной системы UNIX-подобных операционных систем, отличных от операционных систем, применяемых на автоматизированных рабочих местах типа Windows и (или) применением в смежных сетевых сегментах информационной системы разных типов сетевого общесистемного, прикладного и (или) специального программного обеспечения.

При создании гетерогенной среды необходимо учитывать повышение сложности в управлении конфигурацией информационной системы и возможность увеличения ошибок конфигурации и возможных уязвимостей.

Требования к усилению ЗИС.25:

Не установлены.

Содержание базовой меры ЗИС.25:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.25				
Усиление ЗИС.25				

ЗИС.26 ИСПОЛЬЗОВАНИЕ ПРИКЛАДНОГО И СПЕЦИАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИМЕЮЩЕГО ВОЗМОЖНОСТЬ ФУНКЦИОНИРОВАНИЯ НА РАЗЛИЧНЫХ ТИПАХ ОПЕРАЦИОННЫХ СИСТЕМ

Требования к реализации ЗИС.26: В информационной системе должно применяться прикладное и специальное программное обеспечение, имеющее возможность функционирования на различных типах операционных системах (независимое от вида операционной системы прикладное и специальное программное обеспечение).

Целью применения независимого от платформы операционной системы прикладного и специального программного обеспечения является обеспечение бесперебойного (штатного) функционирования прикладного (специального) программного обеспечения путем перевода его под управление операционной системы другого типа в случае реализации компьютерной атаки (возникновения инцидента) на основную операционную систему до восстановления безопасного функционирования информационной системы.

Применение независимого от типа (вида) операционной системы прикладного и специального программного обеспечения достигается в частности применением программного обеспечения, функционирование которого возможно как под управлением UNIX-подобных операционных систем, так и под управлением операционных систем типа Windows или иных операционных систем.

Перечень прикладного и специального программного обеспечения, имеющего возможность функционирования на различных типах операционных системах, определяется оператором.

Требования к усилению ЗИС.26:

Не установлены.

Содержание базовой меры ЗИС.26:

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ЗИС.26				
Усиление ЗИС.26				

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 № 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 № 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			+	+ 1

	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	+	+	+ 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		+	+ 1	+ 1

	информационной системе				
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 компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры			+	+ 1, 2
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			+ З	+ З
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			+ 1	+ 1, 2

	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 видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видео информации			+	+
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.