**Приложение 2**

**Методические рекомендации по реализации мер защиты информации на объектах критической информационной инфраструктуры (далее — методические рекомендации)**

Методические рекомендации детализируют организационные и технические меры защиты информации (далее — меры защиты информации), принимаемые на значимых объектах критической информационной инфраструктуры в соответствии с Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации (утв. приказом ФСТЭК России от 25.12.2017 № 239).

| **Обозначение и номер меры** | **Меры обеспечения безопасности значимого объекта** | **Требование к реализации меры обеспечения безопасности значимого объекта** | **Требование к усилению меры обеспечения безопасности значимого объекта** | **Источник** |
| --- | --- | --- | --- | --- |
| 1. **ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ** | | | | |
| ИАФ.0 | Регламентация правил и процедур идентификации и аутентификации | Субъект КИИ должен документировать политики и процедуры аутентификации и довести их до сведения всех пользователей, включая:  - рекомендации по выбору надежных учетных данных для аутентификации;  - рекомендации для пользователей по защите учетных данных для аутентификации;  - указания не использовать ранее использованные пароли;  - указания по смене пароля в случае подозрения на его компрометацию. |  | Стандарт PCI DSS п. 8.4 |
| ИАФ.1 | Идентификация и аутентификация пользователей и инициируемых ими процессов | В Значимом объекте КИИ должна обеспечиваться идентификация и аутентификация пользователей, являющихся работниками оператора.  При доступе в Значимый объект КИИ должна осуществляться идентификация и аутентификация пользователей, являющихся работниками Субъекта КИИ (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 Субъекта КИИ (пользователи, администраторы), выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств Значимого объекта КИИ в соответствии с должностными регламентами (инструкциями), утвержденными оператором, и которым В Значимом объекте КИИ присвоены учетные записи.  В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, заказчика, уполномоченного лица и (или) Субъекта КИИ, а также лица, привлекаемые на договорной основе для обеспечения функционирования Значимого объекта КИИ (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами Субъекта КИИ и которым в Значимом объекте КИИ также присвоены учетные записи.  Пользователи Значимого объекта КИИ должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации.  Аутентификация пользователя осуществляется с использованием паролей, аппаратных средств, биометрических характеристик, иных средств или в случае многофакторной (двухфакторной) аутентификации - определенной комбинации указанных средств.  В Значимом объекте КИИ 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. | 1) В Значимом объекте КИИ 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 Значимом объекте КИИ 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 Значимом объекте КИИ должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами привилегированных учетных записей (администраторов);  4) В Значимом объекте КИИ должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами непривилегированных учетных записей (пользователей);  5) В Значимом объекте КИИ 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 Значимого объекта КИИ, к которой осуществляется доступ;  6) В Значимом объекте КИИ должна обеспечиваться многофакторная (двухфакторная) аутентификация при доступе в систему с правами непривилегированных учетных записей (пользователей), где один из факторов обеспечивается устройством, отделенным от Значимого объекта КИИ, к которой осуществляется доступ;  7) В Значимом объекте КИИ должен использоваться механизм одноразовых паролей при аутентификации пользователей, осуществляющих удаленный или локальный доступ;  8) В Значимом объекте КИИ для аутентификации пользователей должно обеспечиваться применение в соответствии с законодательством Российской Федерации криптографических методов защиты информации. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ИАФ.2 | Идентификация и аутентификация устройств | В Значимом объекте КИИ до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация и аутентификация устройств (технических средств).  Субъектом КИИ должен быть определен перечень типов устройств, используемых в Значимом объекте КИИ и подлежащих идентификации и аутентификации до начала информационного взаимодействия.  Идентификация устройств в Значимом объекте КИИ 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 Значимом объекте КИИ 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 Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ 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. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ИАФ.3 | Управление идентификаторами | Субъектом КИИ должны быть установлены и реализованы следующие функции управления идентификаторами пользователей и устройств в Значимом объекте КИИ:   * 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 Субъектом КИИ периода времени; * блокирование идентификатора пользователя после установленного Субъектом КИИ времени неиспользования.   Правила и процедуры управления идентификаторами регламентируются в организационно-распорядительных документах Субъекта КИИ по защите информации. | 1) Субъектом КИИ 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 Значимого объекта КИИ;  2) Субъектом КИИ должно быть обеспечено блокирование идентификатора пользователя через период времени неиспользования:  а) не более 90 дней;  б) не более 45 дней;  3) Субъектом КИИ должно быть обеспечено использование различной аутентификационной информации (различных средств аутентификации) пользователя для входа в Значимый объект КИИ и доступа к прикладному (специальному) программному обеспечению;  4) Субъектом КИИ должно быть исключено использование идентификатора пользователя Значимого объекта КИИ при создании учетной записи пользователя публичной электронной почты или иных публичных сервисов;  5) Субъектом КИИ должно быть обеспечено управление идентификаторами внешних пользователей, учетные записи которых используются для доступа к общедоступным ресурсам Значимого объекта КИИ. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ИАФ.4 | Управление средствами аутентификации | Субъектом КИИ должны быть установлены и реализованы следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств в Значимом объекте КИИ:   * 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 Значимого объекта КИИ; * выдача средств аутентификации пользователям; * генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации); * установление характеристик пароля (при использовании в Значимом объекте КИИ механизмов аутентификации на основе пароля):   а) задание минимальной сложности пароля с определяемыми Субъектом КИИ 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 Субъектом КИИ 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 Субъекта КИИ по защите информации. | 1) в случае использования в Значимом объекте КИИ 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 Значимом объекте КИИ 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 Значимом объекте КИИ должно быть обеспечено использование серверов и (или) программного обеспечения аутентификации для единой аутентификации в компонентах Значимого объекта КИИ и компонентах программного обеспечения, предусматривающего собственную аутентификацию;  4) Субъект КИИ должен обеспечить получение (запросить) у поставщика технических средств и программного обеспечения Значимого объекта КИИ аутентификационную информацию, заданную производителем этих технических средств и программного обеспечения и не указанную в эксплуатационной документации;  5) Субъектом КИИ должны быть определены меры по исключению возможности использования пользователями их идентификаторов и паролей в других информационных системах. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ИАФ.5 | Идентификация и аутентификация внешних пользователей | В Значимом объекте КИИ должна осуществляться однозначная идентификация и аутентификация пользователей, не являющихся работниками Субъекта КИИ (внешних пользователей), или процессов, запускаемых от имени этих пользователей.  К пользователям, не являющимся работникам Субъекта КИИ (внешним пользователям), относятся все пользователи Значимого объекта КИИ, 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 Значимого объекта КИИ должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации.  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 Субъекта КИИ по защите информации. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ИАФ.6 | Двусторонняя аутентификация | В Значимом объекте КИИ 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. | 1) В Значимом объекте КИИ должна обеспечиваться аутентификация объектов файловой системы с использованием свидетельств подлинности информации (в том числе электронной подписи или иных свидетельств подлинности информации);  2) В Значимом объекте КИИ должна обеспечиваться аутентификация запускаемых и исполняемых модулей с использованием свидетельств подлинности модулей (в том числе цифровых сигнатур производителя или иных свидетельств подлинности модулей). | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ИАФ.7 | Защита аутентификационной информации при передаче | В Значимом объекте КИИ 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. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| 1. **УПРАВЛЕНИЕ ДОСТУПОМ** | | | | |
| УПД.0 | Регламентация правил и процедур управления доступом | Политика логического контроля доступа задокументирована и направлена на соблюдение следующих принципов:  «Служебная необходимость».  - Только операторам (конечным пользователям и администраторам), которым постоянно требуется доступ к зоне безопасности, разрешено иметь учетные записи в этой зоне.  - Полномочия присваиваются только оператору с подтвержденной необходимостью знания (например, настройка системы гарантирует, что операторы имеют доступ только к информации, файлам и системным ресурсам, необходимым для их определенных задач). Доступ к другим системным функциям отключен.  «Минимум полномочий».  - Настройка системы гарантирует, что права пользователя и администратора контролируются таким образом, чтобы все выданные им полномочия соответствовали индивидуальным потребностям.  - Учетные записи гарантируют только полномочия, необходимые для обычной, повседневной работы. Дополнительные полномочия предоставляются только на временной основе.  «Разграничение обязанностей» и «Четыре глаза».  - Документально оформленное руководство по разделению ролей находит отражение в специализированной документации разработчика.  - Ключевые обязанности разделены. Это означает, что некоторые роли не могут выполняться одними тем же лицом, например роли для отправки и подтверждения транзакций, роли администратора приложений и офицера безопасности, роли администратора сети и администратора операционной системы.  - Ключевые разрешения разделяются, чтобы обеспечить соблюдение принципа четырех глаз. |  | Стандарт SCSF п.5.1 буллет 1 |
| УПД.1 | Управление учетными записями пользователей | Субъектом КИИ 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 Значимом объекте КИИ; * предоставление пользователям прав доступа к объектам доступа Значимого объекта КИИ, основываясь на задачах, решаемых пользователями в Значимом объекте КИИ 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 Значимого объекта КИИ, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к Значимому объекту КИИ).  Правила и процедуры управления учетными записями пользователей регламентируются в организационно-распорядительных документах Субъекта КИИ по защите информации. | 1) Субъектом КИИ должны использоваться автоматизированные средства поддержки управления учетными записями пользователей;  2) В Значимом объекте КИИ должно осуществляться автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования;  3) В Значимом объекте КИИ должно осуществляться автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования:  а) более 90 дней;  б) более 45 дней;  4) В Значимом объекте КИИ 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 Значимом объекте КИИ должен осуществляться автоматический контроль заведения, активации, блокирования и уничтожения учетных записей пользователей и оповещение администраторов о результатах автоматического контроля. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| УПД.2 | Реализация модели управления доступом | В Значимом объекте КИИ для управления доступом субъектов доступа к объектам доступа должны быть реализованы установленные Субъектом КИИ 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 Значимого объекта КИИ, 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 Субъектом КИИ 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 Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ правила разграничения доступа должны обеспечивать управление доступом субъектов при входе в Значимый объект КИИ;  2) В Значимом объекте КИИ правила разграничения доступа должны обеспечивать управление доступом субъектов к техническим средствам, устройствам, внешним устройствам;  3) В Значимом объекте КИИ правила разграничения доступа должны обеспечивать управление доступом субъектов к объектам, создаваемым общесистемным (общим) программным обеспечением;  4) В Значимом объекте КИИ правила разграничения доступа должны обеспечивать управление доступом субъектов к объектам, создаваемым прикладным и специальным программным обеспечением. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| УПД.3 | Доверенная загрузка | В Значимом объекте КИИ должно обеспечиваться исключение несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники Значимого объекта КИИ 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 Значимом объекте КИИ 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 Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ должна осуществляться доверенная загрузка уровня базовой системы ввода-вывода или уровня платы расширения;  2) В Значимом объекте КИИ должна осуществляться доверенная загрузка уровня базовой системы ввода-вывода или уровня платы расширения, реализованные на основе программно-аппаратного модуля;  3) В Значимом объекте КИИ должна осуществляться доверенная загрузка программного обеспечения телекоммуникационного оборудования; | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| УПД.4 | Разделение полномочий (ролей) пользователей | Субъектом КИИ должно быть обеспечено разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование Значимого объекта КИИ, в соответствии с их должностными обязанностями (функциями), фиксирование в организационно-распорядительных документах по защите информации (документирование) полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование Значимого объекта КИИ, и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей). | 1) Субъектом КИИ должно быть обеспечено выполнение каждой роли по обработке информации, администрированию Значимого объекта КИИ, ее системы защиты информации, контролю (мониторингу) за обеспечением уровня защищенности информации, обеспечению функционирования Значимого объекта КИИ отдельным должностным лицом;  2) Субъектом КИИ должно быть обеспечено исключение наделения одного должностного лица полномочиями (ролью) по обработке информации и полномочиями (ролью) по администрированию Значимого объекта КИИ и (или) его системы защиты информации, контролю (мониторингу) за обеспечением уровня защищенности информации, обеспечению функционирования Значимого объекта КИИ;  3) Субъектом КИИ должно быть обеспечено исключение наделения одного должностного лица полномочиями (ролью) по контролю (мониторингу) за обеспечением уровня защищенности информации и полномочиями (ролью) по администрированию Значимого объекта КИИ и (или) его системы защиты информации и обеспечению функционирования Значимого объекта КИИ;  4) Субъектом КИИ должно быть обеспечено исключение наделения одного должностного лица полномочиями (ролью) по администрированию системы защиты информации Значимого объекта КИИ и полномочиями (ролью) по обеспечению функционирования Значимого объекта КИИ;  5) Субъектом КИИ должен быть определен администратор, имеющий права по передаче полномочий по администрированию Значимого объекта КИИ и системы защиты информации другим лицам и осуществляющий контроль за использованием переданных полномочий (супервизор). | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| УПД.5 | Назначение минимально необходимых прав и привилегий | Субъектом КИИ должно быть обеспечено назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование Значимого объекта КИИ, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями.  Субъектом КИИ 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. | 1) Субъектом КИИ 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). | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| УПД.6 | Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему | В Значимом объекте КИИ должно быть установлено и зафиксировано в организационно-распорядительных документах Субъекта КИИ по защите информации (задокументировано) ограничение количества неуспешных попыток входа в Значимый объект КИИ (доступа к Значимому объекту КИИ) 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 Значимый объект КИИ (доступа к Значимому объекту КИИ).  Ограничение количества неуспешных попыток входа в Значимый объект КИИ (доступа к Значимому объекту КИИ) должно обеспечиваться в соответствии с ИАФ.4. | 1) В Значимом объекте КИИ обеспечивается автоматическое блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в Значимый объект КИИ (доступа к Значимому объекту КИИ) за установленный период времени с возможностью разблокирования только администратором или иным лицом, имеющим соответствующие полномочия (роль);  2) В Значимом объекте КИИ обеспечивается автоматическое удаление информации с мобильного технического средства, входящего в состав Значимого объекта КИИ, при превышении допустимого числа неуспешных попыток входа в Значимый объект КИИ (доступа к Значимому объекту КИИ) за установленный период времени, осуществляемых с мобильного устройства;  3) В Значимом объекте КИИ обеспечивается противодействие автоматизированному подбору паролей с использованием однократных кодов, требующих визуального распознавания (в том числе с использованием технологии CAPTCHA). | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| УПД.7 | Предупреждение пользователя при его доступе к информационным ресурсам | В Значимом объекте КИИ должно быть обеспечено предупреждение пользователя в виде сообщения ("окна") при его входе в Значимый объект КИИ (до процесса аутентификации) о том, что в Значимом объекте КИИ реализованы меры защиты информации, а также о том, что при работе в Значимом объекте КИИ пользователем должны быть соблюдены установленные Субъектом КИИ правила и ограничения на работу с информацией.  Вход в Значимый объект КИИ и предоставление пользователю возможности работы в Значимом объекте КИИ осуществляются только после подтверждения пользователем ознакомления с предупреждением. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| УПД.8 | Оповещение пользователя при успешном входе о предыдущем доступе к информационной (автоматизированной) системе | В Значимом объекте КИИ должно быть обеспечено после успешного входа пользователя в Значимый объект КИИ (завершения процесса аутентификации) оповещение этого пользователя о дате и времени предыдущего входа в Значимый объект КИИ от имени этого пользователя. | 1) В Значимом объекте КИИ обеспечивается оповещение пользователя после успешного входа в Значимый объект КИИ о количестве неуспешных попыток входа в Значимый объект КИИ (доступа к Значимому объекту КИИ), зафиксированных с момента последнего успешного входа в Значимый объект КИИ;  2) В Значимом объекте КИИ обеспечивается оповещение пользователя после успешного входа в Значимый объект КИИ о количестве успешных и (или) неуспешных попыток входа в Значимый объект КИИ (доступа к Значимому объекту КИИ), зафиксированных за период времени не менее 7 дней;  3) В Значимом объекте КИИ обеспечивается оповещение пользователя после успешного входа в Значимый объект КИИ 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 Значимый объект КИИ. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| УПД.9 | Ограничение числа параллельных сеансов доступа | В Значимом объекте КИИ должно обеспечиваться ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя Значимого объекта КИИ.  В Значимом объекте КИИ 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 Значимого объекта КИИ в целом, для отдельных сегментов Значимого объекта КИИ, для групп пользователей, отдельных пользователей или их комбинаций.  Ограничения числа параллельных сеансов доступа регламентируются в организационно-распорядительных документах Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ 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 Значимом объекте КИИ 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 Значимом объекте КИИ должны быть предусмотрены программно-технические средства, позволяющие контролировать и отображать администратору число активных параллельных (одновременных) сеансов (сессий) для каждой учетной записи пользователей;  4) В Значимом объекте КИИ 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. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| УПД.10 | Блокирование сеанса доступа пользователя при неактивности | В Значимом объекте КИИ должно обеспечиваться блокирование сеанса доступа пользователя после установленного Субъектом КИИ времени его бездействия (неактивности) в Значимом объекте КИИ или по запросу пользователя.  Блокирование сеанса доступа пользователя в Значимый объект КИИ обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к Значимому объекту КИИ (без выхода из Значимого объекта КИИ).  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 Значимый объект КИИ 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 Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ обеспечивается блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя:  а) до 15 минут;  б) до 5 минут;  2) В Значимом объекте КИИ 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 Значимом объекте КИИ обеспечивается завершение сеанса пользователя (выхода из системы) после превышения установленного Субъектом КИИ времени бездействия (неактивности) пользователя. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| УПД.11 | Управление действиями пользователей до идентификации и аутентификации | Субъектом КИИ 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 Значимого объекта КИИ 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 Субъекта КИИ по защите информации. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| УПД.12 | Управление атрибутами безопасности | В Значимом объекте КИИ 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 Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ обеспечивается динамическое изменение атрибутов безопасности в соответствии с организационно-распорядительными документами по защите информации Субъекта КИИ в зависимости от процесса обработки информации (формирование, объединение, разделение информационных ресурсов);  2) В Значимом объекте КИИ допускается изменение атрибутов безопасности только авторизованными пользователям или процессами;  3) В Значимом объекте КИИ обеспечивается автоматизированный контроль связи атрибутов безопасности с информацией;  4) В Значимом объекте КИИ 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). | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| УПД.13 | Реализация защищенного удаленного доступа | Субъектом КИИ должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа Значимого объекта КИИ 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 Значимого объекта КИИ; * ограничение на использование удаленного доступа в соответствии с задачами (функциями) Значимого объекта КИИ, 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 Значимого объекта КИИ; * контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа Значимого объекта КИИ до начала информационного взаимодействия с Значимым объектом КИИ (передачи защищаемой информации).   Правила и процедуры применения удаленного доступа регламентируются в организационно-распорядительных документах Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ для мониторинга и контроля удаленного доступа должны применяться автоматизированные средства (дополнительные программные или программно-технические средства);  2) В Значимом объекте КИИ используется ограниченное (минимально необходимое) количество точек подключения к Значимому объекту КИИ при организации удаленного доступа к объектам доступа Значимого объекта КИИ;  3) В Значимом объекте КИИ исключается удаленный доступ от имени привилегированных учетных записей (администраторов) для администрирования Значимого объекта КИИ и ее системы защиты информации;  4) В Значимом объекте КИИ при удаленном доступе обеспечивается применение в соответствии с законодательством Российской Федерации криптографических методов защиты информации;  5) В Значимом объекте КИИ обеспечивается мониторинг и контроль удаленного доступа на предмет выявления установления несанкционированного соединения технических средств (устройств) с Значимым объектом КИИ;  6) В Значимом объекте КИИ должен обеспечиваться запрет удаленного доступа с использованием сетевых технологий и протоколов, определенных Субъектом КИИ по результатам анализа защищенности как небезопасных. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| УПД.14 | Контроль доступа из внешних информационных (автоматизированных) систем | Субъектом КИИ 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 Значимого объекта КИИ.  Управление взаимодействием с внешними информационными системами должно включать:   * предоставление доступа к Значимому объекту КИИ только авторизованным (уполномоченным) пользователям в соответствии с УПД.2; * определение типов прикладного программного обеспечения Значимого объекта КИИ, 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 Значимому объекту КИИ 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 Субъекта КИИ по защите информации. | 1) Субъект КИИ предоставляет доступ к Значимому объекту КИИ авторизованным (уполномоченным) пользователям внешних информационных систем или разрешает обработку, хранение и передачу информации с использованием внешней Значимого объекта КИИ при выполнении следующих условий:  а) при наличии договора (соглашения) об информационном взаимодействии с Субъектом КИИ (обладателем, владельцем) внешней Значимого объекта КИИ;  б) при наличии подтверждения выполнения во внешней Значимому объекту КИИ предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения). | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| 1. **ОГРАНИЧЕНИЕ ПРОГРАММНОЙ СРЕДЫ** | | | | |
| ОПС.0 | Регламентация правил и процедур ограничения программной среды | Субъектом КИИ должны быть разработаны и утверждены:   * политика ограничения программной среды; * процедуры, обеспечивающие осуществление политики ограничения программной среды и соответствующих механизмов ограничения программной среды. |  | NIST Special Publication 800-53 Revision 5 |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения | Субъектом КИИ 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 Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ обеспечивается разрешение запуска только тех программных компонентов, которые явно разрешены администратором безопасности;  2) В Значимом объекте КИИ обеспечивается использование средств автоматизированного контроля перечня (списка) компонентов программного обеспечения, запускаемого автоматически при загрузке операционной системы средства вычислительной техники;  3) В Значимом объекте КИИ обеспечивается использование автоматизированных механизмов управления запуском (обращениями) компонентов программного обеспечения;  4) В Значимом объекте КИИ 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 Значимом объекте КИИ обеспечивается управление временем запуска и завершения работы компонентов программного обеспечения (например, ограничение запуска только в течение рабочего дня);  6) В Значимом объекте КИИ 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 Значимом объекте КИИ обеспечивается контроль обновления запускаемых компонентов программного обеспечения;  8) В Значимом объекте КИИ обеспечивается регистрация событий, связанных с контролем состояния и обновлением запускаемых компонентов программного обеспечения;  9) В Значимом объекте КИИ обеспечивается запрет (блокирование) запуска определенных Субъектом КИИ компонентов программного обеспечения, не прошедших аутентификацию в соответствии с ИАФ.7. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения | Субъектом КИИ должны быть реализованы следующие функции по управлению установкой (инсталляцией) компонентов программного обеспечения Значимого объекта КИИ:   * определение компонентов программного обеспечения (состава и конфигурации), подлежащих установке в Значимом объекте КИИ 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 Значимого объекта КИИ (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 невключение 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 Значимого объекта КИИ, 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 Субъекта КИИ по защите информации с учетом эксплуатационной документации. | 1) В Значимом объекте КИИ должно обеспечиваться использование средств автоматизации для применения и контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации;  2) В Значимом объекте КИИ 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 Значимом объекте КИИ должно обеспечиваться использование средств автоматизации для инсталляции и централизованного управления процессами инсталляции, в том числе с применением пакетов соответствующих дистрибутивов программного обеспечения. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ОПС.3 | Управление временными файлами | В Значимом объекте КИИ 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).  Субъектом КИИ должен быть определен и зафиксирован в организационно-распорядительной документации по защите информации (задокументирован) порядок очистки (стирания) временных файлов. | 1) В Значимом объекте КИИ должны осуществляться:  а) контроль доступа к временным файлам;  б) удаление временных файлов по завершении сеанса работы с ними. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| 1. **ЗАЩИТА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ** | | | | |
| ЗНИ.0 | Регламентация правил и процедур защиты машинных носителей информации | Должны быть реализованы процедуры по управлению сменными носителями информации в соответствии с принятой Субъектом КИИ системой категорирования информации.  Руководство по применению  Необходимо рассмотреть следующие рекомендации в отношении управления съемными носителями:  Для управления съемными носителями должны быть учтены следующие рекомендации:  содержимое, в котором отпала необходимость, на a) любых перезаписываемых носителях, которые могут быть вынесены из организации, должно быть удалено без возможности восстановления;  b) где это необходимо и целесообразно, должно требоваться разрешение на вынос носителей информации из организации, а записи о выносе следует хранить как контрольную запись для аудита;  c) все носители должны храниться в безопасном, надежном месте в соответствии с инструкциями производителей;  d) если конфиденциальность или целостность данных являются важными факторами, следует использовать криптографические методы для защиты данных на съемных носителях;  e) для снижения риска деградации носителей, когда сохраняемые данные все еще необходимы, данные должны быть перенесены на новые носители, прежде чем они станут нечитаемыми;  f) несколько копий ценных данных должны храниться на отдельных носителях для снижения риска случайного повреждения или потери данных;  g) для уменьшения возможности потери данных должна быть предусмотрена регистрация съемных носителей информации;  h) съемные диски разрешается использовать только в случаях, обусловленных потребностями бизнеса;  i) в случае необходимости использования съемных носителей, перенос информации на них должен контролироваться.  Все процедуры и уровни авторизации должны быть задокументированы. |  | Стандарт ISO 27001 п. A8.3.1 |
| ЗНИ.1 | Учет машинных носителей информации | Субъектом КИИ должен быть обеспечен учет машинных носителей информации, используемых в Значимом объекте КИИ 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 Значимого объекта КИИ 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). | 1) Субъектом КИИ обеспечивается маркировка машинных носителей информации (технических средств), дополнительно включающая:  а) информацию о возможности использования машинного носителя информации вне Значимого объекта КИИ;  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) Субъектом КИИ 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) Субъектом КИИ обеспечиваться маркировка машинных носителей информации (технических средств), дополнительно включающая использование механизмов распознавания (идентификации) носителя информации по его уникальным физическим характеристикам. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗНИ.2 | Управление физическим доступом к машинным носителям информации | Субъектом КИИ должны быть реализованы следующие функции по управлению доступом к машинным носителям информации, используемым в Значимом объекте КИИ:   * 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 Субъекта КИИ по защите информации. | 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 Значимом объекте КИИ 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. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗНИ.3 | Контроль перемещения машинных носителей информации за пределы контролируемой зоны | Субъектом КИИ должен обеспечиваться контроль перемещения используемых в Значимом объекте КИИ 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 (функций); * 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 Субъекта КИИ по защите информации. | 1) Субъектом КИИ 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) Субъектом КИИ определяется должностное лицо, ответственное за перемещение машинных носителей информации;  4) Субъектом КИИ Значимого объекта КИИ осуществляется периодическая проверка машинных носителей информации после их возврата в пределы контролируемой зоны. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗНИ.4 | Исключение возможности несанкционированного чтения информации на машинных носителях информации | Субъектом КИИ 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 Субъекта КИИ по защите информации. | 1) Субъектом КИИ должны применяться средства контроля съемных машинных носителей информации;  2) Субъектом КИИ должны применяться в соответствии с законодательством Российской Федерации криптографические методы защиты информации, хранящейся на машинных носителях;  3) Субъектом КИИ должен быть определен перечень машинных носителей информации, подлежащих хранению в помещениях, специально предназначенных для хранения машинных носителей информации (хранилище машинных носителей информации). | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации | В Значимом объекте КИИ должен осуществляться контроль использования интерфейсов ввода (вывода).  Контроль использования (разрешение или запрет) интерфейсов ввода (вывода) должен предусматривать:   * определение Субъектом КИИ интерфейсов средств вычислительной техники, которые могут использоваться для ввода (вывода) информации, разрешенных и (или) запрещенных к использованию в Значимом объекте КИИ; * определение Субъектом КИИ 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 Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ должна быть обеспечена регистрация использования интерфейсов ввода (вывода) в соответствии с РСБ.3;  2) Субъектом КИИ обеспечивается конструктивное (физическое) исключение из средства вычислительной техники запрещенных к использованию интерфейсов ввода (вывода);  3) Субъектом КИИ Субъектом КИИ обеспечивается программное отключение запрещенных к использованию интерфейсов ввода (вывода). | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗНИ.6 | Контроль ввода (вывода) информации на съемные машинные носители информации | В Значимом объекте КИИ должен осуществляться контроль ввода (вывода) информации на машинные носители информации.  Контроль ввода (вывода) информации на машинные носители информации должен предусматривать:   * определение Субъектом КИИ типов носителей информации, ввод (вывод) информации на которые подлежит контролю; * определение Субъектом КИИ 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 Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ должна создаваться копия информации, записываемой пользователями на съемные машинные носители информации (теневое копирование);  2) Субъектом КИИ должны применяться средства контроля подключения съемных машинных носителей информации. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗНИ.7 | Контроль подключения съемных машинных носителей | В Значимом объекте КИИ должен обеспечиваться контроль подключения машинных носителей информации.  Контроль подключения машинных носителей информации должен предусматривать:   * определение Субъектом КИИ типов носителей информации, подключение которых к Значимому объекту КИИ разрешено в соответствии с УПД.2; * определение Субъектом КИИ категорий пользователей, которым предоставлены полномочия по подключению носителей к Значимому объекту КИИ в соответствии с УПД.2; * запрет подключения носителей информации, подключение которых к Значимому объекту КИИ не разрешено; * регистрация действий пользователей и событий по подключению к Значимому объекту КИИ носителей в соответствии с РСБ.3.   Правила и процедуры контроля подключения машинных носителей информации регламентируются в организационно-распорядительных документах Субъекта КИИ по защите информации. | 1) Субъектом КИИ 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 Значимому объекту КИИ носителей пользователями, не имеющими полномочий на подключение носителей. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗНИ. 8 | Уничтожение (стирание) информации на машинных носителях информации | Субъектом КИИ 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 Субъектом КИИ и включены в организационно-распорядительные документы по защите информации. | 1) Субъектом КИИ должны быть обеспечены регистрация и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации;  2) Субъектом КИИ должны проводиться периодическая проверка процедур и тестирование средств стирания информации и контроля удаления информации;  3) Субъектом КИИ перед подключением к Значимому объекту КИИ должно быть обеспечено уничтожение (стирание) информации с носителей информации после их приобретения и при первичном подключении к Значимому объекту КИИ, 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) Субъектом КИИ должно быть обеспечено уничтожение машинных носителей информации, которые не подлежат очистке (неперезаписываемые машинные носители информации, такие как оптические диски типа CD-R);  5) Субъектом КИИ 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;  6) 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). | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| 1. **АУДИТ БЕЗОПАСНОСТИ** | | | | |
| АУД.0 | Регламентация правил и процедур аудита безопасности | Мера обеспечения ИБ  Требования к процессу регистрации событий [аудиту] и деятельности, связанной с контролем находящихся в эксплуатации систем, должны быть тщательно спланированы и согласованы для минимизации сбоев в бизнес-процессах.  Руководство по применению  Необходимо придерживаться следующих рекомендаций:  требования доступа к системам и данным для проведения a) аудита должны быть согласованы с соответствующим руководством;  b) область действия технического аудита должна быть согласована и проконтролирована;  c) аудиторские тесты должны быть ограничены доступом уровня «только на чтение» в отношении программного обеспечения и данных;  d) доступ, отличный от режима «только на чтение», должен быть разрешен только для изолированных копий системных файлов, которые должны быть уничтожены по завершению аудита или обеспечены соответствующей защитой, если существует необходимость сохранять такие файлы в соответствии с требованиями документации по аудиту;  e) требования к специальной и дополнительной обработке должны быть идентифицированы и согласованы;  f) доступность системы, следует проводить в нерабочее время;  g) любой доступ должен контролироваться и регистрироваться для создания прослеживаемости. |  | Стандарт ISO 27002 п.12.7.1 |
| АУД.1 | Инвентаризация информационных ресурсов | Мера обеспечения ИБ  Информация, средства обработки информации и другие активы, связанные с информацией, должны быть идентифицированы, а также должен быть составлен и поддерживаться в актуальном состоянии перечень этих активов.  Руководство по применению  Организация должна идентифицировать активы, относящиеся к жизненному циклу информации, и задокументировать их значимость. Жизненный цикл информации должен включать в себя создание, обработку, хранение, передачу, удаление и уничтожение. Документация должна храниться в специально созданных или уже существующих перечнях, в зависимости от ситуации.  Перечень активов должен быть точным, актуальным, полным и согласованным с другими инвентаризационными перечнями.  Для каждого актива, включенного в перечень, должен быть определен его владелец (см. 0) и проведено категорирование (см. 0).  Дополнительная информация  Инвентаризация активов помогает обеспечить эффективную защиту и может также потребоваться для других целей, таких как здоровье и безопасность, страхование или финансы (управление активами).  ИСО/МЭК 27005 [11] предоставляет примеры активов, которые могут быть приняты во внимание Субъектом КИИ в процессе идентификации активов. Процесс составления перечня активов является важной предпосылкой управления рисками (см. также ИСО/МЭК 27000 и ИСО/МЭК 27005 [11]). |  | Стандарт ISO 27002 п.8.1.1 |
| АУД.2 | Анализ уязвимостей и их устранение | Субъектом КИИ должны осуществляться выявление (поиск), анализ и устранение уязвимостей в Значимом объекте КИИ.  При выявлении (поиске), анализе и устранении уязвимостей в Значимом объекте КИИ 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 Субъекта КИИ (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 Значимого объекта КИИ. 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 Значимом объекте КИИ.  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 Значимого объекта КИИ), направленные на устранение возможности использования выявленных уязвимостей.  Субъектом КИИ 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 Субъекта КИИ по защите информации. | 1) Субъектом КИИ 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 Значимого объекта КИИ на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей;  2) Субъект КИИ должен уточнять перечень сканируемых в Значимом объекте КИИ уязвимостей с установленной им периодичностью, а также после появления информации о новых уязвимостях;  3) Субъектом КИИ определяется информация об Значимому объекту КИИ, 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) Субъектом КИИ предоставляется доступ только администраторам к функциям выявления (поиска) уязвимостей (предоставление такой возможности только администраторам безопасности);  5) Субъектом КИИ применяются автоматизированные средства для сравнения результатов сканирования уязвимостей в разные периоды времени для анализа изменения количества и классов (типов) уязвимостей в Значимом объекте КИИ;  6) Субъектом КИИ применяются автоматизированные средства для обнаружения в Значимом объекте КИИ неразрешенного программного обеспечения (компонентов программного обеспечения) и уведомления об этом уполномоченных должностных лиц (администратора безопасности);  7) Субъектом КИИ проводится анализ журналов регистрации событий безопасности (журнала аудита) в целях определения, были ли выявленные уязвимости ранее использованы в Значимом объекте КИИ для нарушения безопасности информации;  8) Субъектом КИИ обеспечивается проведение выявления уязвимостей "нулевого дня", о которых стало известно, но информация о которых не включена в сканеры уязвимостей;  9) Субъектом КИИ обеспечивается проведение выявления новых уязвимостей, информация о которых не опубликована в общедоступных источниках;  10) Субъектом КИИ должно осуществляться выявление (поиск) уязвимостей в Значимом объекте КИИ с использованием учетных записей на сканируемых ресурсах;  11) Субъектом КИИ должно использоваться тестирование Значимого объекта КИИ на проникновение. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| АУД.3 | Генерирование временных меток и (или) синхронизация системного времени | В Значимом объекте КИИ 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 Значимом объекте КИИ достигается посредством применения внутренних системных часов Значимого объекта КИИ. | 1) Субъектом КИИ должен быть определен источник надежных меток времени; в Значимом объекте КИИ должна выполняться синхронизация системного времени с периодичностью, определенной оператором. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| АУД.4 | Регистрация событий безопасности | Субъектом КИИ должны быть определены события безопасности в Значимом объекте КИИ, подлежащие регистрации, и сроки их хранения.  События безопасности, подлежащие регистрации в Значимом объекте КИИ, должны определяться с учетом способов реализации угроз безопасности для Значимого объекта КИИ. К событиям безопасности, подлежащим регистрации в Значимом объекте КИИ, должны быть отнесены любые проявления состояния Значимого объекта КИИ и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов Значимого объекта КИИ, нарушения процедур, установленных организационно-распорядительными документами по защите информации оператора, а также на нарушение штатного функционирования средств защиты информации.  События безопасности, подлежащие регистрации в Значимом объекте КИИ, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в Значимом объекте КИИ. Подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации в Значимом объекте КИИ.  Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется Субъектом КИИ исходя из возможностей реализации угроз безопасности информации и фиксируется в организационно-распорядительных документах по защите информации (документируется).  В Значимом объекте КИИ как минимум подлежат регистрации следующие события:   * вход (выход), а также попытки входа субъектов доступа в Значимый объект КИИ 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 Субъектом КИИ 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. | 1) Субъектом КИИ 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 Значимом объекте КИИ;  2) Субъектом КИИ в перечень событий безопасности, подлежащих регистрации, должны быть включены события, связанные с действиями от имени привилегированных учетных записей (администраторов);  3) Субъектом КИИ в перечень событий безопасности, подлежащих регистрации, должны быть включены события, связанные с изменением привилегий учетных записей;  4) Субъектом КИИ 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. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| АУД.5 | Контроль и анализ сетевого трафика | Использовать методы обнаружения и (или) предотвращения вторжений для обнаружения и (или) предотвращения вторжения в сеть. Осуществлять мониторинг всего сетевого трафика по периметру среды ДДК и в критичных точках внутри среды ДДК, и оповещать работников о подозрениях на компрометацию.  Поддерживать в актуальном состоянии системы обнаружения и предотвращения вторжений, их сигнатуры и правила. |  | Стандарт PCI DSS п.10.2 |
| АУД.6 | Защита информации о событиях безопасности | В Значимом объекте КИИ 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 Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ обеспечивается резервное копирование записей регистрации (аудита);  2) В Значимом объекте КИИ обеспечивается резервное копирование записей регистрации (аудита) на носители однократной записи (неперезаписываемые носители информации);  3) В Значимом объекте КИИ для обеспечения целостности информации о зарегистрированных событиях безопасности должны применяться в соответствии с законодательством Российской Федерации криптографические методы;  4) Субъект КИИ предоставляет доступ к записям регистрации событий безопасности (аудита) ограниченному кругу администраторов. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| АУД.7 | Мониторинг безопасности | Субъектом КИИ 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 Значимом объекте КИИ.  В случае выявление признаков инцидентов безопасности в Значимом объекте КИИ 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 Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ 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 Значимом объекте КИИ 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 Значимом объекте КИИ обеспечивается полнотекстовый анализ привилегированных команд;  4) Субъектом КИИ обеспечивается анализ записанных сетевых потоков (дампов). | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| АУД.8 | Реагирование на сбои при регистрации событий безопасности | В Значимом объекте КИИ 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 Значимого объекта КИИ, запись поверх устаревших хранимых записей событий безопасности.   Правила и процедуры реагирования на сбои при регистрации событий безопасности регламентируются в организационно-распорядительных документах Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ обеспечивается выдача предупреждения администратору при заполнении установленной Субъектом КИИ части (процент или фактическое значение) объема памяти для хранения информации о событиях безопасности;  2) В Значимом объекте КИИ обеспечивается выдача предупреждения администратору в масштабе времени, близком к реальному, при наступлении критичных сбоев в механизмах сбора информации, определенных оператором;  3) В Значимом объекте КИИ обеспечивается запрет обработки информации в случае аппаратных или программных ошибок, сбоев в механизмах сбора информации или достижения предела или переполнения объема (емкости) памяти. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| АУД.9 | Анализ действий отдельных пользователей | В Значимом объекте КИИ должна иметься возможность просмотра и анализа информации о действиях отдельных пользователей в Значимом объекте КИИ.  Сведения о действиях отдельных пользователей в Значимом объекте КИИ должны предоставляться уполномоченным должностным лицам для просмотра и анализа с целью расследования причин возникновения инцидентов в Значимом объекте КИИ в соответствии с законодательством Российской Федерации.  Правила и процедуры просмотра и анализа информации о действиях отдельных пользователей регламентируются в организационно-распорядительных документах Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ должна быть обеспечена возможность автоматизированной обработки записей регистрации (аудита) событий безопасности на основе критериев избирательности. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| АУД.10 | Проведение внутренних аудитов | Субъектом КИИ 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 Субъектом КИИ в организационно-распорядительных документах по защите информации. | 1) В Значимом объекте КИИ 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) Субъектом КИИ в случае обнаружения нарушений работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации должен обеспечиваться перевод Значимого объекта КИИ, сегмента или компонента Значимого объекта КИИ в режим ограничения обработки информации и (или) запрет обработки информации в Значимом объекте КИИ, сегменте или компоненте Значимого объекта КИИ до устранения нарушений;  3) Субъектом КИИ 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 Значимом объекте КИИ должно использоваться программное обеспечение, прошедшее контроль отсутствия недекларированных возможностей и отсутствия влияния на корректность работы средств защиты информации. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| АУД.11 | Проведение внешних аудитов | Мера обеспечения ИБ  Подход организации к менеджменту ИБ и ее реализация (т. е. цели, меры и средства, политики, процессы и процедуры ИБ) должны проверяться независимо друг от друга через запланированные интервалы времени или в случае значительных изменений.  Руководство по применению  Руководство должно инициировать проведение независимой проверки. Такая независимая проверка необходима для обеспечения постоянной пригодности, адекватности и эффективности подхода организации к управлению ИБ. Проверка должна включать оценку возможностей для улучшения и необходимости изменений в подходе к безопасности, включая задачи политики и мер обеспечения ИБ.  Такая проверка должна выполняться лицами, не связанными с проверяемой областью, например, теми, кто проводит внутренние аудиты, независимыми руководителями или сторонними организациями, специализирующимися на проведении таких проверок. Лица, проводящие проверки, должны иметь соответствующие навыки и опыт.  Результаты независимой проверки должны быть задокументированы и доведены до сведения руководства, которое инициировало проверку. Эти записи должны сохраняться.  Если независимая проверка выявляет, что подход организации и реализация управления ИБ недостаточны, например, документированные цели и требования не выполняются или не соответствуют направлению ИБ, установленному в политиках ИБ (см. Ошибка! Источник ссылки не найден.), руководство должно рассмотреть необходимость корректирующих действий.  Дополнительная информация  ИСО/МЭК 27007 [12] «Руководство по аудиту систем управления информационной безопасностью» и ИСО/МЭК TR 27008 [13] «Руководство для аудиторов по мерам обеспечения информационной безопасности» также представляют руководства для проведения независимой проверки. |  | Стандарт ISO 27001 п.18.2.1 |
| 1. **АНТИВИРУСНАЯ ЗАЩИТА** | | | | |
| АВЗ.0 | Регламентация правил и процедур антивирусной защиты | Гарантировать, что политики безопасности и операционные процедуры защиты систем от вредоносного ПО документированы, используются и известны всем заинтересованным лицам. |  | Стандарт PCI DSS п. 5.4 |
| АВЗ.1 | Реализация антивирусной защиты | Субъектом КИИ должна обеспечиваться антивирусная защита Значимого объекта КИИ, 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 Значимый объект КИИ, 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 Значимого объекта КИИ, которые должны быть подвергнуты проверке средством антивирусной защиты; * проведение периодических проверок компонентов Значимого объекта КИИ (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 Значимом объекте КИИ объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).   Правила и процедуры антивирусной защиты Значимого объекта КИИ регламентируются в организационно-распорядительных документах Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ должно обеспечиваться предоставление прав по управлению (администрированию) средствами антивирусной защиты администратору безопасности;  2) В Значимом объекте КИИ должно обеспечиваться централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий программного обеспечения средств антивирусной защиты) средствами антивирусной защиты, установленными на компонентах Значимого объекта КИИ (серверах, автоматизированных рабочих местах);  3) Субъектом КИИ должен обеспечиваться запрет использования съемных машинных носителей информации, которые могут являться источниками вредоносных компьютерных программ (вирусов);  4) В Значимом объекте КИИ должно обеспечиваться использование на разных уровнях Значимого объекта КИИ средств антивирусной защиты разных производителей;  5) В Значимом объекте КИИ должны обеспечиваться проверка работоспособности, актуальность базы данных признаков компьютерных вирусов и версии программного обеспечения средств антивирусной защиты;  6) В Значимом объекте КИИ должна обеспечиваться проверка объектов файловой системы средством антивирусной защиты до загрузки операционной системы;  7) В Значимом объекте КИИ должна обеспечиваться регистрация событий о неуспешном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);  8) Субъектом КИИ должна обеспечиваться антивирусная защита на этапе инициализации микропрограммного обеспечения средства вычислительной техники. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| АВЗ.2 | Антивирусная защита электронной почты и иных сервисов | Реализация защиты от вредоносного кода на уровне контроля почтового трафика |  | ГОСТ 57580.1 п.ЗВК.5 |
| АВЗ.3 | Контроль использования архивных, исполняемых и зашифрованных файлов | Возможность неконтролируемого открытия самораспаковывающихся архивов и исполняемых файлов, полученных из сети Интернет должна быть ограничена (блокирована) |  | ГОСТ 57580.1 п.ЗВК.21 |
| АВЗ.4 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | Субъектом КИИ 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 Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ должно обеспечиваться централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов);  2) В Значимом объекте КИИ должно обеспечиваться автоматическое обновление базы данных признаков вредоносных компьютерных программ (вирусов) на всех компонентах Значимого объекта КИИ;  3) В Значимом объекте КИИ должен обеспечиваться запрет изменений настроек системы обновления базы данных признаков вредоносных компьютерных программ (вирусов) на автоматизированных рабочих местах и серверах;  4) В Значимом объекте КИИ должна обеспечиваться возможность возврата (отката) к предыдущим обновлениям базы данных признаков вредоносных компьютерных программ (вирусов). | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| АВЗ.5 | Использование средств антивирусной защиты различных производителей | Использование средств защиты от вредоносного кода различных производителей, как минимум для уровней:  -физические АРМ пользователей и эксплуатационного персонала;  - серверное оборудование;  - контроль межсетевого трафика |  | ГОСТ 57580.1 п.ЗВК.14 |
| 1. **ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ (КОМПЬЮТЕРНЫХ АТАК)** | | | | |
| СОВ.0 | Регламентация правил и процедур предотвращения вторжений (компьютерных атак) | Субъектом КИИ должны быть разработаны и утверждены:  • политика предотвращения вторжений (компьютерных атак);  • процедуры, обеспечивающие осуществление политики предотвращения вторжений (компьютерных атак) и соответствующих механизмов предотвращения вторжений (компьютерных атак) |  | NIST Special Publication 800-53 Revision 5 |
| СОВ.1 | Обнаружение и предотвращение компьютерных атак | Субъектом КИИ 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 Значимого объекта КИИ (системы обнаружения вторжений уровня сети) и (или) на внутренних узлах (системы обнаружения вторжений уровня узла) сегментов Значимого объекта КИИ (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 Субъекта КИИ по защите информации. | 1) Субъектом КИИ обеспечивается применение систем обнаружения вторжений уровня сети, обеспечивающих сбор и анализ информации об информационных потоках, передаваемых в рамках сегмента (сегментов) Значимого объекта КИИ;  2) В Значимом объекте КИИ обеспечивается централизованное управление (администрирование) компонентами системы обнаружения вторжений, установленными в различных сегментах Значимого объекта КИИ;  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) Субъектом КИИ обеспечивается применение систем обнаружения вторжений уровня узла на автоматизированных рабочих местах и серверах Значимого объекта КИИ;  6) Субъектом КИИ обеспечивается применение систем обнаружения вторжений на прикладном уровне базовой эталонной модели взаимосвязи открытых систем. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| СОВ.2 | Обновление базы решающих правил | Субъектом КИИ должно обеспечиваться обновление базы решающих правил системы обнаружения вторжений, применяемой в Значимом объекте КИИ.  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 Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ должно обеспечиваться централизованное управление обновлением базы решающих правил системы обнаружения вторжений;  2) В Значимом объекте КИИ должна обеспечиваться возможность редактирования базы решающих правил (добавление и (или) исключение решающих правил) со стороны уполномоченных должностных лиц (администраторов) для предотвращения определенных Субъектом КИИ компьютерных атак и (или) сокращения нагрузки на Значимый объект КИИ, а также минимизации ложных срабатываний системы обнаружения вторжений;  3) Субъектом КИИ 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. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| 1. **ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ** | | | | |
| ОЦЛ.0 | Регламентация правил и процедур обеспечения целостности | Субъектом КИИ должны быть разработаны и утверждены:  • политика обеспечения целостности;  • процедуры, обеспечивающие осуществление политики обеспечения целостности и соответствующих механизмов обеспечения целостности |  | NIST Special Publication 800-53 Revision 5 |
| ОЦЛ.1 | Контроль целостности программного обеспечения | В Значимом объекте КИИ 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 Значимого объекта КИИ; * контроль целостности компонентов программного обеспечения (за исключением средств защиты информации), определяемого Субъектом КИИ 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 Значимого объекта КИИ; * контроль применения средств разработки и отладки программ в составе программного обеспечения Значимого объекта КИИ; * 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 Значимого объекта КИИ в соответствии с ЗТС.2 и ЗТС.3.   В случае если функциональные возможности Значимого объекта КИИ должны предусматривать применение в составе ее программного обеспечения средств разработки и отладки программ, Субъектом КИИ 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 Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ 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 Значимом объекте КИИ 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) Субъектом КИИ исключается возможность использования средств разработки и отладки программ во время обработки и (или) хранения информации в целях обеспечения целостности программной среды;  4) Субъектом КИИ обеспечивается выделение рабочих мест с установленными средствами разработки и отладки программ в отдельный сегмент (тестовую среду);  5) В Значимом объекте КИИ должна обеспечиваться блокировка запуска программного обеспечения и (или) блокировка сегмента (компонента) Значимого объекта КИИ (автоматизированного рабочего места, сервера) в случае обнаружения фактов нарушения целостности. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ОЦЛ.2 | Контроль целостности информации | В Значимом объекте КИИ должен осуществляться контроль целостности информации, содержащейся в базах данных Значимого объекта КИИ.  Контроль целостности информации, содержащейся в базах данных Значимого объекта КИИ, 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 Значимого объекта КИИ; * 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 Значимого объекта КИИ; * обеспечение физической защиты технических средств Значимого объекта КИИ, на которых установлена база данных, в соответствии с ЗТС.2 и ЗТС.3.   Правила и процедуры контроля целостности информации регламентируются в организационно-распорядительных документах Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ должны выполняться процедуры контроля целостности информации, содержащейся в базе данных, перед каждым запуском программного обеспечения доступа к базе данных;  2) В Значимом объекте КИИ должен обеспечиваться контроль целостности исполняемых модулей, хранящихся в базах данных (например, хранимые процедуры, триггеры);  3) В Значимом объекте КИИ должна обеспечиваться блокировка запуска системы управления базы данных и (или) блокировка сегмента (компонента) Значимого объекта КИИ (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. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ОЦЛ.3 | Ограничения по вводу информации в информационную (автоматизированную) систему | В Значимом объекте КИИ должно осуществляться ограничение прав пользователей по вводу информации в Значимый объект КИИ.  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 Значимом объекте КИИ.  Ограничения прав пользователей по вводу информации в Значимый объект КИИ должны фиксироваться в организационно-распорядительных документах по защите информации (документироваться) и реализовываться в соответствии с УПД.4 и УПД.5. | 1) В Значимом объекте КИИ обеспечивается исключение возможности ввода пользователями информации в Значимый объект КИИ, вследствие реализации ограничительных интерфейсов по вводу информации только через специальные формы прикладного программного обеспечения. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ОЦЛ.4 | Контроль данных, вводимых в информационную (автоматизированную) систему | в Значимом объекте КИИ должен осуществляться контроль точности, полноты и правильности данных, вводимых в Значимый объект КИИ.  Контроль точности, полноты и правильности данных, вводимых в Значимый объект КИИ, обеспечивается путем установления и проверки соблюдения форматов ввода данных, синтаксических, семантических и (или) иных правил ввода информации в Значимый объект КИИ (допустимые наборы символов, размерность, область числовых значений, допустимые значения, количество символов) для подтверждения того, что ввод информации соответствует заданному Субъектом КИИ формату и содержанию.  Вводимые данные должны проверяться на наличие конструкций, которые могут быть интерпретированы программно-техническими средствами Значимого объекта КИИ как исполняемые команды. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ОЦЛ.5 | Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях | В Значимом объекте КИИ 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 Субъектом КИИ типов ошибочных действий пользователей, которые потенциально могут привести к нарушению безопасности информации в Значимом объекте КИИ; * генерирование сообщений для пользователей об их ошибочных действиях и о возможности нарушения безопасности информации в Значимом объекте КИИ для корректировки действий пользователей; * регистрация информации об ошибочных действиях пользователей, которые могут привести к нарушению безопасности информации в Значимом объекте КИИ, в журналах регистрации событий безопасности в соответствии с РСБ.3; * предоставление доступа к сообщениям об ошибочных действиях пользователей только администраторам. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ОЦЛ.6 | Обезличивание и (или) деидентификация информации | Субъектом КИИ должны быть разработаны и утверждены:   * политика обеспечения доступности; * процедуры, обеспечивающие осуществление политики обеспечения доступности и соответствующих механизмов обеспечения доступности. |  | NIST Special Publication 800-53 Revision 5 |
| 1. **ОБЕСПЕЧЕНИЕ ДОСТУПНОСТИ** | | | | |
| ОДТ.0 | Регламентация правил и процедур обеспечения доступности | Субъектом КИИ должны быть разработаны и утверждены:   * политика обеспечения доступности; * процедуры, обеспечивающие осуществление политики обеспечения доступности и соответствующих механизмов обеспечения доступности. |  | NIST Special Publication 800-53 Revision 5 |
| ОДТ.1 | Использование отказоустойчивых технических средств | Субъектом КИИ должно обеспечиваться использование отказоустойчивых технических средств, предусматривающее:   * определение сегментов Значимого объекта КИИ, 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 Значимого объекта КИИ и доступности информации, установленных оператором; * определение предельных (пороговых) значений характеристик (коэффициента) готовности, показывающего, какую долю времени от общего времени работы Значимого объекта КИИ 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 Значимого объекта КИИ и доступности информации, установленных оператором; * применение в Значимом объекте КИИ технических средств с установленными Субъектом КИИ характеристиками (коэффициентом) готовности и надежности, обеспечивающих требуемые условия непрерывности функционирования Значимого объекта КИИ и доступности информации; * контроль с установленной Субъектом КИИ 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.   Субъектом КИИ должно быть обеспечено определение требуемых характеристик (коэффициентов) надежности и готовности в соответствии с национальными стандартами. | 1) Субъект КИИ 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 Значимом объекте КИИ реализуется автоматическое оповещение (сигнализация) о достижении техническим средством предельных (пороговых) значений характеристик (коэффициентов) готовности и надежности (степень достижения предельных значений определяется оператором);  3) В Значимом объекте КИИ реализуется автоматическое оповещение (сигнализация) о достижении техническим средством предельных (пороговых) значений характеристик загрузки. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ОДТ.2 | Резервирование средств и систем | Субъектом КИИ должно обеспечиваться резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования Значимого объекта КИИ, предусматривающее:   * определение сегментов Значимого объекта КИИ, 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 Значимого объекта КИИ и доступности информации, установленных оператором; * применение резервных (дублирующих) технических средств, программного обеспечения, каналов передачи информации и (или) средств обеспечения функционирования Значимого объекта КИИ, обеспечивающих требуемые условия непрерывности функционирования Значимого объекта КИИ и доступности информации; * ввод в действие резервного технического средства, программного обеспечения, канала передачи информации или средства обеспечения функционирования при нарушении требуемых условий непрерывности функционирования Значимого объекта КИИ и доступности информации.   Резервирование технических средств в зависимости от требуемых условий обеспечения непрерывности функционирования Значимого объекта КИИ 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 Значимого объекта КИИ и доступности информации.  Резервирование каналов передачи информации включает:   * резервирование каналов связи, обеспечивающее снижение вероятности отказа в доступе к Значимому объекту КИИ; * наличие у основных и альтернативных поставщиков телекоммуникационных услуг (провайдеров) Значимого объекта КИИ планов по восстановлению связи при авариях и сбоях, с указанием времени восстановления. * Резервирование средств обеспечения функционирования Значимого объекта КИИ включает: * использование кратковременных резервных источников питания для обеспечения правильного (корректного) завершения работы сегмента Значимого объекта КИИ (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 Значимого объекта КИИ (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 Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ 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 Субъектом КИИ процедур обеспечения требуемых условий обеспечения непрерывности функционирования Значимого объекта КИИ 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 Значимом объекте КИИ должно обеспечиваться предоставление резервных каналов связи от альтернативных поставщиков телекоммуникационных услуг (провайдеров), отличных от поставщиков (провайдеров) основных каналов связи;  3) В Значимом объекте КИИ должно обеспечиваться использование резервных каналов связи, проходящих по трассам, отличным от трасс прохождения основных каналов связи;  4) В Значимом объекте КИИ должно обеспечиваться использование резервных (отделенных от основных) телекоммуникационных сервисов, обеспечивающих доступность информации, до восстановления доступности основных телекоммуникационных сервисов поставщиком телекоммуникационных услуг (провайдером). | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ОДТ.3 | Контроль безотказного функционирования средств и систем | Субъектом КИИ 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 Значимого объекта КИИ 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. | 1) В Значимом объекте КИИ должна быть обеспечена сигнализация (уведомление) о неисправностях, сбоях и отказах в функционировании программно-технических средств Значимого объекта КИИ;  2) Субъектом КИИ должна обеспечиваться регистрация сбоев и отказов в функционировании технических средств Значимого объекта КИИ;  3) В Значимом объекте КИИ должны применяться программные средства мониторинга технического состояния Значимого объекта КИИ, осуществляющие мониторинг отказов программных и программно-технических средств в соответствии с перечнем, определенным оператором. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ОДТ.4 | Резервное копирование информации | Субъектом КИИ должно обеспечиваться периодическое резервное копирование информации на резервные машинные носители информации, предусматривающее:   * резервное копирование информации на резервные машинные носители информации с установленной Субъектом КИИ 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 Субъекта КИИ по защите информации. | 1) Субъектом КИИ 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) Субъектом КИИ должно осуществляться хранение (размещение) резервных копий информации на отдельных (размещенных вне Значимого объекта КИИ) средствах хранения резервных копий и в помещениях, специально предназначенных для хранения резервных копий информации, которые исключают воздействие внешних факторов на хранимую информацию;  3) Субъектом КИИ должно осуществляться резервное копирование информации на зеркальную Значимый объект КИИ (сегмент Значимого объекта КИИ, техническое средство, устройство);  4) Субъектом КИИ 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 Значимого объекта КИИ и доступности информации;  5) Субъектом КИИ должно осуществляться пространственное (географическое) разнесение мест хранения носителей резервных копий информации и мест расположения оригиналов этой информации. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ОДТ.5 | Обеспечение возможности восстановления информации | Субъектом КИИ должна быть обеспечена возможность восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного Субъектом КИИ 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 Значимого объекта КИИ и доступности информации; * восстановление информации с резервных машинных носителей информации (резервных копий) в течение установленного Субъектом КИИ 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 Субъекта КИИ по защите информации. | 1) Субъектом КИИ должна обеспечиваться возможность восстановления информации с учетом нагруженного ("горячего") резервирования технических средств в соответствии с ОДТ.2;  2) В Значимом объекте КИИ 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. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ОДТ.6 | Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях | Субъектом КИИ должна быть предусмотрена возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.  Для обеспечения возможности восстановления программного обеспечения в Значимом объекте КИИ 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 Значимого объекта КИИ в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей Значимого объекта КИИ, определенных оператором, позволяющих решать задачи по обработке информации.   Субъектом КИИ 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 Субъекта КИИ по защите информации. | 1) Субъектом КИИ обеспечивается восстановление отдельных функциональных возможностей Значимого объекта КИИ с применением резервированного программного обеспечения зеркальной Значимого объекта КИИ (сегмента Значимого объекта КИИ, технического средства, устройства) в соответствии с ОДТ.2 и ОДТ.4. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ОДТ.7 | Кластеризация информационной (автоматизированной) системы | В Значимом объекте КИИ должно обеспечиваться выделение групп однотипных узлов, объединенных каналами передачи информации и рассматриваемых как единый программно-технический ресурс, Значимого объекта КИИ 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. | 1) В Значимом объекте КИИ должна осуществляться кластеризация серверов контроллеров доменов, серверов резервного копирования, серверов управления и мониторинга состояния Значимого объекта КИИ, серверов виртуальной инфраструктуры и иных основных устройств и программного обеспечения системного уровня;  2) В Значимом объекте КИИ должна осуществляться кластеризация серверов приложений, файловых серверов, серверов баз данных, почтовых серверов и иных устройств и программного обеспечения прикладного уровня;  3) В Значимом объекте КИИ должна осуществляться кластеризация средств защиты информации (в случаях, когда это технически возможно), включая средства межсетевого экранирования, средства защиты каналов передачи информации. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ОДТ.8 | Контроль предоставляемых вычислительных ресурсов и каналов связи | Необходимо осуществлять мониторинг, корректировку и прогнозирование использования ресурсов, исходя из будущих требований к производительности, для обеспечения требуемой производительности системы.  Руководство по применению  Требования к производительности должны быть определены с учетом важности рассматриваемой системы для бизнеса. Необходимо проводить настройку и мониторинг системы для гарантии и, где это применимо, повышения доступности и эффективности системы. Для своевременного выявления проблем следует задействовать соответствующие средства обнаружения. Прогнозирование требований к производительности должны учитывать новые требования как со стороны бизнеса, так и со сторон систем, а также текущие и будущие тенденции в возможностях обработки информации в организации.  Особое внимание следует уделять ресурсам, требующим длительного времени на закупку или высоких затрат, поэтому руководители должны следить за использованием ключевых системных ресурсов. Они должны определять тенденции использования, особенно в отношении бизнес-приложений или инструментов управления информационными системами.  Руководители должны использовать эту информацию для выявления зависимости от основных работников и предотвращения потенциальных узких мест, которые могут представлять угрозу безопасности систем или сервисов, а также планирования соответствующего действия.  Обеспечение достаточного уровня производительности может быть достигнуто как путем наращивания мощностей, так и снижением спроса. Примеры мер снижения спроса включают в себя:  удаление устаревших данных a) (дисковое пространство);  b) вывод из эксплуатации приложений, систем, баз данных или сред;  c) оптимизация пакетных заданий и расписаний;  d) оптимизация логики приложения или запросов к базе данных;  e) запрет или ограничение полосы пропускания для ресурсоемких служб, если они не являются критически важными для бизнеса (например, потоковое видео).  В отношении критически важных систем следует иметь задокументированный план управления производительностью.  Дополнительная информация  Данная мера также применима к человеческим ресурсам, а также к помещениям и оборудованию. |  | Стандарт ISO 27002 п. 12.1.3 |
| 1. **ЗАЩИТА ТЕХНИЧЕСКИХ СРЕДСТВ И СИСТЕМ** | | | | |
| ЗТС.0 | Регламентация правил и процедур защиты технических средств и систем | Субъектом КИИ должны быть разработаны и утверждены:  • политика защиты технических средств и систем;  • процедуры, обеспечивающие осуществление политики защиты технических средств и систем и соответствующих механизмов защиты технических средств и систем. |  | NIST Special Publication 800-53 Revision 5 |
| ЗТС.1 | Защита информации от утечки по техническим каналам | Субъектом КИИ 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. N 282, а также иными методическими документами ФСТЭК России по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, от утечки по техническим каналам. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗТС.2 | Организация контролируемой зоны | Субъектом КИИ 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) Субъекта КИИ и лиц, не имеющих постоянного допуска на объекты Значимого объекта КИИ (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 Значимого объекта КИИ (его сегментов) может быть организовано несколько контролируемых зон. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗТС.3 | Управление физическим доступом | Субъектом КИИ 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 Значимого объекта КИИ 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 Субъекта КИИ по защите информации. | 1) Субъектом КИИ 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) Субъектом КИИ 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) Субъектом КИИ обеспечивается интеграция системы контроля и управления доступом (СКУД) со средствами идентификации и аутентификации пользователей в Значимом объекте КИИ в соответствии с ИАФ.1, ИАФ.6 и средствами управления доступом в соответствии с УПД.2, УПД.10. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | Субъектом КИИ должно осуществляться размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.  В качестве устройств вывода (отображения) информации в Значимом объекте КИИ 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. | 1) Субъектом КИИ обеспечивается установка на окна помещений Значимого объекта КИИ 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. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗТС.5 | Защита от внешних воздействий | Субъектом КИИ 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. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗТС.6 | Маркирование аппаратных компонентов системы относительно разрешенной к обработке информации | Субъект КИИ должен классифицировать носители так, чтобы можно было определить уровень критичности хранимых данных |  | Стандарт PCI DSS п.9.6.1 |
| ЗИС.0 | Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов | Гарантировать, что политики безопасности и операционные процедуры разработки и поддержки безопасных систем и приложений документированы, используются и известны всем заинтересованным лицам. |  | PCI DSS, п. 6.7 |
| ЗИС.1 | Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями | В Значимом объекте КИИ должно быть обеспечено разделение функциональных возможностей по управлению (администрированию) Значимым объектом КИИ, управлению (администрированию) системой защиты информации (функций безопасности) и функциональных возможностей пользователей по обработке информации.  Функциональные возможности по управлению (администрированию) Значимым объектом КИИ 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 Значимого объекта КИИ, реализующих функциональные возможности по управлению (администрированию) Значимым объектом КИИ 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. | 1) В Значимом объекте КИИ должно обеспечиваться исключение отображения функциональных возможностей по управлению (администрированию) Значимым объектом КИИ, управлению (администрированию) системой защиты информации в интерфейсе пользователя;  2) В Значимом объекте КИИ должно обеспечиваться выделение автоматизированных рабочих мест для администраторов Значимого объекта КИИ;  3) В Значимом объекте КИИ должно обеспечиваться выделение автоматизированных рабочих мест для администраторов безопасности;  4) Субъектом КИИ должно обеспечиваться исключение возможности управления (администрирования) Значимым объектом КИИ, управления (администрирования) системой защиты информации из-за пределов контролируемой зоны. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.2 | Защита периметра информационной (автоматизированной) системы | В Значимом объекте КИИ должна осуществляться защита периметра (физических и (или) логических границ) Значимого объекта КИИ при его взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, предусматривающая:   * управление (контроль) входящими в Значимый объект КИИ и исходящими из Значимого объекта КИИ информационными потоками на физической и (или) логической границе Значимого объекта КИИ (сегментов Значимого объекта КИИ); * обеспечение взаимодействия Значимого объекта КИИ и (или) его 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 Значимого объекта КИИ или его 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 Значимого объекта КИИ регламентируются в организационно-распорядительных документах Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ должна быть обеспечена возможность размещения публичных общедоступных ресурсов (в частности общедоступный веб-сервер), взаимодействующих с Значимым объектом КИИ через отдельные физические управляемые (контролируемые) сетевые интерфейсы;  2) В Значимом объекте КИИ должно быть обеспечено предоставление доступа во внутренние сегменты Значимого объекта КИИ (демилитаризованную зону) из внешних информационных систем и сетей только через средства защиты периметра (за исключением внутренних сегментов, которые специально выделены для такого взаимодействия);  3) Субъект КИИ должен ограничить количество точек доступа в Значимый объект КИИ 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) Субъектом КИИ:  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 Значимом объекте КИИ, и определение продолжительности потребности таких исключений;  д) должно обеспечиваться удаление введенных исключений из правил управления информационными потоками после истечения установленного времени;  5) В Значимом объекте КИИ должен быть исключен выход (вход) через управляемые (контролируемые) сетевые интерфейсы информационных потоков по умолчанию (реализация принципа "запрещено все, что не разрешено");  6) Субъектом КИИ обеспечивается запрет передачи информации за пределы периметра Значимого объекта КИИ при отказе (сбое) функционирования средств защиты периметра;  7) В Значимом объекте КИИ 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 Значимому объекту КИИ с использованием средств построения виртуальных частных сетей;  8) В Значимом объекте КИИ обеспечивается сетевое соединение внутренних сегментов Значимого объекта КИИ (отдельных средств вычислительной 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 Значимом объекте КИИ 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 Значимом объекте КИИ 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 Значимом объекте КИИ 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 Значимом объекте КИИ обеспечивается защита периметра с использованием шлюза безопасности на уровне узлов (хостов) для серверов, рабочих станций и мобильных технических средств;  13) В Значимом объекте КИИ 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) Субъектом КИИ обеспечивается отделение через отдельный физический управляемый (контролируемый) сетевой интерфейс функций безопасности и управления (администрирования) Значимого объекта КИИ, определенных оператором, от других (внутренних) компонентов Значимого объекта КИИ;  15) Субъектом КИИ обеспечивается исключение возможности несанкционированного физического сетевого подключения к управляемым (контролируемым) сетевым интерфейсам (сетевым интерфейсам средств защиты периметра);  16) В Значимом объекте КИИ для контроля (анализа) защищенности доступ администраторов обеспечивается через выделенный отдельный физический управляемый (контролируемый) сетевой интерфейс;  17) Субъектом КИИ применяются автоматизированные средства, обеспечивающие строгое соблюдение формата сетевых протоколов на уровне приложений (проверка пакетов на предмет соблюдения спецификаций протокола на уровне приложений);  18) В Значимом объекте КИИ обеспечивается корректное завершение ее функционирования в случае нарушения функционирования (сбоя, отказов) средств защиты периметра;  19) В Значимом объекте КИИ при необходимости предоставлять доступ к ресурсам Значимого объекта КИИ должна быть организована демилитаризованная зона, содержащая доступные ресурсы;  20) В Значимом объекте КИИ должна быть обеспечена возможность размещения публичных общедоступных ресурсов (например, общедоступный веб-сервер), взаимодействующих с Значимым объектом КИИ через отдельные физические управляемые (контролируемые) сетевые интерфейсы. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.3 | Эшелонированная защита информационной (автоматизированной) системы | Субъект КИИ должен осуществлять сегментацию системы на [Назначение: компоненты системы, определенные организацией], находящихся в отдельных [Выбор: физический; логические] доменах или средах на основе [Назначение: определенные организацией обстоятельства для физического или логического разделения компонентов].  Обсуждение: Сегментация системы является частью стратегии защиты. Организации определяют степень физического разделения компонентов системы. Варианты физического разделения включают в себя физически отдельные компоненты в отдельных стойках в одной комнате, критические компоненты в разных комнатах и географическое разделение критических компонентов. Категоризация безопасности может направлять выбор кандидатов для разделения домена. Управляемые интерфейсы ограничивают или запрещают доступ к сети и поток информации между отдельными компонентами системы. | Распределение привилегированных функций по отдельным физическим доменам.  Обсуждение: Привилегированные функции, которые работают в одном физическом домене, могут представлять собой единую точку отказа, если этот домен становится скомпрометированным или испытывает отказ в обслуживании | NIST Special Publication 800-53 Revision 5 |
| ЗИС.4 | Сегментирование информационной (автоматизированной) системы | Субъектом КИИ должно осуществляться разбиение Значимого объекта КИИ на сегменты (сегментирование Значимого объекта КИИ) и обеспечиваться защита периметров сегментов Значимого объекта КИИ.  Сегментирование Значимого объекта КИИ проводится с целью построения многоуровневой (эшелонированной) системы защиты информации путем построения сегментов на различных физических доменах или средах. Принципы сегментирования Значимого объекта КИИ определяются Субъектом КИИ 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 Значимого объекта КИИ также может проводиться с целью разделения Значимого объекта КИИ на сегменты, имеющие различные классы защищенности Значимого объекта КИИ.  При сегментировании Значимого объекта КИИ должна быть обеспечена защита периметров сегментов Значимого объекта КИИ. | 1) Субъектом КИИ осуществляется выделение сегментов Значимого объекта КИИ для размещения общедоступной (публичной) информации:  а) путем выделения отдельных физических сетевых интерфейсов коммуникационного оборудования и (или) средств защиты периметра;  б) путем физической изоляции сегментов Значимого объекта КИИ для размещения общедоступной (публичной) информации. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.5 | Организация демилитаризованной зоны | Субъект КИИ должен осуществлять:  а. Мониторинг и контроль обмена данными на внешних интерфейсах с системой и на ключевых внутренних интерфейсах внутри системы; b. Выделение в подсети общедоступных компонентов системы, которые [Выбор: физически; логически] отделены от внутренней сети; и c. Подключение к внешним сетям или системам только через управляемые интерфейсы, через устройства защиты периметра, организованные в соответствии с архитектурой безопасности и конфиденциальности организации.  Субъект КИИ должен осуществлять защиту периметра (услуги внешней телекоммуникации):  а) реализовать управляемый интерфейс для каждой внешней службы электросвязи; (b) Установить политики маршрутизации для каждого управляемого интерфейса; с) защищать конфиденциальность и целостность информации, передаваемой через каждый интерфейс; (d) Документировать каждое исключение из политики  маршрутизации с указанием с указанием цели и продолжительности; e) пересматривать исключения из политики маршрутизации с [Назначение: частота, определяемая организацией] и удалять исключения, которые больше не нужны; (f) предотвращать несанкционированный обмен управляющим трафиком с внешними сетями; (g) публиковать информацию, позволяющую удаленным сетям обнаруживать неавторизованный трафик уровня управления из внутренних сетей; и (h) Фильтрация неавторизованного трафика уровня управления из внешних сетей. |  | NIST Special Publication 800-53 Revision 5 |
| ЗИС.6 | Управление сетевыми потоками | В Значимом объекте КИИ должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках Значимого объекта КИИ, включающее:   * фильтрацию информационных потоков в соответствии с правилами управления потоками, установленными оператором; * разрешение передачи информации в Значимом объекте КИИ 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 Значимого объекта КИИ, 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 Значимого объекта КИИ, 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 Значимого объекта КИИ и (или) входящие в Значимый объект КИИ.  Правила и процедуры управления информационными потоками регламентируются в организационно-распорядительных документах Субъекта КИИ по защите информации.  В Значимом объекте КИИ должно осуществляться управление потоками информации между компонентами виртуальной инфраструктуры и по периметру виртуальной инфраструктуры  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, объему 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. | 1) В Значимом объекте КИИ должно обеспечиваться управление информационными потоками на основе атрибутов (меток) безопасности, связанных с передаваемой информацией, источниками и получателями информации;  2) В Значимом объекте КИИ должно обеспечиваться динамическое управление информационными потоками, запрещающее и (или) разрешающее передачу информации на основе анализа изменения текущего состояния Значимого объекта КИИ или условий ее функционирования;  3) В Значимом объекте КИИ должен исключаться обход правил управления информационными потоками за счет преобразования передаваемой информации;  4) В Значимом объекте КИИ должен исключаться обход правил управления информационными потоками за счет встраивания одних данных в другие данные информационного потока;  5) В Значимом объекте КИИ должен обеспечиваться контроль соединений между техническими средствами (устройствами), используемыми для организации информационных потоков;  6) В Значимом объекте КИИ при передаче информации между сегментами Значимого объекта КИИ и (или) информационными системами разных классов защищенности должна обеспечиваться однонаправленная передача информации с использованием аппаратных средств;  7) В Значимом объекте КИИ должно обеспечиваться управление информационными потоками на основе структуры передаваемых данных (текст, таблицы, видео, аудиоинформация);  8) В Значимом объекте КИИ должно обеспечиваться управление информационными потоками на основе используемых сетевых протоколов;  9) В Значимом объекте КИИ должно обеспечиваться управление информационными потоками на основе типов (расширений) файлов и (или) имен файлов;  10) В Значимом объекте КИИ должна обеспечиваться возможность запрета, разрешения и изменения маршрута передачи информации только администраторами;  11) В Значимом объекте КИИ должно обеспечиваться разделение информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской информации;  12) В Значимом объекте КИИ должна обеспечиваться возможность автоматического блокирования передачи информации при выявлении в передаваемой информации вредоносных компьютерных программ;  13) В Значимом объекте КИИ должно осуществляться управление информационными потоками при передаче информации между информационными системами;  14) В Значимом объекте КИИ должна обеспечиваться возможность фильтрации информационных потоков на уровне прикладного программного обеспечения (приложений);  15) В Значимом объекте КИИ 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.  Требования к усилению ЗСВ.4:  17) В Значимом объекте КИИ, 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);  18) В Значимом объекте КИИ должна обеспечиваться фильтрация сетевого трафика от (к) каждой гостевой операционной системы, в виртуальных сетях гипервизора и для каждой виртуальной машины;  19) В Значимом объекте КИИ 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;  20) В Значимом объекте КИИ в соответствии с законодательством Российской Федерации применяются криптографические методы защиты информации конфиденциального характера, передаваемой по виртуальным и физическим каналам связи гипервизора, хостовой операционной системы;  21) В Значимом объекте КИИ при реализации мер по управлению потоками информации между компонентами виртуальной инфраструктуры должны обеспечиваться семантический и статистический анализ сетевого трафика;  22) В Значимом объекте КИИ должно обеспечиваться определение перечня протоколов и портов (включая динамически выделяемые порты), необходимых для работы приложений и сервисов в рамках виртуальной инфраструктуры;  23) В Значимом объекте КИИ 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. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.7 | Использование эмулятора среды функционирования программного обеспечения ("песочница") | Субъектом КИИ должны использоваться эмуляторы среды функционирования программного обеспечения, позволяющие открывать вложения электронной почты, выполнять ненадежные или подозрительные приложения и выполнять запросы Universal Resource Locator (URL) в изолированной среде или виртуализированной изолированной среде. «Песочницы» должны определять, содержат ли связанные вложения/приложения вредоносный код. Хотя контроль связан с концепцией ложных сетей, он не предназначен для поддержания долгосрочной среды, в которой могут действовать противники и могут наблюдаться их действия. |  | NIST Special Publication 800-53 Revision 5 |
| ЗИС.8 | Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы | Субъектом КИИ должно обеспечиваться воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик Значимого объекта КИИ или его сегментов, обеспечивающее навязывание у нарушителя ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках Значимого объекта КИИ.  Воспроизведение (визуализация) ложных и (или) скрытие (маскирование) истинных отдельных информационных технологий и (или) структурно-функциональных характеристик Значимого объекта КИИ или его 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 Значимый объект КИИ.  При этом визуализация ложных и (или) маскирование истинных отдельных информационных технологий и (или) структурно-функциональных характеристик Значимого объекта КИИ позволяют снизить или исключить затраты на внедрение сложных средств защиты информации. | 1) визуализация ложных информационных технологий и (или) структурно-функциональных характеристик осуществляется в произвольном порядке с периодичностью, определяемой оператором. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.9 | Создание гетерогенной среды | 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 Значимого объекта КИИ UNIX-подобных операционных систем, отличных от операционных систем, применяемых на автоматизированных рабочих местах типа Windows и (или) применением в смежных сетевых сегментах Значимого объекта КИИ разных типов сетевого общесистемного, прикладного и (или) специального программного обеспечения.  При создании гетерогенной среды необходимо учитывать повышение сложности в управлении конфигурацией Значимого объекта КИИ и возможность увеличения ошибок конфигурации и возможных уязвимостей. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.10 | Использование программного обеспечения, функционирующего в средах различных операционных систем | В Значимом объекте КИИ 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 Значимого объекта КИИ.  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. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.11 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом | В Значимом объекте КИИ 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 Значимом объекте КИИ; * выполнение процессов (служб, сервисов) в Значимом объекте КИИ 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. | 1) В Значимом объекте КИИ должно обеспечиваться исключение возможности несанкционированного изменения приоритетов выполнения процессов. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.12 | Изоляция процессов (выполнение программ) в выделенной области памяти | В Значимом объекте КИИ 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. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.13 | Защита неизменяемых данных | В Значимом объекте КИИ 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 Субъектом КИИ 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 Значимом объекте КИИ. | 1) Субъектом КИИ 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. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.14 | Использование не перезаписываемых машинных носителей информации | В Значимом объекте КИИ 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. | 1) в сегментах (компонентах) Значимого объекта КИИ, определяемых оператором, применяются неперезаписываемые (защищенные от записи) машинные носители информации, устойчивые к сбоям в программном обеспечении Значимого объекта КИИ и отключению питания;  2) Субъектом КИИ должен осуществляться контроль целостности программного обеспечения, записанного на машинные носители информации, доступные только для чтения | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.15 | Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек | Реализация почтового обмена с сетью Интернет через ограниченное количество контролируемых точек информационного взаимодействия, состоящих из внешнего (подключенного к сети Интернет) и внутреннего (размещенного во внутренних сетях финансовой организации) почтовых серверов с безопасной репликацией почтовых сообщений между ними |  | ГОСТ Р 57580.1, СМЭ.20 |
| ЗИС.16 | Защита от спама | Субъектом КИИ должно обеспечиваться обнаружение и реагирование на поступление незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию Значимого объекта КИИ (защита от спама).  Защита от спама реализуется на точках входа в Значимый объект КИИ (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).   Субъектом КИИ 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 Субъекта КИИ по защите информации. | 1) Субъектом КИИ обеспечивается централизованное управление средствами защиты от спама;  2) В Значимом объекте КИИ 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 Значимом объекте КИИ должна обеспечиваться аутентификация отправителей электронных сообщений в соответствии;  4) В Значимом объекте КИИ должна обеспечиваться аутентификация серверов электронной почты;  5) В Значимом объекте КИИ должен обеспечиваться контроль поступления в Значимый объект КИИ информационных сообщений и документов на основе контентного анализа. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.17 | Защита информации от утечек | В Значимом объекте КИИ должен осуществляться контроль содержания информации, передаваемой из Значимого объекта КИИ (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 Значимого объекта КИИ.  Контроль содержания информации, передаваемой из Значимого объекта КИИ, должен предусматривать:   * выявление фактов неправомерной передачи защищаемой информации из Значимого объекта КИИ 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 Значимого объекта КИИ, 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 Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ должно осуществляться хранение всей передаваемой из Значимого объекта КИИ информации и (или) информации с недопустимым к передаче из Значимого объекта КИИ содержанием, в течение времени, определяемого оператором;  2) В Значимом объекте КИИ должна осуществляться блокировка передачи из Значимого объекта КИИ информации с недопустимым содержанием. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.18 | Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию | Включить в правила поведения ограничения на:  (а) Использование социальных меди, сайтов социальных сетей и внешних сайтов/приложений;  b) размещение информации об организации на общедоступных веб-сайтах; и  (c) Использование предоставленных Субъектом КИИ идентификаторов (например, адресов электронной почты) и средств аутентификации (например, паролей) для создания учетных записей на внешних сайтах/приложениях.  Ограничения на использование социальных медиа, социальных сетей и внешних сайтов/приложений касаются правил поведения, связанных с использованием социальных меди, социальных сетей и внешних сайтов, когда персонал организации использует такие сайты для служебных обязанностей или ведения официальных дел; когда организационная информация используется в социальных сетях, а также когда сотрудники получают доступ к социальным сетям и сетевым сайтам из систем организации. Организации соблюдают правила, которые не позволяют неавторизованным лицам получать непубличную информацию об организации из социальных сетей и сетевых сайтов либо напрямую, либо опосредованно. Непубличная информация включает в себя личную информацию и информацию о системной учетной записи. |  | NIST Special Publication 800-53 Revision 5 |
| ЗИС.19 | Защита информации при ее передаче по каналам связи | Субъектом КИИ 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. | 1) Субъект КИИ 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) Субъект КИИ обеспечивает защиту от модификации и навязывания (ввода ложной информации) передаваемой видеоинформации путем выявления и удаления скрытых вставок. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.20 | Обеспечение доверенных канала, маршрута | В Значимом объекте КИИ должны обеспечиваться доверенные маршруты передачи данных между администратором (пользователем) и средствами защиты информации (функциями безопасности средств защиты информации), определяемыми оператором.  Субъектом КИИ 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 Значимый объект КИИ. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.21 | Запрет несанкционированной удаленной активации периферийных устройств | В Значимом объекте КИИ 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 обеспечения, 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 Субъектом КИИ отдельных задач, решаемых Значимым объектом КИИ, 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. | 1) В Значимом объекте КИИ должна обеспечиваться возможность физического отключения периферийных устройств (например, отключение при организации и проведении совещаний в помещениях, где размещены видеокамеры и микрофоны);  2) В Значимом объекте КИИ 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) Субъектом КИИ обеспечивается удаление (отключение) из Значимого объекта КИИ (отдельных сегментов, например, расположенных в защищаемых и выделенных помещениях) периферийных устройств, перечень которых определяется оператором;  4) Субъектом КИИ 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. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.22 | Управление атрибутами безопасности при взаимодействии с иными информационными (автоматизированными) системами | В Значимом объекте КИИ 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 Значимом объекте КИИ, в явном или скрытом виде. | 1) В Значимом объекте КИИ должен обеспечиваться контроль целостности атрибутов безопасности (меток безопасности). | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.23 | Контроль использования мобильного кода | Субъектом КИИ должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий мобильного кода (активного контента) в Значимом объекте КИИ, 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 Значимом объекте КИИ; * определение разрешенных мест распространения (серверы Значимого объекта КИИ) и использования мобильного кода (автоматизированные рабочие места, мобильные технические средства Значимого объекта КИИ) и функций Значимого объекта КИИ, 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 Значимом объекте КИИ, 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 Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ 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 Значимом объекте КИИ должен осуществляться запрет загрузки и выполнения запрещенного мобильного кода;  3) В Значимом объекте КИИ 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 Значимом объекте КИИ должен осуществляться контроль подлинности источника мобильного кода и контроль целостности мобильного кода. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.24 | Контроль передачи речевой информации | Субъектом КИИ должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий передачи речи в Значимом объекте КИИ, 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 Значимом объекте КИИ; * 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 Значимом объекте КИИ, 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 Субъекта КИИ по защите информации. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.25 | Контроль передачи видеоинформации | Субъектом КИИ должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий передачи видеоинформации в Значимом объекте КИИ, 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 Значимом объекте КИИ; * 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 Значимом объекте КИИ, 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 Субъекта КИИ по защите информации. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.26 | Подтверждение происхождения источника информации | В Значимом объекте КИИ 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 сервера, являющегося источником ответов на запросы (сервер доменных имен или DNS-сервер) по определению сетевых адресов (IP-адресов) по сетевым именам (доменные имена); * аутентификация сервера, являющегося источником ответов на запросы (кэширующий DNS-сервер) по определению сетевых имен (доменных имен) по сетевым адресам (IP-адресам). | 1) В Значимом объекте КИИ 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). | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.27 | Обеспечение подлинности сетевых соединений | В Значимом объекте КИИ 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.  Контроль целостности передаваемой информации должен включать проверку целостности передаваемых пакетов. | 1) В Значимом объекте КИИ должно обеспечиваться признание идентификатора сеанса связи недействительным после окончания сетевого соединения;  2) В Значимом объекте КИИ должна осуществляться регистрация установления и разрыва сетевых соединений (сеансов взаимодействия) в целях выявления возможных инцидентов (событий безопасности);  3) В Значимом объекте КИИ должна осуществляться генерация и присвоение уникальных идентификаторов (одноразовых) для каждого сетевого соединения (сеанса взаимодействия) и контроль их подлинности (восприниматься должны только идентификаторы, сгенерированные Значимым объектом КИИ);  4) В Значимом объекте КИИ должно обеспечиваться обнаружение попыток повторного использования идентификаторов сетевых соединений и реагирование на эти попытки;  5) В Значимом объекте КИИ должна осуществляться защита от подбора идентификаторов, присваиваемых будущим сетевым соединениям (сеансам взаимодействия). | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.28 | Исключение возможности отрицания отправки информации | Субъектом КИИ 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; * регистрация событий, связанных с отправкой информации другому пользователю. | 1) В Значимом объекте КИИ должна обеспечиваться генерация свидетельства отправления информации (например, электронной подписи);  2) В Значимом объекте КИИ должна обеспечиваться связь атрибутов отправителя информации с полями отправляемой информации (текстом сообщения);  3) В Значимом объекте КИИ должна быть обеспечена возможность верификации (проверки) свидетельства отправления информации;  4) В Значимом объекте КИИ должна быть обеспечена возможность записи и защищенного хранения в течение установленного Субъектом КИИ времени информации, отправленной пользователем другому пользователю. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.29 | Исключение возможности отрицания получения информации | Субъектом КИИ 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; * регистрация событий, связанных с получением информации от другого пользователя. | 1) В Значимом объекте КИИ должна обеспечиваться генерация свидетельства получения информации (запрос подтверждения получения или электронная подпись);  2) В Значимом объекте КИИ должна быть обеспечена связь атрибутов получателя информации с полями отправляемой информации (текстом сообщения);  3) В Значимом объекте КИИ должна быть обеспечена возможность верификации (проверки) свидетельства получения информации;  4) В Значимом объекте КИИ должна быть обеспечена возможность записи и защищенного хранения в течение установленного Субъектом КИИ времени информации, полученной пользователем от другого пользователя. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.30 | Использование устройств терминального доступа | Субъектом КИИ для обработки информации в Значимом объекте КИИ 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. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.31 | Защита от скрытых каналов передачи информации | Субъектом КИИ 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 Значимого объекта КИИ.  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. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.32 | Защита беспроводных соединений | Субъектом КИИ должны обеспечиваться регламентация и контроль использования в Значимом объекте КИИ технологий беспроводного доступа пользователей к объектам доступа (стандарты коротковолновой радиосвязи, спутниковой и пакетной радиосвязи), направленные на защиту информации в Значимом объекте КИИ.  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) Значимого объекта КИИ, для решения которых такой доступ необходим, и предоставление беспроводного доступа; * 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 Значимого объекта КИИ; * контроль беспроводного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа Значимого объекта КИИ до начала информационного взаимодействия с Значимым объектом КИИ.   Правила и процедуры применения технологий беспроводного доступа регламентируются в организационно-распорядительных документах Субъекта КИИ по защите информации.  Субъектом КИИ должна быть обеспечена защита беспроводных соединений, применяемых в Значимом объекте КИИ. Защита беспроводных соединений включает:   * ограничение на использование в Значимом объекте КИИ беспроводных соединений (в частности 802.11xWi-Fi, 802.15.1 Bluetooth, 802.22WRAN, IrDA и иных беспроводных соединений) в соответствии с задачами (функциями) Значимого объекта КИИ, для решения которых такие соединения необходимы; * предоставление доступа к параметрам (изменению параметров) настройки беспроводных соединений только администраторам Значимого объекта КИИ; * 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 Значимому объекту КИИ через беспроводные соединения.   При обеспечении защиты беспроводных соединений в зависимости от их типов должны реализовываться меры по идентификации и аутентификации.  При невозможности исключения установления беспроводных соединений из-за пределов контролируемой зоны должны приниматься меры защищенного удаленного доступа.  Правила и процедуры применения беспроводных соединений регламентируются в организационно-распорядительных документах Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ обеспечивается аутентификация подключаемых с использованием технологий беспроводного доступа устройств в соответствии с ИАФ.2;  2) В Значимом объекте КИИ обеспечивается мониторинг точек беспроводного подключения устройств к Значимому объекту КИИ на предмет выявления несанкционированного беспроводного подключения устройств;  3) В Значимом объекте КИИ исключается возможность изменения пользователем точек беспроводного доступа Значимого объекта КИИ;  4) Субъектом КИИ одолжен быть предусмотрен запрет беспроводного доступа к Значимому объекту КИИ из-за пределов контролируемой зоны;  5) В Значимом объекте КИИ должен быть запрещен беспроводный доступ от имени привилегированных учетных записей (администраторов) для администрирования Значимого объекта КИИ и ее системы защиты информации;  6) В Значимом объекте КИИ исключается возможность изменения пользователем устройств и настроек беспроводного доступа;  7) Субъектом КИИ обеспечивается определение местонахождения несанкционированного беспроводного устройства;  8) Субъектом КИИ обеспечивается блокирование функционирования несанкционированного беспроводного устройства.  9) Субъектом КИИ для защиты беспроводных соединений в соответствии с законодательством Российской Федерации должны применяться средства криптографической защиты информации;  10) В Значимом объекте КИИ должны применяться программно-технические средства обнаружения, анализа и блокирования несанкционированного использования беспроводных технологий и подключений к Значимому объекту КИИ;  11) Субъектом КИИ должно обеспечиваться блокирование несанкционированных беспроводных подключений к Значимому объекту КИИ;  12) Субъектом КИИ должна быть исключена возможность установления беспроводных соединений из-за пределов контролируемой зоны. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.33 | Исключение доступа через общие ресурсы | В Значимом объекте КИИ 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 Значимого объекта КИИ.  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. | 1) В Значимом объекте КИИ должна быть исключена возможность использования в качестве общих для пользователей ресурсов Значимого объекта КИИ, которые используются как интерфейс (память, однонаправленные интерфейсы (устройства) и сетевые карты) взаимодействия (связи) с системами, имеющими другие классы защищенности. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.34 | Защита от угроз отказа в обслуживании (DOS, DDOS-атак) | В Значимом объекте КИИ должна обеспечиваться защита от угроз безопасности информации, направленных на отказ в обслуживании этой системы.  Субъектом КИИ 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 Значимом объекте КИИ мер защиты Значимого объекта КИИ и повышенными характеристиками производительности телекоммуникационного оборудования и каналов передачи совместно с резервированием информации и технических средств, программного обеспечения, каналов передачи информации. | 1) В Значимом объекте КИИ обеспечивается ограничение возможностей пользователей по реализации угроз безопасности информации, направленных на отказ в обслуживании, в отношении отдельных сегментов Значимого объекта КИИ и других информационных систем;  2) В Значимом объекте КИИ обеспечивается управление характеристиками производительности телекоммуникационного оборудования и каналов передачи информации в зависимости от интенсивности реализации угроз безопасности информации, направленных на отказ в обслуживании;  3) Субъектом КИИ 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 Значимого объекта КИИ);  4) Субъектом КИИ обеспечивается применение средств защиты информации, предназначенных для нейтрализации угроз безопасности, направленных на отказ в обслуживании;  5) В Значимом объекте КИИ меры защиты от угроз безопасности информации, направленных на отказ в обслуживании, должны обеспечить возможность защиты от соответствующих атак на Значимый объект КИИ без воздействия на трафик сети (подсети), в которой функционирует Значимый объект КИИ;  6) Субъектом КИИ 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. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.35 | Управление сетевыми соединениями | В Значимом объекте КИИ должно осуществляться завершение сетевых соединений (например, открепление пары порт/адрес (TCP/IP)) по их завершении и (или) по истечении заданного Субъектом КИИ временного интервала неактивности сетевого соединения. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.36 | Создание (эмуляция) ложных компонентов информационных (автоматизированных) систем | В Значимом объекте КИИ должны применяться специально созданные (эмулированные) ложные компоненты Значимого объекта КИИ 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 Значимого объекта КИИ 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 Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ применяются ложные компоненты Значимого объекта КИИ, выступающие в качестве цели для вредоносного программного обеспечения (вируса) и провоцирующие преждевременное (до воздействия на защищаемый объект доступа) проявление его признаков. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.37 | Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев) | В Значимом объекте КИИ должен осуществляться перевод Значимого объекта КИИ или его устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации Значимого объекта КИИ.  Перевод Значимого объекта КИИ или ее устройств (компонентов) в заранее определенную конфигурацию должен обеспечивать защиту информации при наступлении (возникновении) отказов (сбоев) в функционировании Значимого объекта КИИ или его сегментов, которые могут привести к нарушению конфиденциальности, целостности и (или) доступности этой информации.  Субъектом КИИ должны быть определены типы отказов (сбоев) в системе защиты информации Значимого объекта КИИ, которые могут привести к нарушению конфиденциальности, целостности и (или) доступности этой информации, и при наступлении (возникновении) которых должен обеспечиваться перевод Значимого объекта КИИ или его устройств (компонентов) в заранее определенную конфигурацию.  Заранее определенная конфигурация Значимого объекта КИИ должна содержать информацию о состоянии Значимого объекта КИИ и его системе защиты информации (системная информация, параметры настроек программного обеспечения, включая средств защиты информации), достаточной для перезапуска Значимого объекта КИИ и обеспечения его функционирования в штатном режиме, при котором также обеспечивается защита информации.  Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования Значимого объекта КИИ осуществляется в соответствии с ОДТ.2, резервное копирование информации - в соответствии с ОДТ.4.  Контроль безотказного функционирования технических средств Значимого объекта КИИ 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. |  | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.38 | Защита информации при использовании мобильных устройств | Субъектом КИИ должны обеспечиваться регламентация и контроль использования в Значимом объекте КИИ мобильных технических средств, направленные на защиту информации в Значимом объекте КИИ.  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 Значимого объекта КИИ с использованием мобильных технических средств, входящих в состав Значимого объекта КИИ; * использование в составе Значимого объекта КИИ 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) Значимого объекта КИИ, 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 Значимого объекта КИИ; * запрет возможности запуска без команды пользователя в Значимом объекте КИИ 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 Субъекта КИИ по защите информации.  Субъектом КИИ должна осуществляться защита применяемых в Значимом объекте КИИ 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 Значимом объекте КИИ программного обеспечения на мобильных технических средствах.   Правила и процедуры защиты мобильных технических средств регламентируются в организационно-распорядительных документах Субъекта КИИ по защите информации. | 1) Субъектом КИИ обеспечивается запрет использования в Значимом объекте КИИ, не входящих в ее состав (находящихся в личном использовании) съемных машинных носителей информации;  2) Субъектом КИИ обеспечивается запрет использования в Значимом объекте КИИ съемных машинных носителей информации, для которых не определен владелец (пользователь, организация, ответственные за принятие мер защиты информации);  3) Субъектом КИИ 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) Субъектом КИИ обеспечивается предоставление доступа с использованием мобильных технических средств к объектам доступа Значимого объекта КИИ только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);  5) В Значимом объекте КИИ обеспечивается запрет использования мобильных технических средств, на которые в Значимом объекте КИИ может быть осуществлена запись информации (перезаписываемых съемных машинных носителей информации).  6) Субъектом КИИ 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;  7) Субъектом КИИ должна обеспечиваться очистка (удаление) информации в мобильном техническом средстве:  а) при превышении допустимого числа неуспешных попыток входа в Значимый объект КИИ под конкретной учетной записью (доступа к Значимому объекту КИИ), осуществляемых с мобильного устройства;  б) при превышении допустимого интервала времени с начала осуществления попыток входа в Значимый объект КИИ под конкретной учетной записью, осуществляемых с мобильного устройства;  8) Субъектом КИИ должно обеспечиваться применение технических средств защиты периметра уровня узла, устанавливаемых на портативные вычислительные устройства;  9) Субъектом КИИ должно обеспечиваться использование радиометок (RFID-меток) для контроля вноса или выноса мобильных технических устройств из помещения и (или) контролируемой зоны в целом;  10) Субъектом КИИ обеспечивается шифрование хранимой на носителе мобильного технического средства информации с применением криптографических методов защиты информации в соответствии с законодательством Российской Федерации. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ЗИС.39 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных | Субъектом КИИ 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 Значимого объекта КИИ (сегмента Значимого объекта КИИ); * ограничение перемещения виртуальных машин (контейнеров) между сегментами Значимого объекта КИИ. | 1) Субъектом КИИ должно обеспечиваться перемещение виртуальных машин (контейнеров) и обрабатываемых на них данных в пределах Значимого объекта КИИ только на контролируемые им (или уполномоченным лицом) технические средства (сервера виртуализации, носители, системы хранения данных);  2) Субъектом КИИ должна осуществляться обработка отказов перемещения виртуальных машин (контейнеров) и обрабатываемых на них данных;  3) В Значимом объекте КИИ должны использоваться механизмы централизованного управления перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных;  4) В Значимом объекте КИИ должна быть обеспечена непрерывность регистрации событий безопасности в виртуальных машинах (контейнерах) в процессе перемещения;  5) В Значимом объекте КИИ должна осуществляться очистка освобождаемых областей памяти на серверах виртуализации, носителях, системах хранения данных при перемещении виртуальных машин (контейнеров) и обрабатываемых на них данных. | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ИНЦ.0 | Регламентация правил и процедур реагирования на компьютерные инциденты | Должны быть установлены обязанности и процедуры менеджмента для обеспечения уверенности в быстром, эффективном и надлежащем реагировании на инциденты ИБ.  Должны быть приняты во внимание следующие рекомендации для обязанностей и процедур по управлению инцидентами ИБ:  должны быть установлены обязанности по управлению, a) чтобы гарантировать, что следующие процедуры разработаны и должным образом доведены до сведения внутри организации:  1) процедуры планирования и подготовки реагирования на инциденты;  2) процедуры мониторинга, обнаружения, анализа и информирования о событиях и инцидентах ИБ;  3) процедуры регистрации действий по управлению инцидентами;  4) процедуры обращения с криминалистическими свидетельствами;  5) оценка недостатков ИБ;  6) процедуры реагирования, включая процедуры эскалации, контролируемого восстановления после инцидента и информирования персонала внутри организации, лиц за ее пределами, а также организаций;  b) установленные процедуры должны обеспечивать, что:  1) вопросы, связанные с инцидентами ИБ в организации, решает компетентный персонал;  2) существуют контактные лица по вопросам обнаружения и информирования об инцидентах безопасности;  3) поддерживаются соответствующие контакты с органами власти,  внешними заинтересованными группами или форумами, которые занимаются вопросами, связанными с инцидентами ИБ;  процедуры оповещения c) должны включать:  1) подготовку форм оповещения о событиях ИБ для обеспечения действий по оповещению и для того, чтобы лица, сообщающие о нарушениях, могли запомнить все необходимые действия в случае, если произошло событие ИБ;  2) процедуру, которая должна быть предпринята в случае, если произошло событие ИБ, например, немедленное фиксирование всех деталей, таких как вид несоответствия или нарушения, произошедший отказ, сообщения на экране и незамедлительное оповещение контактных лиц, а также принятие скоординированных действий;  3) ссылку на установленный формальный процесс принятия дисциплинарных мер к работникам, которые совершают нарушения безопасности;  4) соответствующие процессы обратной связи для обеспечения того,  чтобы лица, сообщающие о событиях ИБ, были уведомлены о результатах после решения и закрытия проблемы.  Цели управления инцидентами ИБ должны быть согласованы с руководством, и должны гарантировать, что лица, ответственные за управление инцидентами ИБ, понимают приоритеты организации при обработке инцидентов ИБ.  Инциденты ИБ могут выходить за пределы организационных и национальных границ. Для реагирования на такие инциденты возрастает необходимость в координации и обмене информацией об этих инцидентах со сторонними организациями, в той мере, насколько это возможно. |  | ISO/IEC 27002:2013,  16.1.1 |
| ИНЦ.1 | Выявление компьютерных инцидентов | Должна быть проведена оценка событий ИБ и принято решение, следует ли их классифицировать как инциденты ИБ.  Контактные лица по вопросам обнаружения и информирования об инцидентах должны оценивать каждое событие ИБ, используя согласованную шкалу классификации событий и инцидентов ИБ, и решать, следует ли классифицировать событие как инцидент ИБ. Классификация и распределение инцидентов по приоритетам может помочь в определении влияния и масштаба инцидента.  В тех случаях, когда в Субъекте КИИ есть группа реагирования на инциденты ИБ (ГРИИБ), оценка и принятие решения могут быть переданы ей для подтверждения или повторной оценки.  Результаты оценки и принятых решений должны быть подробно зафиксированы с целью обращения к ним в будущем и проверки. |  | ISO/IEC 27002:2013,  16.1.4 |
| ИНЦ.2 | Информирование о компьютерных инцидентах | Требуется незамедлительно сообщать о событиях ИБ по соответствующим каналам управления.  Все работники и подрядчики должны быть осведомлены о своей обязанности незамедлительно сообщать о событиях ИБ. Они должны быть также осведомлены о процедуре оповещения о событиях ИБ и контактных лицах, которым следует сообщать о событиях.  Ситуации, которые предполагают передачу сообщения о событии ИБ, включают в себя:  неэффективный a) контроль безопасности;  b) нарушение ожидаемого уровня целостности, конфиденциальности или доступности информации;  c) человеческие ошибки;  d) несоответствия политикам или руководствам;  e) нарушения мер физической безопасности;  f) неконтролируемые системные изменения;  g) неисправности программного или аппаратного обеспечения;  h) нарушения доступа.  Сбои или иное ненормальное поведение системы могут быть индикаторами атаки на систему защиты или фактического нарушения защиты и, следовательно, о них всегда необходимо сообщать, как о событиях ИБ. |  | ISO/IEC 27002:2013,  16.1.2 |
| ИНЦ.3 | Анализ компьютерных инцидентов | Проведение реагирования на каждый обнаруженный инцидент защиты информации, включающего:  - анализ инцидента;  - определение источников и причин возникновения инцидента;  - оценку последствий инцидента на предоставление финансовых услуг, реализацию бизнес-процессов или технологических процессов финансовой организации |  | ГОСТ Р 57580.1, РИ.12 |
| ИНЦ.4 | Устранение последствий компьютерных инцидентов | Реагирование на инциденты ИБ должно осуществляться в соответствии с документально оформленными процедурами.  Реагирование на инциденты ИБ должно осуществляться назначенными контактными лицами и другими соответствующими лицами из числа самой организации или сторонних организаций.  Реагирование должно включать в себя следующее:  как можно более быстрый сбор свидетельств a) происшедшего;  b) проведение криминалистического анализа ИБ по мере необходимости;  c) эскалация, если требуется;  d) обеспечение того, что все выполняемые действия по реагированию соответствующим образом зарегистрированы для дальнейшего анализа;  e) информирование о факте инцидента ИБ или любых существенных деталях о нем других лиц из числа самой организации или сторонних организаций в соответствии с принципом «необходимого знания»;  f) устранение недостатка(ов) ИБ, которые могут стать причиной или способствовать возникновению инцидента;  g) после того, как инцидент успешно отработан, необходимо формально закрыть и записать его.  После инцидента должен проводиться анализ для выявления первопричины инцидента.  Первоочередной целью реагирования на инцидент является возобновление  «нормального уровня безопасности», а затем инициирование необходимого восстановления. |  | ISO/IEC 27002:2013,  16.1.5 |
| ИНЦ.5 | Принятие мер по предотвращению повторного возникновения компьютерных инцидентов | Знания, приобретенные в результате анализа и урегулирования инцидентов ИБ, должны использоваться для уменьшения вероятности или влияния будущих инцидентов.  Должны быть внедрены механизмы, позволяющие количественно определять и отслеживать типы, объемы и стоимость инцидентов ИБ. Информация, полученная в результате оценки инцидентов ИБ, должна использоваться для выявления повторяющихся или значительных инцидентов.  Оценка инцидентов ИБ может указывать на необходимость в усилении или дополнении мер обеспечения ИБ для снижения частоты, ущерба и стоимости в будущем или может быть принята во внимание при пересмотре политики безопасности.  При должном внимании к аспектам конфиденциальности, истории про реальные инциденты ИБ могут быть использованы при обучении персонала в качестве примеров того, что может случиться, как реагировать на такие инциденты и как избежать их в будущем. |  | ISO/IEC 27002:2013,  16.1.6 |
| ИНЦ.6 | Хранение и защита информации о компьютерных инцидентах | Субъектом КИИ должны быть определены и применяться процедуры для идентификации, сбора, получения и сохранения информации, которая может использоваться в качестве свидетельств.  Должны быть разработаны и затем выполняться внутренние процедуры при рассмотрении свидетельств с целью принятия мер дисциплинарного и юридического характера.  В общем случае эти процедуры должны обеспечивать процессы идентификации, сбора, получения и сохранения свидетельств в зависимости от типа носителей, устройств и состояния устройств, например, включенных или выключенных. Процедуры должны учитывать:  a) цепочку поставок;  b) безопасность свидетельств;  c) безопасность персонала;  d) роли и обязанности задействованного персонала;  e) компетентность персонала;  f) документацию;  g) инструктаж.  Там, где это возможно, должна быть предусмотрена сертификация или другие соответствующие способы оценки квалификации персонала и инструментария, для того, чтобы повысить ценность сохраненных свидетельств.  Криминалистические свидетельства могут выходить за пределы организации или границы юрисдикции. В таких случаях следует обеспечить, чтобы организация имела право собирать требуемую информацию в качестве криминалистических свидетельств. Должны быть учтены требования различных юрисдикций, чтобы максимально увеличить шансы на признание в соответствующих юрисдикциях.  Идентификация – это процесс, включающий в себя поиск, распознавание и документирование возможного свидетельства.  Сбор – это процесс сбора физических предметов, которые могут содержать потенциальные свидетельства. Получение – это процесс создания копии данных в рамках определенного набора.  Сохранение – это процесс поддержания и защиты целостности и первоначального состояния потенциальных свидетельств.  Когда событие ИБ обнаружено впервые, может быть неясно, приведет ли это событие к судебному разбирательству. Следовательно, существует опасность, что необходимое свидетельство будет намеренно или случайно уничтожено до того, как выяснится серьезность инцидента. Рекомендуется заранее привлекать юриста или полицию к любым предполагаемым действиям юридического характера и прислушиваться к советам по поводу необходимых свидетельств. |  | ISO/IEC 27002:2013,  16.1.7 |
| УКФ.0 | Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы | Необходимо управлять изменениями в системах в течение жизненного цикла разработки посредством применения формализованных процедур управления изменениями.  Формальные процедуры управления изменениями должны быть задокументированы и применены для обеспечения целостности системы, приложений и продуктов, начиная с ранних этапов проектирования и до всех последующих действий по поддержке. Внедрение новых систем и значительные изменения в существующие системы должны происходить в соответствии с формальным процессом документирования, спецификации, тестирования, контроля качества и управляемой реализации.  Этот процесс должен включать оценку риска, анализ последствий от изменений и определение необходимых мер обеспечения ИБ, а также должен гарантировать, что существующие меры не будут нарушены, что программистам поддержки предоставлен доступ только к тем частям системы, которые необходимы для их работы, и что получено формальное согласие и одобрение любых изменений.  Везде, где это практически возможно, процедуры управления изменениями для приложений и среды эксплуатации должны быть объединены. Процедуры управления изменениями должны включать (но не ограничиваться) следующее:  ведение учета согласованных уровней a) разрешений;  b) обеспечение внесения изменений авторизованными пользователями;  c) пересмотр процедур управления и целостности для гарантии того, что они не будут нарушены изменениями;  d) идентификация всего программного обеспечения, информации, объектов базы данных и аппаратного обеспечения, которые требуют изменений;  e) выявление и проверка критического с точки зрения безопасности кода для минимизации вероятности реализации известных ошибок программирования;  f) получение официального одобрения на предлагаемые изменения до начала работ;  g) обеспечение того, чтобы авторизованные пользователи одобрили все изменения до их реализации;  h) обеспечение того, чтобы набор системной документации был обновлен по завершению каждого изменения, а старая документация архивировалась или удалялась;  i) поддержание контроля версий всех обновлений программного обеспечения;  j) ведение записей всех запросов на изменение;  k) обеспечение того, чтобы эксплуатационная документация и пользовательские процедуры подвергались изменениями по мере необходимости и оставались актуальными;  l) обеспечение того, чтобы внедрение изменений происходило в согласованное время и не нарушало вовлеченные бизнес-процессы.  Также как изменение программного обеспечения может повлиять на среду эксплуатации, так и наоборот.  Общепринятая практика включает в себя тестирование нового программного обеспечения в среде, отделенной как от среды эксплуатации, так и от среды разработки . Это позволит иметь средства управления над новым программным обеспечением и обеспечивает дополнительную защиту эксплуатационной информации, которая используется в целях тестирования. Это относится к пакетам обновлений и исправлений, а также к прочим типам обновлений.  В тех случаях, где рассматривается автоматическое применение обновлений, риск в отношении целостности и доступности системы должен быть сопоставлен с преимуществами быстрого развертывания обновлений. Автоматические обновления не должны использоваться в критических системах, так как некоторые из них могут привести к сбою критических приложений. |  | ISO/IEC 27002:2013,  п. 14.2.2 |
| УКФ.1 | Идентификация объектов управления конфигурацией | Информация, средства обработки информации и другие активы, связанные с информацией, должны быть идентифицированы, а также должен быть составлен и  поддерживаться в актуальном состоянии перечень этих активов.  Организация должна идентифицировать активы, относящиеся к жизненному циклу информации, и задокументировать их значимость. Жизненный цикл информации должен включать в себя создание, обработку, хранение, передачу, удаление и уничтожение. Документация должна храниться в специально созданных или уже существующих перечнях, в зависимости от ситуации.  Перечень активов должен быть точным, актуальным, полным и согласованным с другими инвентаризационными перечнями.  Для каждого актива, включенного в перечень, должен быть определен его владелец и проведено категорирование .  Инвентаризация активов помогает обеспечить эффективную защиту и может  также потребоваться для других целей, таких как здоровье и безопасность, страхование или финансы (управление активами).  ИСО/МЭК 27005 предоставляет примеры активов, которые могут быть приняты во внимание Субъектом КИИ в процессе идентификации активов. Процесс составления перечня активов является важной предпосылкой управления рисками |  | ISO/IEC 27002:2013,  п. 8.1.1 |
| УКФ.2 | Управление изменениями | Необходимо обеспечить управление изменениями в организации, бизнес-процессах, средствах обработки информации и системах, влияющих на ИБ.  Руководство по применению  В частности, необходимо принять во внимание следующее:  a) идентификацию и регистрацию существенных изменений;  b) планирование и тестирование изменений;  c) оценку потенциального влияния от реализации существенных изменений, включая влияние на ИБ;  d) процедуры утверждения предлагаемых изменений;  e) подтверждение того, что выполняются требования по ИБ;  f) информирование об изменении всех заинтересованных лиц;  g) процедуры по возврату в исходное состояние, включая процедуры и обязанности по прерыванию процесса и последующего восстановления после неудачных изменений и непредвиденных событий;  h) установление процесса экстренного изменения для обеспечения быстрой и управляемой реализации изменений, необходимых для разрешения инцидента.  С целью обеспечения уверенности в надлежащем контроле всех изменений, должна быть формально определена ответственность и разработаны соответствующие процедуры управления. При внесении изменений вся необходимая информация должна быть сохранена в контрольном журнале.  Неадекватный контроль над изменениями в средствах и системах обработки информации является распространенной причиной системных сбоев или нарушений безопасности . |  | ISO/IEC 27002:2013,  п. 12.1.2 |
| УКФ.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения | Должны быть установлены и реализованы правила, регулирующие установку программного обеспечения пользователями.  Организация должна определить и закрепить строгую политику в отношении того, какие типы программного обеспечения могут устанавливать пользователи.  Следует исходить из принципа наименьших привилегий. В случае предоставления определенных привилегий, пользователи могут иметь возможность устанавливать программное обеспечение. Организация должна определить, какие виды установок разрешены (например, обновления и исправления безопасности для существующего программного обеспечения) и какие виды запрещены (например, программное обеспечение, предназначенное только для личного использования, и неизвестное программное обеспечение, которое потенциально может быть вредоносным). Эти привилегии должны предоставляться с учетом ролей соответствующих пользователей.  Неконтролируемая установка программного обеспечения на вычислительные устройства может привести к появлению уязвимостей, а затем к утечке информации, нарушению целостности или другим инцидентами ИБ, либо к нарушению прав на интеллектуальную собственность. |  | ISO/IEC 27002:2013,  п. 12.6.2 |
| УКФ.4 | Контроль действий по внесению изменений | Везде, где это практически возможно, процедуры управления изменениями для приложений и среды эксплуатации должны быть объединены. Процедуры управления изменениями должны включать (но не ограничиваться) следующее:  ведение учета согласованных уровней a) разрешений;  b) обеспечение внесения изменений авторизованными пользователями;  c) пересмотр процедур управления и целостности для гарантии того, что они не будут нарушены изменениями;  d) идентификация всего программного обеспечения, информации, объектов базы данных и аппаратного обеспечения, которые требуют изменений;  e) выявление и проверка критического с точки зрения безопасности кода для минимизации вероятности реализации известных ошибок программирования;  f) получение официального одобрения на предлагаемые изменения до начала работ;  g) обеспечение того, чтобы авторизованные пользователи одобрили все изменения до их реализации;  h) обеспечение того, чтобы набор системной документации был обновлен по завершению каждого изменения, а старая документация архивировалась или удалялась;  i) поддержание контроля версий всех обновлений программного обеспечения;  j) ведение записей всех запросов на изменение;  k) обеспечение того, чтобы эксплуатационная документация и пользовательские процедуры подвергались изменениями по мере необходимости и оставались актуальными;  l) обеспечение того, чтобы внедрение изменений происходило в согласованное время и не нарушало вовлеченные бизнес-процессы.  Также как изменение программного обеспечения может повлиять на среду эксплуатации, так и наоборот.  Общепринятая практика включает в себя тестирование нового программного обеспечения в среде, отделенной как от среды эксплуатации, так и от среды разработки . Это позволит иметь средства управления над новым программным обеспечением и обеспечивает дополнительную защиту эксплуатационной информации, которая используется в целях тестирования. Это относится к пакетам обновлений и исправлений, а также к прочим типам обновлений.  В тех случаях, где рассматривается автоматическое применение обновлений, риск в отношении целостности и доступности системы должен быть сопоставлен с преимуществами быстрого развертывания обновлений. Автоматические обновления не должны использоваться в критических системах, так как некоторые из них могут привести к сбою критических приложений. |  | ISO/IEC 27002:2013,  п. 14.2.2 |
| ОПО.0 | Регламентация правил и процедур управления обновлениями программного обеспечения | а. Выявлять, сообщать и устранять дефекты системы;  b. Перед установкой необходимо тестировать обновления программного обеспечения и прошивки, устраняющие дефекты, на предмет эффективности и потенциальных побочных эффектов;  c. Устанавливать обновления программного обеспечения и микропрограмм, относящихся к безопасности, в течение [Назначение: период времени, определяемый организацией] после выпуска обновлений;  d. Включить устранение дефектов в процесс управления конфигурацией организации.  Обсуждение: необходимость исправления системных дефектов относится ко всем типам программного обеспечения и прошивок. Организации выявляют системы, подверженные дефектам программного обеспечения, включая потенциальные уязвимости, возникающие в результате этих дефектов, и сообщают эту информацию назначенному персоналу организации, отвечающему за информационную безопасность и конфиденциальность. Обновления, относящиеся к безопасности, включают исправления, пакеты обновления и сигнатуры вредоносного кода. Организации также обращаются к недостаткам, обнаруженным во время оценок, постоянного мониторинга, действий по реагированию на инциденты и обработки системных ошибок. Отслеживание и проверка необходимые действия по исправлению осуществляется путем включения устранения дефектов в процессы управления конфигурацией.  Определенные Субъектом КИИ периоды времени для обновления программного обеспечения и микропрограмм, относящихся к безопасности, могут варьироваться в зависимости от множества факторов риска, включая категорию безопасности системы, критичность обновления (т.е. серьезность уязвимости, связанной с обнаруженным дефектом), терпимость организации к риску, миссия, поддерживаемая системой, или среда угроз. Для устранения некоторого типа дефектов может потребоваться большее количество тестов. Организации определяют тип тестирования, необходимого для определенного типа рассматриваемой деятельности по устранению дефектов, и типы изменений, которые должны быть произведены в конфигурации. В некоторых ситуациях организации могут решить, что тестирование обновлений программного обеспечения или микропрограмм не является необходимым, например, при простом обновлении сигнатур вредоносного кода. При принятии решений о тестировании организации учитывают, получены ли обновления программного обеспечения или прошивки, имеющие отношение к безопасности, из авторизованных источников с соответствующими цифровыми подписями. | (1) УСТРАНЕНИЕ ДЕФЕКТОВ | ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ  (2) УСТРАНЕНИЕ ДЕФЕКТОВ | СОСТОЯНИЕ АВТОМАТИЧЕСКОГО УСТРАНЕНИЯ ДЕФЕКТОВ  Определить, установлены ли в компонентах системы соответствующие обновления программного обеспечения и микропрограмм, относящиеся к безопасности, с помощью [Назначение: автоматические механизмы, определенные организацией] с [Назначение: частота, определенная организацией].  Обсуждение: Автоматизированные механизмы могут отслеживать и определять статус известных дефектов для компонентов системы.  Связанные элементы контроля: CA-7, SI-4.  (3) УСТРАНЕНИЕ ДЕФЕКТОВ | ВРЕМЯ ДЛЯ ИСПРАВЛЕНИЯ ДЕФЕКТОВ И БЕНЧМАРКИНГ ДЛЯ КОРРЕКТИРУЮЩИХ ДЕЙСТВИЙ  (а) Измерить время между выявлением дефектов и их устранением; и  (b) Установить следующие критерии для принятия корректирующих действий: [Назначение: критерии, определенные организацией].  Обсуждение: организации определяют время, которое в среднем требуется для исправления дефектов системы после того, как такие недостатки были обнаружены, и впоследствии устанавливают организационные контрольные показатели (т.е. SLA) для принятия корректирующих действий. Контрольные показатели могут быть установлены по типу недостатка или серьезности потенциальной уязвимости, если уязвимость может быть использована.  Связанные элементы контроля: Нет.  (4) УСТРАНЕНИЕ ДЕФЕКТОВ | ИНСТРУМЕНТЫ АВТОМАТИЧЕСКОГО ПАТЧ-МЕНЕДЖМЕНТА  Использовать автоматизированные инструменты управления исправлениями, чтобы облегчить устранение дефектов в следующих компонентах системы: [Назначение: системные компоненты, определенные организацией].  Обсуждение: использование автоматизированных инструментов патч-менеджмента помогает обеспечить своевременность и полноту операций по установке обновлений системы.  Связанные элементы контроля: Нет.  (5) УСТРАНЕНИЕ ДЕФЕКТОВ | АВТОМАТИЧЕСКИЕ ОБНОВЛЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ  Устанавливать [Назначение: определенные Субъектом КИИ обновления программного обеспечения и микропрограмм] автоматически в [Назначение: системные компоненты, определенные организацией].  Обсуждение: из-за проблем с целостностью и доступностью системы организации рассматривают методологию, используемую для выполнения автоматических обновлений. Организации балансируют между необходимостью обеспечить, чтобы обновления были установлены как можно скорее, с необходимостью поддерживать управление конфигурацией и контроль с любыми задачами или операционными воздействиями, которые могут иметь автоматические обновления.  Связанные элементы контроля: Нет.  (6) УСТРАНЕНИЕ ДЕФЕКТОВ | УДАЛЕНИЕ ПРЕДЫДУЩИХ ВЕРСИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ПРОШИВОК  Удаление предыдущие версии [Назначение: программное обеспечение и компоненты микропрограмм, определяемые организацией] после установки обновленных версий.  Обсуждение: предыдущие версии программного обеспечения или компонентов прошивки, которые не удаляются из системы после установки обновлений, могут быть использованы злоумышленниками. Некоторые продукты могут автоматически удалять из системы предыдущие версии программного обеспечения и прошивки. | NIST Special Publication 800-53 Revision 5 |
| ОПО.1 | Поиск, получение обновлений программного обеспечения от доверенного источника | Контроль целостности и достоверности источников получения при распространении и (или) обновлении ПО АС, ПО средств и систем защиты информации, системного ПО |  | ГОСТ Р 57580.1, ЦЗИ.19 |
| ОПО.2 | Контроль целостности обновлений программного обеспечения | Проверить инструменты обслуживания, с целью убедиться, что установлены последние обновления программного обеспечения и патчи.  Инструменты обслуживания, использующие устаревшее и / или не имеющее исправлений программное обеспечение, могут обеспечить вектор угроз для злоумышленников и привести к значительной уязвимости для организаций. |  | NIST Special Publication 800-53 Revision 5 |
| ОПО.3 | Тестирование обновлений программного обеспечения | Для новых информационных систем, обновлений и новых версий должны быть разработаны программы приемо-сдаточных испытаний и установлены связанные с ними критерии.  Приемочные испытания должны включать в себя проверку выполнения требований по ИБ и соблюдение правил безопасной разработки системы. Тестирование также должно проводиться в отношении заимствованных компонентов и интегрированных систем. Организации могут использовать автоматизированные инструменты, такие как анализаторы кода или сканеры уязвимостей, и должны гарантировать исправление связанных с безопасностью дефектов.  Испытания должны проводится в реалистичной среде тестирования, чтобы гарантировать надежность результатов, и, что система не будет создавать дополнительные уязвимости в среде организации. |  |  |
| ОПО.4 | Установка обновлений программного обеспечения | Субъектом КИИ должен осуществляться контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.  Субъектом КИИ 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 Значимом объекте КИИ и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.  Контроль установки обновлений проводится с периодичностью, установленной Субъектом КИИ 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, баз решающих правил систем обнаружения вторжений, 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 Субъекта КИИ по защите информации. | 1) Субъектом КИИ должна осуществляться проверка корректности функционирования обновлений в тестовой среде с обязательным оформлением результатов проверки в соответствующем журнале;  2) Субъектом КИИ обеспечивается регламентация и контроль обновлений программного обеспечения базовой системы ввода-вывода (иного микропрограммного обеспечения). | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ПЛН.0 | Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации | В рамках функционирования системы безопасности субъектом критической информационной инфраструктуры должны быть внедрен процесс планирования и разработка мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры;  В ходе планирования мероприятий по обеспечению безопасности значимого объекта осуществляются:  а) определение лиц, ответственных за планирование и контроль мероприятий по обеспечению безопасности значимого объекта;  б) разработка, утверждение и актуализация плана мероприятий по обеспечению безопасности значимого объекта;  в) определения порядка контроля выполнения мероприятий по обеспечению безопасности значимого объекта, предусмотренных утвержденным планом.  Планирование мероприятий по обеспечению безопасности значимого объекта должно осуществляться в рамках процесса планирования, внедренного в соответствии с требованиями к созданию систем безопасности значимых объектов и обеспечению их функционирования, утвержденными в соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». |  | Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования (утв. приказом ФСТЭК России от 21 декабря 2017 г. № 235), п. 28;  Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утв. приказом ФСТЭК России от 25 декабря 2017 г. № 239), п. 13.1 |
| ПЛН.1 | Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации | Организационно-распорядительные документы по безопасности значимых объектов должны определять планы мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры.  В рамках планирования мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры осуществляются разработка и утверждение ежегодного плана мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры (далее - план мероприятий).  По решению субъекта критической информационной инфраструктуры план мероприятий может разрабатываться на более длительный срок с учетом имеющихся программ (планов) по модернизации, оснащению значимых объектов критической информационной инфраструктуры.  План мероприятий разрабатывается структурным подразделением по безопасности, специалистами по безопасности с участием подразделений (работников), эксплуатирующих значимые объекты критической информационной инфраструктуры, и подразделений (работников), обеспечивающих функционирование значимых объектов критической информационной инфраструктуры.  В план мероприятий должны включаться мероприятия по обеспечению безопасности значимых объектов критической информационной инфраструктуры, функционирующих в обособленных подразделениях (филиалах, представительствах) субъекта критической информационной инфраструктуры.  План мероприятий должен содержать наименования мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры, сроки их выполнения, наименования подразделений (работников), ответственных за реализацию каждого мероприятия.  В план мероприятий включаются мероприятия по обеспечению функционирования системы безопасности, а также организационные и технические мероприятия по обеспечению безопасности значимых объектов критической информационной инфраструктуры, направленные на решение задач, установленных пунктом 6 требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования.  Разработка мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры осуществляется в соответствии с требованиями к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, требованиями по безопасности, иными нормативными правовыми актами по обеспечению безопасности критической информационной инфраструктуры, а также организационно-распорядительными документами по безопасности значимых объектов.  План мероприятий утверждается руководителем субъекта критической информационной инфраструктуры и доводится до подразделений (работников) субъекта критической информационной инфраструктуры в части, их касающейся.  В подразделениях, эксплуатирующих значимые объекты критической информационной инфраструктуры, и подразделениях, обеспечивающих функционирование значимых объектов критической информационной инфраструктуры, на основе утвержденного плана мероприятий могут разрабатываться соответствующие отдельные планы мероприятий.  Мероприятия по обеспечению безопасности значимых объектов критической информационной инфраструктуры могут включаться в общий план деятельности субъекта критической информационной инфраструктуры (в случае его разработки) отдельным разделом.  Порядок разработки, утверждения и внесения изменений в план мероприятий определяется субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимых объектов. |  | Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования (утв. приказом ФСТЭК России от 21 декабря 2017 г. № 235), п. 25, пп. 29-31, п. 33 |
| ПЛН.2 | Контроль выполнения мероприятий по обеспечению защиты информации | Контроль за выполнением плана мероприятий осуществляется структурным подразделением по безопасности, специалистами по безопасности.  Структурное подразделение по безопасности, специалисты по безопасности ежегодно должны готовить отчет о выполнении плана мероприятий, который представляется руководителю субъекта критической информационной инфраструктуры.  Результаты реализации мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры подлежат документированию в порядке, установленном субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимых объектов. |  | Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования (утв. приказом ФСТЭК России от 21 декабря 2017 г. № 235), п. 32, п. 34 |
| ДНС.0 | Регламентация правил и процедур обеспечения действий в нештатных ситуациях | Организация должна определить свои требования к ИБ и менеджменту непрерывности ИБ при неблагоприятных ситуациях, например, во время кризиса или бедствия.  Организация должна определить, обеспечивается ли непрерывность ИБ в рамках процесса менеджмента непрерывностью бизнеса или в рамках процесса менеджмента восстановления после чрезвычайных ситуаций. Требования ИБ должны быть определены при планировании непрерывности бизнеса и восстановления после чрезвычайных ситуаций. При отсутствии формально утвержденных планов непрерывности бизнеса и восстановления после чрезвычайных ситуаций, управление ИБ должно исходить из того, что требования ИБ в неблагоприятных ситуациях те же, что и при обычных условиях. В качестве альтернативы организация может провести анализ влияния на бизнес в разрезе аспектов ИБ, чтобы определить требования ИБ, которые применимы в неблагоприятных ситуациях. Чтобы сократить время и затраты на дополнительный анализ влияния на бизнес, рекомендуется учитывать аспекты ИБ в рамках обычного анализа влияния на менеджмент непрерывности бизнеса или восстановления после чрезвычайных ситуаций. Это предполагает, что требования к непрерывности ИБ четко сформулированы в процессах менеджмента непрерывности бизнеса или восстановления после чрезвычайных ситуаций. |  | ISO/IEC 27002:2013, п. 17.1.1 |
| ДНС.1 | Разработка плана действий в нештатных ситуациях | Организация должна установить, документировать, реализовать и поддерживать процессы, процедуры, а также меры для обеспечения требуемого уровня непрерывности ИБ при неблагоприятных ситуациях.  Организация должна обеспечить следующее:  a) наличие адекватной структуры управления по подготовке, реагированию и снижению последствий от неблагоприятных событий, включающей персонал, обладающий необходимым опытом, компетенциями и полномочиями;  b) утверждение ответственного персонала по реагированию на инциденты, обладающего необходимыми полномочиями и компетенциями, для управления инцидентами и обеспечения ИБ;  c) разработку и утверждение документированных планов, процедур реагирования и восстановления, подробно описывающих, как организация будет справляться с неблагоприятным событием и будет поддерживать ИБ на заранее определенном уровне, основанном на утвержденных руководством целях обеспечения непрерывности ИБ.  В соответствии с требованиями непрерывности ИБ организация должна установить, задокументировать, реализовать и поддерживать:  a) меры ИБ в процессах обеспечения непрерывности бизнеса или восстановления после аварийных ситуаций, процедуры, вспомогательные системы и инструменты;  b) процессы, процедуры и изменения для поддержания существующих мер обеспечения ИБ во время неблагоприятных ситуаций;  c) компенсирующие меры для тех мер обеспечения ИБ, которые не могут поддерживаться во время неблагоприятной ситуации.  В контексте непрерывности бизнеса или восстановления после аварий могут быть определены конкретные процессы и процедуры. Информация, обрабатываемая в рамках этих процессов и процедур или поддерживающих информационных систем, должна быть защищена. Поэтому организация должна привлекать специалистов по ИБ при создании, внедрении и поддержке процессов и процедур обеспечения непрерывности бизнеса или восстановления после аварий.  Внедренные меры обеспечения ИБ должны оставаться работоспособными в неблагоприятных ситуациях. Если меры не могут продолжать выполнять свои функции по защите информации, следует определить, внедрить и поддерживать другие меры для обеспечения приемлемого уровня ИБ. |  | ISO/IEC 27002:2013, п. 17.1.2 |
| ДНС.2 | Обучение и отработка действий персонала в нештатных ситуациях | Субъект КИИ не реже одного раза в год организует и проводит тренировки по отработке мероприятий плана. Объем и содержание тренировки определяются субъектом критической информационной инфраструктуры с учетом мероприятий, содержащихся в плане.  Организация и проведение тренировок возлагаются на подразделения и должностных лиц субъекта критической информационной инфраструктуры, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак. |  | ФСБ 282: П.10 |
| ДНС.3 | Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций | Хранить носители с резервными копиями в безопасном месте, желательно в удаленном подразделении, например, в альтернативном или резервном месте, либо на территории организации, обеспечивающей безопасное хранение. Проверять безопасность этого места не реже раза в год. |  | PCI DSS: 9.5.1 |
| ДНС.4 | Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций | Субъектом КИИ должно обеспечиваться резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования Значимого объекта КИИ, предусматривающее:  определение сегментов Значимого объекта КИИ, 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 Значимого объекта КИИ и доступности информации, установленных оператором;  применение резервных (дублирующих) технических средств, программного обеспечения, каналов передачи информации и (или) средств обеспечения функционирования Значимого объекта КИИ, обеспечивающих требуемые условия непрерывности функционирования Значимого объекта КИИ и доступности информации;  ввод в действие резервного технического средства, программного обеспечения, канала передачи информации или средства обеспечения функционирования при нарушении требуемых условий непрерывности функционирования Значимого объекта КИИ и доступности информации.  Резервирование технических средств в зависимости от требуемых условий обеспечения непрерывности функционирования Значимого объекта КИИ 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 Значимого объекта КИИ и доступности информации.  Резервирование каналов передачи информации включает:  резервирование каналов связи, обеспечивающее снижение вероятности отказа в доступе к Значимому объекту КИИ;  наличие у основных и альтернативных поставщиков телекоммуникационных услуг (провайдеров) Значимого объекта КИИ планов по восстановлению связи при авариях и сбоях, с указанием времени восстановления.  Резервирование средств обеспечения функционирования Значимого объекта КИИ включает:  использование кратковременных резервных источников питания для обеспечения правильного (корректного) завершения работы сегмента Значимого объекта КИИ (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 Значимого объекта КИИ (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 Субъекта КИИ по защите информации. | 1) В Значимом объекте КИИ 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 Субъектом КИИ процедур обеспечения требуемых условий обеспечения непрерывности функционирования Значимого объекта КИИ 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 Значимом объекте КИИ должно обеспечиваться предоставление резервных каналов связи от альтернативных поставщиков телекоммуникационных услуг (провайдеров), отличных от поставщиков (провайдеров) основных каналов связи;  3) В Значимом объекте КИИ должно обеспечиваться использование резервных каналов связи, проходящих по трассам, отличным от трасс прохождения основных каналов связи;  4) В Значимом объекте КИИ должно обеспечиваться использование резервных (отделенных от основных) телекоммуникационных сервисов, обеспечивающих доступность информации, до восстановления доступности основных телекоммуникационных сервисов поставщиком телекоммуникационных услуг (провайдером). | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ДНС.5 | Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций | Субъектом КИИ должна быть предусмотрена возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.  Для обеспечения возможности восстановления программного обеспечения в Значимом объекте КИИ 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 Значимого объекта КИИ в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей Значимого объекта КИИ, определенных оператором, позволяющих решать задачи по обработке информации.  Субъектом КИИ 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 Субъекта КИИ по защите информации. | 1) Субъектом КИИ обеспечивается восстановление отдельных функциональных возможностей Значимого объекта КИИ с применением резервированного программного обеспечения зеркальной Значимого объекта КИИ (сегмента Значимого объекта КИИ, технического средства, устройства) | Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.) |
| ДНС.6 | Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения | Контроль:  а. Разработать план действий в чрезвычайных ситуациях для системы, который:  1. Определяет основные миссии и бизнес-функции и связанные с ними требования на случай непредвиденных обстоятельств;  2. Определяет цели восстановления, приоритеты восстановления и критерии;  3. Обращается к непредвиденным ролям, обязанностям, назначенным лицам с контактной информацией;  4. Обращается к поддержанию основных миссий и бизнес-функций, несмотря на сбой, компрометацию или сбой системы;  5. Регламентирует возможное полное восстановление системы без ухудшения изначально запланированных и реализованных средств управления;  6. Обращается внимание на обмен информацией о непредвиденных обстоятельствах; и  7. Рассматривается и утверждается [Назначение: персонал или роли, определенные организацией];  b. Распространение плана действий в чрезвычайных ситуациях на [Назначение: определенный Субъектом КИИ ключевой персонал на случай нештатной ситуации (идентифицированный по имени и/или роли) и организационные элементы];  c. Координировать действия по планированию действий в чрезвычайных ситуациях с действиями по управлению инцидентами  d. Рассмотреть план действий в чрезвычайных ситуациях для системы с [Назначение: частота, определяемая организацией];  е. Обновлять план действий в чрезвычайных ситуациях, для учета изменений в организации, системе или операционной среде, а также проблемы, возникшие во время реализации, выполнения или апробации плана действий в чрезвычайных ситуациях;  f. Информировать об изменениях плана действий в чрезвычайных ситуациях [Назначение: определенный Субъектом КИИ ключевой персонал на случай нештатных ситуаций (идентифицированный по имени и / или роли) и организационные элементы];  g. Включить, извлеченные из тестирования плана, обучения или фактических действий полезный опыт в план; и  h. Обеспечить конфиденциальность и неизменность плана.  Обсуждение:  Планирование на случай чрезвычайных обстоятельств для систем является частью общей программы обеспечения непрерывности бизнес-процессов и миссии для организации. Планирование касается восстановления системы и реализации альтернативной миссии или бизнес-процессов, на случай компрометации или вторжения в систему. Планирование рассматривается на протяжении всего жизненного цикла разработки системы и является фундаментальной частью ее проектирования. Системы должны быть спроектированы с целью отказоустойчивости, при использовании резервного копирования. План отражает требуемую степень восстановления системы для достижения непрерывности операций. Цели восстановления системы отражают применимые к системе законы, распоряжения, директивы, постановления, политики, стандарты, руководящие принципы, устойчивость к организационным рискам и уровень воздействия на систему. Действия, указанные в планах, включают упорядоченную деградацию системы, завершение работы системы, переход в ручной режим, альтернативные информационные потоки и работу в режимах, зарезервированных для случаев, когда системы подвергаются атаке. Необходимо координировать план с действиями по обработке инцидентов, организации предусматривают необходимые действия в плане и их выполнение в случае инцидента. Организации рассматривают, противоречит ли непрерывность операций во время инцидента возможности автоматического отключения системы, как указано в IR-4 (5). План реагирования на инциденты является частью плана действий в нештатных ситуациях. | (1) ПЛАН ДЕЙСТВИЙ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ | СОГЛАСОВАНИЕ СО СМЕЖНЫМИ ПЛАНАМИ  Координация плана с ответственными.  Обсуждение: планы, которые связаны с действиями в чрезвычайных ситуациях включают планы обеспечения непрерывности бизнеса, планы аварийного восстановления, планы критически важной инфраструктуры, планы непрерывности операций, планы кризисных коммуникаций, планы реализации внутренних угроз, планы реагирования на утечки данных, планы реагирования на инциденты кибербезопасности, планы реагирования на нарушения, и планы действий в чрезвычайных ситуациях.  Связанные элементы управления: Нет.  (2) ПЛАН ДЕЙСТВИЙ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ | ПЛАНИРОВАНИЕ МОЩНОСТЕЙ  Планировать ресурсы таким образом, чтобы во время непредвиденных обстоятельств существовала необходимая мощность для обработки информации, коммуникации и защиты окружающей среды.  Обсуждение: Планирование мощностей необходимо, поскольку различные угрозы могут привести к сокращению доступных услуг обработки, телекоммуникаций и поддержки, предназначенных для поддержки важных миссий и бизнес-функций. Организации ожидают ухудшения работы во время аварийных операций и учитывают ухудшение при планировании мощностей. При планировании мощностей, защита окружающей среды относится к любому экологическому фактору, для которого организация определяет, что ей необходимо обеспечить поддержку, даже если она находится в ухудшенном состоянии. Такие определения основаны на организационной оценке риска, категоризации системы (уровень воздействия) и допустимости организационного риска.  Связанные элементы контроля: PE-11, PE-12, PE-13, PE-14, PE-18, SC-5.  (3) ПЛАН ДЕЙСТВИЙ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ | ВОЗОБНОВЛЕНИЕ МИССИИ И БИЗНЕС-ФУНКЦИЙ  План возобновления [Выбор: все; основные] миссия и бизнес-функции в [Назначение: период времени, определенный организацией] активации плана действий в чрезвычайных ситуациях.  Обсуждение: Организации могут выбрать проведение мероприятий по планированию на случай нештатных ситуаций для возобновления миссии и бизнес-функций в рамках планирования непрерывности бизнеса или в рамках анализа воздействия на бизнес. Организации отдают предпочтение возобновлению миссии и бизнес-функций. Период времени для возобновления миссии и бизнес-функций может зависеть от серьезности и степени сбоев в системе и поддерживающей ее инфраструктуре.  Связанные элементы контроля: Нет.  (4) ПЛАН ДЕЙСТВИЙ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ | ВОЗОБНОВЛЕНИЕ ВСЕХ МИССИЙ И БИЗНЕС-ФУНКЦИЙ  (Выведено: включено в CP-2(3).)  (5) ПЛАН ДЕЙСТВИЙ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ | ПРОДОЛЖЕНИЕ МИССИИ И БИЗНЕС-ФУНКЦИЙ  План продолжения [Выбор: все; основная] миссии и бизнес-функции с минимальными или их отсутствием потерь и поддержка этой непрерывности до полного восстановления системы на ключевых участках и/или местах хранения.  Обсуждение: Организации могут выбрать проведение мероприятий по планированию на случай непредвиденных обстоятельств, чтобы продолжить выполнение миссии и бизнес-функций в рамках планирования непрерывности бизнеса или анализа воздействия на бизнес. Ключевые участки и/или места хранения, включенные в план, могут изменяться в зависимости от обстоятельств.  Связанные элементы контроля Нет.  (6) ПЛАН ДЕЙСТВИЙ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ | МЕСТА АЛЬТЕРНАТИВНОЙ ОБРАБОТКИ И ХРАНЕНИЯ  План передачи [Выборка: все; основная] миссии и бизнес-функции на альтернативные площадок обработки и/или места хранения с минимальной потерей непрерывности работы или без нее и поддержание этой непрерывности посредством восстановления системы в ключевых участках и/или местах хранения.  Обсуждение: Организации могут выбрать проведение мероприятий по планированию действий в чрезвычайных ситуациях для альтернативных площадок обработки и хранения в рамках планирования непрерывности бизнеса или анализа воздействия на бизнес. Ключевые участки и/или места хранения, включенные в план, могут изменяться.  Связанные элементы контроля: Нет.  (7) ПЛАН ДЕЙСТВИЙ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ | КООРДИНАЦИЯ С ВНЕШНИМИ ПОСТАВЩИКАМИ УСЛУГ  Координировать план действий в чрезвычайных ситуациях с планами действий в чрезвычайных ситуациях внешних поставщиков услуг, чтобы обеспечить выполнение требований в чрезвычайных ситуациях.  Обсуждение: Когда способность организации выполнять свою миссию и бизнес-функции зависит от внешних поставщиков услуг, разработка всеобъемлющего и своевременного плана действий в чрезвычайных ситуациях может стать более сложной задачей. Когда миссия и бизнес-функции зависят от внешних поставщиков услуг, организации координируют действия по планированию действий в чрезвычайных ситуациях с внешними организациями, чтобы гарантировать, что отдельные планы отражают общие потребности организации в нештатных ситуациях.  Связанные элементы контроля: SA-9.  (8) ПЛАН ДЕЙСТВИЙ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ | ИДЕНТИФИКАЦИЯ КРИТИЧЕСКИХ АКТИВОВ  Определить критически важные системные активы, поддерживающие [Выбор: все; основные] миссии и бизнес-функции.  Обсуждение: Организации могут выбрать определение критических активов как часть анализа критичности, планирования непрерывности бизнеса или анализа воздействия на бизнес. Организации идентифицируют критические системные активы, чтобы можно было использовать дополнительные средства контроля (помимо средств контроля, которые обычно используются), чтобы гарантировать, что миссия организации и бизнес-функции не будут прерваны в чрезвычайных ситуациях. Идентификация критически важных информационных активов также облегчает определение приоритетов ресурсов организации. Критические системные активы включают технические и эксплуатационные аспекты. Технические аспекты включают компоненты системы, ИТ-услуги, продукты и механизмы информационных технологий. К операционным аспектам относятся процедуры (т.е. операции, выполняемые вручную) и персонал (т.е. лица, осуществляющие технический контроль и/или выполняющие процедуры вручную). Планы защиты программ организации могут помочь в выявлении важнейших активов. Если критически важные активы находятся внутри или поддерживаются внешними поставщиками услуг, организации рассматривают внедрение CP-2 (7) как средство повышения контроля. |  |
| ИПО.0 | Регламентация правил и процедур информирования и обучения персонала | Организационно-распорядительные документы по безопасности значимых объектов должны определять порядок информирования и обучения работников |  | Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования (утв. приказом ФСТЭК России от 21 декабря 2017 г. № 235), п. 25, пп. «а» |
| ИПО.1 | Информирование персонала об угрозах безопасности информации и о правилах безопасной работы | Субъект критической информационной инфраструктуры должен проводить не реже одного раза в год организационные мероприятия, направленные на повышение уровня знаний работников по вопросам обеспечения безопасности критической информационной инфраструктуры и о возможных угрозах безопасности |  | Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования (утв. приказом ФСТЭК России от 21 декабря 2017 г. № 235), п. 15 |
| ИПО.2 | Обучение персонала правилам безопасной работы | Все работники организации и при необходимости подрядчики должны быть надлежащим образом обучены, практически подготовлены и на регулярной основе осведомлены об обновлениях политик и процедур ИБ организации, необходимых для выполнения их функциональных обязанностей.  Программа повышения осведомленности в области ИБ должна быть направлена на то, чтобы работники и, в соответствующих случаях, подрядчики понимали свои обязанности по обеспечению ИБ и средства, с помощью которых эти обязанности выполняются. Программа повышения осведомленности в области ИБ должна быть разработана в соответствии с политикой и соответствующими процедурами ИБ организации, принимая во внимание информацию и меры обеспечения ИБ, которые внедрены для её защиты. Программа должна включать в себя ряд мероприятий, таких как кампании по повышению осведомленности (например, «День информационной безопасности») и выпуск буклетов или информационных бюллетеней.  Программа повышения осведомленности должна планироваться с учетом роли работников в Субъекте КИИ и, при необходимости, ожиданий организации в отношении осведомленности подрядчиков. Мероприятия в рамках программы должны быть рассчитаны на длительный период, предпочтительно быть регулярными, повторялись и охватывали новых работников и подрядчиков. Следует регулярно обновлять программу, чтобы она соответствовала политикам и процедурам организации и основывалась на уроках, извлеченных из инцидентов ИБ. |  | ISO/IEC 27002:2013, п. 7.2.2 |
| ИПО.3 | Проведение практических занятий с персоналом по правилам безопасной работы | При внедрении организационных мер по обеспечению безопасности значимого объекта осуществляется отработка действий пользователей и администраторов значимого объекта по реализации мер по обеспечению безопасности значимого объекта |  | Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утв. приказом ФСТЭК России от 25 декабря 2017 г. № 239), п. 12.3, пп. «д» |
| ИПО.4 | Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы | Проведение проверок знаний работников Субъекта КИИ в части применения мер защиты информации в рамках процесса системы защиты информации |  | ГОСТ Р 57580.1, КЗИ.7 |