Код меры	Наименование меры	Частота совпадений
ЗИС.35.5	Обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри инфраструктуры, в том числе для	18
УПД.6.2	Блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при	17
УПД.1.9	Предоставление пользователям прав доступа к объектам доступа, основываясь на задачах, решаемых пользователя	16
ЗИС.35.2	Обеспечение доверенных канала, маршрута внутри инфраструктуры между администратором, пользователем и сре	16
УПД.2.1	Реализация дискреционного метода управления доступом, предусматривающего управление доступом субъектов д	15
УПД.2.2	Реализация ролевого метода управления доступом, предусматривающего управление доступом субъектов доступа	15
УПД.4.1	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование инф	15
ЗИС.19.1	Защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (под	15
ЗИС.35.4	Отключение неиспользуемых сетевых протоколов компонентами инфраструктуры, хостовой операционной системь	15
УПД.2.3	Реализация мандатного метода управления доступом, предусматривающего управление доступом субъектов досту	15
ЗИС.35.7	Семантический и статистический анализ сетевого трафика вычислительной сети	15
ЗИС.35.1	Фильтрация сетевого трафика, в том числе между внешними сетями и внутренними, в том числе при организации се	15
ЗИС.27.1	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сете	14
ИАФ.1.4	Многофакторная (двухфакторная) аутентификация пользователей	14
УПД.14.1	Предоставление доступа только авторизованным (уполномоченным) пользователям	13
АУД.2.1	Выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (об	13
ЗИС.35.6	Обеспечение изоляции потоков данных, передаваемых и обрабатываемых компонентами инфраструктуры и сетевь	13
УПД.14.2	Определение типов прикладного программного обеспечения, к которым разрешен доступ авторизованным (уполнс	13
ЗИС.35.3	Контроль передачи служебных информационных сообщений, передаваемых в сетях, хостовой операционной систег	13
УПД.1.2	Объединение учетных записей в группы (при необходимости)	12
системная,	приложения	12
гостевая	(анонимная), временная и (или) иные типы записей)	12
УПД.1.1	Определение типа учетной записи (внутреннего пользователя, внешнего пользователя	12
УПД.1.7	Оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении све	12
УПД.13.2	Ограничение на использование удаленного доступа в соответствии с задачами (функциями), для решения которых т	12
УПД.1.5	Пересмотр и, при необходимости, корректировка учетных записей пользователей с периодичностью, определяемой	12
УПД.1.6	Регламентация и контроль использования гостевых (анонимных) и временных учетных записей пользователей, а так	12
УПД.5.1	Назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, с	12
УПД.1.4	Заведение, активация, блокирование и уничтожение учетных записей пользователей	12
УПД.13.1	Установление (в том числе документальное) видов доступа, разрешенных для удаленного доступа к объектам досту	12
УПД.13.3	Предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установле	12
УПД.13.5	Контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа	12
УПД.1.8	Уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по вр	12
УПД.1.3	Верификация пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) п	12
УПД.6.1	Регламентация и контроль количества неуспешных попыток входа	11
ЗИС.12.1	Изоляция процессов (выполнение программ) в выделенной области памяти	11
АУД.2.2	Разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и плано	10
АУД.2.4	Информирование должностных лиц оператора (пользователей, администраторов, подразделения по защите инфор	10
АУД.2.3	Устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств	10
анализ	отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации	10
ИНЦ.4.4	Проведение обучения персонала организации, включая сотрудников подразделения по защите информации, для по	10
УПД.10.1	Блокирование сеанса доступа пользователя после установленного Субъектом времени его бездействия (неактивнос	10
ЗИС.2.2	Обеспечение взаимодействия информационной системы и (или) ее сегментов с иными информационными система	10
УПД.14.5	Определение порядка обработки, хранения и передачи информации с использованием внешних информационных	9
УПД.14.3	Определение системных учетных записей, используемых в рамках данного взаимодействия	9
УПД.14.4	Определение порядка предоставления доступа авторизованными (уполномоченным) пользователями из внешних и	9
ИАФ.1.1	Аутентификация пользователей с применением логина и пароля	8
ЗИС.20.1	Обеспечение доверенных маршрутов передачи данных между администратором (пользователем) и средствами заш	8
ИАФ.5.1	Обеспечение однозначной идентификации и аутентификации пользователей для всех видов доступа, кроме тех вид	8
ИАФ.1.3	Аутентификация пользователей с применением одноразовых паролей	8
ЗИС.3.1	Распределение средств защиты информации по разным уровням (эшелонам) защищаемой системы	8
генерация	и выдача начальной аутентификационной информации (начальных значений средств аутентификации)	8
ЗИС.28.1	Определение объектов или типов информации, для которых требуется обеспечение неотказуемости отправки (напр	8
ЗИС.29.1	Определение объектов или типов информации, для которых требуется обеспечение неотказуемости получения (сос	8
ИАФ.4.2	Выдача средств аутентификации пользователям	8
ИНЦ.3.2	Определение текущего и потенциального воздействия инцидента на организацию, идентификация затронутой инфр	8
ИНЦ.5.6	Ограничение доступа сотрудника к конфиденциальной информации	8
УКФ.3.2	Установка (инсталляция) в информационной системе программного обеспечения и (или) его компонентов должна с	8
ОДТ.7.1	Выделение групп однотипных узлов, объединенных каналами передачи информации и рассматриваемых как единь	8
ИНЦ.6.3	Обеспечение доступа к записям о компьютерных инцидентах и функциям управления механизмами выявления (рег	8
ИНЦ.6.1	Регламентация правил и процедур защиты информации о событиях безопасности	8
ИНЦ.6.2	Обеспечение защиты средств выявления (регистрации) инцидентов и настроек механизмов выявления (регистрации	8
ИНЦ.5.11	Проведение аудита защищенности, тестирования на проникновение	8
ИНЦ.5.10	Пересмотр и настройка минимальных прав доступа	8
ИНЦ.5.4	Доведение до сотрудников информации о недопустимости несанкционированной передачи конфиденциальной ин	8
УПД.13.4	Мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к об	8
УПД.12.1	Поддержка (обновление, назначение, изменение) и сохранение атрибутов безопасности (меток безопасности), связ	8
УПД.11.1	Регламентация и контроль действий пользователей, разрешенных до прохождения ими процедур идентификации и	8
УПД.9.1	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя	8
УПД.8.1	Оповещение пользователя после успешного входа о дате и времени предыдущего входа от имени этого пользовате	8
УПД.7.1	Оповещение пользователей в виде сообщения («окна») при его входе (до процесса аутентификации) о том, что реа	8
УПД.0.1	Разработка правил и процедур (политик) управления доступом	8
ИНЦ.5.9	Модернизация или замена компонентов информационных систем	8
ИНЦ.4.3	Актуализация необходимых политик, регламентов, инструкций	8
ИНЦ.5.1	Совершенствование политик информационной безопасности	8
ИНЦ.5.2	Проведение дополнительного обучения сотрудников, ознакомление с правилами обращения с конфиденциальной	8
ИНЦ.4.2	Определение в соответствии с выявленными угрозами безопасности инофрмации мер защиты информации для ми	8
ИНЦ.2.1	Определение механизмов оперативного информирования пользователями службы безопасности о фактах выявлен	8

ИНЦ.1.2	Автоматический анализ событий информационной безопасности и выявление компьютерных инцидентов (компьют	8
ИНЦ.1.3	Ретроспективный анализ данных и выявление не обнаруженных ранее компьютерных инцидентов	8
ИНЦ.3.1	Назначение должностного лица (группы расследования), имеющего навыки проведения подобных расследований	8
ИНЦ.4.1	Переоценка угроз безопасности информации, повлекших возникновение инцидента	8
ИНЦ.5.8	Установка средств защиты информации	8
ИНЦ.5.7	Вынесение предупреждений и другие меры административного характера	8
ИНЦ.5.3	Разработка соответствующих регламентов	8
ИНЦ.5.5	Доведение до сотрудников информации о недопустимости несанкционированной передачи конфиденциальной ин	8
ИНЦ.1.1	Сбор и первичная обработка информации, поступающей от источников событий информационной безопасности	8
ИАФ.1.2	Аутентификация пользователей с применением аппаратных средств (токенов)	8
ОЦЛ.4.2	Вводимые данные должны проверяться на наличие конструкций, которые могут быть интерпретированы программ	6
ОПО.2.1	Проведение проверки целостности программного обеспечения путем сверки контрольных сумм, предоставляемых	6
АУД.5.1	Применение систем анализа сетевого трафика, предназначенных для перехвата потоков данных и обнаружения пр	6
ОЦЛ.1.2	Контроль целостности компонентов программного обеспечения (за исключением средств защиты информации), оп	6
ОПО.1.1	Проведение поиска и получение обновлений программного обеспечения от доверенного источника	6
ЗИС.26.2	Аутентификация сервера, являющегося источником ответов на запросы (кэширующийDNS-сервер) по определению	6
ЗИС.26.1	Аутентификация сервера, являющегося источником ответов на запросы (сервер доменных имен или DNS\002сервер	6
АВЗ.3.1	Проверку в масштабе времени, близком к реальному, объектов (файлов) архивных, исполняемых и зашифрованных	5
АВЗ.1.5	Проверка в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинн	5
АВЗ.2.1	Применение средств антивирусной защиты на прокси-серверах, почтовых шлюза, почтовых серверах и иных точках	5
АВЗ.1.1	Применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, периметральных сре	5
ОПС.2.5	Определение и применение параметров настройки компонентов программного обеспечения, включая программнь	5
ЗИС.17.1	Мониторинг и контроль использования сервисов электронной почты (в том числе с использованием web-интерфейс	5
ЗИС.29.3	Регистрация событий, связанных с получением информации от другого пользователя	4
ЗИС.28.3	Регистрация событий, связанных с отправкой информации другому пользователю	4
УКФ.1.1	Идентификация сетевых подключений информационной системы к внешним информационным системам и сетям	4
УПД.3.2	Контроль доступа пользователей к процессу загрузки операционной системы	4
УКФ.2.2	Оценка возможных последствий от внесения изменений в конфигурацию	4
УКФ.4.1	Контроль действий по внесению изменений в информационной системе	4
УКФ.1.2	Идентификация сетевых подключений внешних информационных систем и сетей к информационной системе	4
ЗИС.31.1	Выявление и анализ скрытых каналов передачи информации для определения параметров передачи информации,	4
ОЦЛ.3.1	Ограничение прав пользователей по вводу информации в информационную систему (ограничение по вводу в опред	4
УКФ.0.1	Разработка правил и процедур (политик) управления конфигурацией информационной (автоматизированной) систе	4
ИАФ.4.5	Обновление аутентификационной информации (замена средств аутентификации) с периодичностью, установленной	4
ЗИС.18.1	Ограничение доступа к сайтам или типам сайтов, запрещенных к использованию	4
ИАФ.4.4	Блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств ауте	4
ЗИС.8.1	Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-фун	4
СОВ.1.1	Обнаружение (предотвращение) вторжений (компьютерных атак), направленных на преднамеренный несанкциони	4
ОЦЛ.1.1	Контроль целостности программного обеспечения средств защиты информации, включая их обновления, по наличи	4
ОЦЛ.1.3	Контроль применения средств разработки и отладки программ в составе программного обеспечения информацион	4
ОЦЛ.1.4	Тестирование с периодичностью, установленной оператором, функций безопасности средств защиты информации,	4
ОЦЛ.1.5	Обеспечение физической защиты технических средств информационной системы	4
ЗИС.23.4	Исключение возможности использования запрещенного мобильного кода в информационной системе, а также вне	4
ЗИС.23.3	Регистрация и анализ событий, связанных с разработкой, приобретением или внедрением технологии мобильного	4
ИНЦ.0.1	Разработка правил и процедур (политик) реагирования на компьютерные инциденты	4
ИАФ.7.1	Организация защиты аутентификационной информации криптографическими методами шифрования трафика. Осуш	4
ИАФ.0.1	Разработка правил и процедур (политик) идентификации и аутентификации субъектов доступа и объектов доступа.	4
ИАФ.1.5	Аутентификация пользователей с применением биометрии	4
ИАФ.6.1	Использование протоколов аутентификации, обеспечивающих взаимную аутентификацию пользователей	4
ИАФ.4.6	Защита аутентификационной информации от неправомерного доступа к ней и модификации	4
ИАФ.3.1	Определение должностного лица (администратора) оператора, ответственного за создание, присвоение и уничтоже	4
ИАФ.3.2	Формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство и присвоен	4
ИАФ.3.3	Предотвращение повторного использования идентификатора пользователя и (или) устройства в течение установлен	4
ИАФ.3.4	Блокирование идентификатора пользователя после установленного оператором времени неиспользования	4
ИАФ.4.1	Определение должностного лица (администратора) оператора, ответственного за хранение, выдачу, инициализаци	4
ИАФ.4.3	Установление характеристик пароля устойчивых к перебору (искользование нескольких алфавитов, специальных си	4
ИАФ.2.1	Определение перечня типов устройств, подлежащих аутентифкации по логическим именам (имя устройства и (или)	4
ИАФ.2.2	Аутентификация устройств с использованием соответствующих протоколов аутентификации или с применением кри	4
ЗНИ.5.1	Определение оператором интерфейсов средств вычислительной техники, которые могут использоваться для ввода	4
ЗИС.15.1	Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых т	4
ЗИС.23.2	Определение разрешенных мест распространения (серверы информационной системы) и использования мобильно	4
ЗИС.23.1	Определение перечня мобильного кода и технологий мобильного кода разрешенных и (или) запрещенных для испо	4
ЗИС.16.1	Обнаружение и реагирование на поступление незапрашиваемых электронных сообщений (писем, документов) и ин	4
ЗИС.17.3	Определение перечня ресурсов сети Интернет, на которых высока вероятность публикации информации конфиденц	3
ЗИС.17.4	Мониторинг содержания указанных выше ресурсов сети Интернет с целью возможной публикации информации кон	3
ОЦЛ.5.1	Определение оператором типов ошибочных действий пользователей, которые потенциально могут привести к нару	2
ОЦЛ.4.1	Контроль точности, полноты и правильности данных, вводимых в информационную систему, обеспечивается путем	2
ОЦЛ.2.1	Контроль целостности с периодичностью, установленной оператором, структуры базы данных по наличию имен (ид	2
ОПС.3.1	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временны	2
ИПО.4.1	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы	2
ИПО.3.1	Проведение практических занятий с персоналом по правилам безопасной работы	2
ИПО.2.1	Обучение персонала правилам безопасной работы	2
ИПО.1.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы	2
АУД.4.1	Определение событий безопасности в информационной системе, подлежащие регистрации, и сроки их хранения	2
ОПС.1.2	Разрешение запуска компонентов программного обеспечения, включенных в перечень (список) программного обес	2
ОЦЛ.5.2	Генерирование сообщений для пользователей об их ошибочных действиях и о возможности нарушения безопасно	2
ЗТС.2.1	Обеспечение контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средс	2
ЗТС.3.1	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам	2
ОПС.1.1	Определение перечня (списка) компонентов программного обеспечения (файлов, объектов баз данных, хранимых	2

ОПС.1.3	Ограничение запуска компонентов программного обеспечения от имени администраторов безопасности	2
ЗИС.17.12	Контроль физического доступа с целью предотвращения визуального и слухового ознакомления с информацией во	1
ЗИС.17.5	Мониторинг, контроль, блокирование копирования информации на переносные носители информации для всех сре	1
ЗИС.17.2	Обеспечить мониторинг и контроль использования сети Интернет для всех средств вычислительной техники, распол	1
ЗИС.17.11	Контроль передачи (выноса) всех средств вычислительной техники независимо от осуществления обработки и (или)	1
ЗИС.17.10	Мониторинг и анализ всех действий возможных внутренних нарушителей, связанных с доступом к информационны	1
ЗИС.17.9	Определение перечня действий возможных внутренних нарушителей, связанных с доступом к информационным ак	1
ЗИС.17.8	Блокирование возможности доступа к информации конфиденциального характера для всех средств вычислительно	1
ЗИС.17.7	Контроль (блокирование) возможности использования и (или) доступа к информации конфиденциального характер	1
ЗИС.17.6	Мониторинг и контроль печати и (или) копирования информации на бумажных носителях для сегментов вычислите	1
АВЗ.1.6	Оповещение администраторов безопасности в масштабе времени, близком к реальному, об обнаружении вредоно	1
АВЗ.1.7	Определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, под	1
ЗИС.34.2	Резервирование информации и технических средств, программного обеспечения, каналов передачи информации	1
АВЗ.1.4	Проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест,	1
ОДТ.2.1	Определение сегментов информационной системы, в которых должно осуществляться резервирование технически	1
ОДТ.2.3	Ввод в действие резервного технического средства, программного обеспечения, канала передачи информации или	1
ОДТ.2.2	Применение резервных (дублирующих) технических средств, программного обеспечения, каналов передачи инфор	1
ЗИС.7.1	Применение специально созданных (эмулированных) ложных компонентов информационной системы или создани	1
ЗИС.13.1	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных д	1
ЗИС.14.2	Загрузка и выполнение на средствах вычислительной техники, определяемых оператором, операционной системы	1
ЗИС.14.3	Загрузка и выполнение на средствах вычислительной техники прикладного программного обеспечения, определяем	1
ОДТ.4.1	Резервное копирование информации на резервные машинные носители информации с установленной оператором	1
ОДТ.4.4	Принятие мер для защиты резервируемой информации, обеспечивающих ее конфиденциальность, целостность и до	1
ОПС.2.1	Определение компонентов программного обеспечения (состава и конфигурации), подлежащих установке после заг	1
ОПС.2.2	Настройка параметров установки компонентов программного обеспечения, обеспечивающая исключение установки	1
ОПС.2.3	Конфигурация устанавливаемых компонентов программного обеспечения (в том числе конфигурации, предусматри	1
ОПС.2.4	Контроль за установкой компонентов программного обеспечения (состав компонентов, параметры установки, конф	1