**СТАЖИРОВКА 2023 | ОБЩИЕ СВЕДЕНИЯ**

В настоящем документе приведены задания для участников конкурсного отбора на оплачиваемую стажировку в Альтирикс Групп на позицию «Специалист по защите информации».

**На что мы обращаем внимание:**

* на полноту и правильность ответов
* на «ход мыслей» кандидата, если ответ получается развернутым и не односложным
* на умение искать информацию в открытых источниках
* на соблюдение орфографических правил и правил пунктуации
* на умение грамотно формулировать мысли и текст
* на единообразие и аккуратность при оформлении документа

**Кому подойдет стажировка:**

* гражданам РФ;
* студентам последних курсов или уже окончившим обучение по специальностям, связанным, с информационной безопасностью или информационными технологиями (21-24 года);
* тем, кто готов уделять стажировке не менее 20 часов в неделю;
* тем, кто обладает кругозором в области информационной безопасности и уверенными знаниями базовых основ сетевых технологий;
* тем, кто готов работать в компании по окончанию стажировки;
* целеустремленным, легкообучаемым, педантичным, пунктуальным, ответственным, коммуникабельным и инициативным.

**Условия стажировки:**

* Период стажировки: 3 месяца
* 12 000 руб. на руки ежемесячно при работе не менее 20 часов в неделю
* Оформляется договор-подряда (ГПХ)
* Дистанционный формат работы (электронная почта, группа в Телеграм)
* График работы преимущественно с 9:00 до 18:00 МСК
* Возможен индивидуальный график и перенос рабочего времени на выходные дни
* Предоставляется доступ на партнерские порталы для сертификации по СЗИ
* Наставничество и получение опыта на реальных проектах по защите информации

**Успешно прошедшим стажировку:**

* Сертификат о прохождении стажировки
* Предложение о заключении бессрочного трудового договора на начальную позицию «Специалист по защите информации» с ежемесячным окладом 40 000 – 50 000 руб. на руки и дополнительными премиями за успехи и реализованные проекты (для более опытных кандидатов может быть установлен оклад в размере 60 000 – 70 000 руб. на руки).

**После заключения трудового договора:**

* Составление Плана индивидуального развития экспертами по защите информации
* Сертификация и обучение за счет компании

Два тестовых задания представлено ниже. Заполненную версию файла направлять по адресу [info@altirixgroup.com](mailto:info@altirixgroup.com), прикладывая актуальную версию резюме. Успешные кандидаты будут приглашены на онлайн-интервью. Вы можете пересылать этот файл своим друзьям/знакомым, кому может быть интересна стажировка.

Заявки принимаются до 01.09.2023

**ЗАДАНИЕ № 1 | РУБРИКА «ВОПРОС-ОТВЕТ»**

|  |
| --- |
| 1. Какими нормативными правовыми актами регулируется вопрос защиты персональных данных?[[1]](#footnote-1) |
| > |
| 1. Какими нормативными правовыми актами регулируется вопрос защиты объектов критической информационной инфраструктуры? |
| > |
| 1. Какими нормативными правовыми актами регулируется вопрос защиты государственных информационных систем? |
| > |
| 1. Какими нормативными правовыми актами регулируется порядок аттестации информационных систем? |
| > |
| 1. Какие существуют категории персональных данных? Привести примеры для каждой категории. |
| > |
| 1. В соответствии с каким методическим документом должна разрабатываться модель угроз? |
| > |
| 1. Относится ли фотография человека к биометрическим персональным данным? |
| > |
| 1. Относятся ли cookie-файлы к персональным данным? |
| > |
| 1. Опишите основные стадии создания автоматизированной системы |
| > |
| 1. Какой документ устанавливает требования к содержанию документов по созданию автоматизированных систем? |
| > |
| 1. Чем отличается автоматизированная система от информационной системы? |
| > |
| 1. Какие классы защиты сертифицированных средств защиты информации могут применяться для обеспечения безопасности значимого объекта критической информационной инфраструктуры 2 категории? |
| > |
| 1. Чем отличается межсетевой экран от системы обнаружения вторжений? |
| > |
| 1. Какие выделяют виды электронных подписей? |
| > |
| 1. Чем отличается симметричное шифрование от ассиметричного? |
| > |
| 1. Какие уровни АСУ ТП выделяются в документации ФСТЭК России? |
| > |
| 1. Какими нормативными правовыми актами регулируется вопрос защиты АСУ ТП? |
| > |
| 1. Является ли станок с ЧПУ – АСУ ТП? |
| > |
| 1. Чем анализ защищенности отличается от пентеста? |
| > |
| 1. Какие регуляторы по защите информации определены в РФ? |
| > |
| 1. С каким аппаратом ФСТЭК России (региональным или центральным) надо согласовывать сведения о категорировании объектов КИИ в сфере ОПК? |
| > |
| 1. Необходимо ли в процессе моделирования УБИ рассматривать в качестве возможных угрозы, связанные с нарушением безопасности облачной инфраструктуры, если оператор размещает серверный сегмент системы во внешнем ЦОД? |
| > |
| 1. Какие существуют виды испытаний автоматизированных систем? |
| > |
| 1. Чем отличается оценка соответствия средств защиты информации от аттестации информационной системы? |
| > |
| 1. Обязательно ли использовать сертифицированные средства защиты информации для защиты персональных данных? |
| > |
| 1. Какие классы средств защиты информации вы знаете? |
| > |
| 1. Чем маршрутизатор отличается от роутера? |
| > |
| 1. Что такое Control plane, Data plane и Management plane применительно к сетевому оборудованию? |
| > |
| 1. Какой протокол динамической маршрутизации самый лучший? |
| > |
| 1. Чем L3 коммутатор отличается от маршрутизатора? |
| > |
| 1. Опишите пошагово ваши действия по проверке подключения к Интернету, если у вас дома пропал Интернет. |
| > |
| 1. Для сети с адресом 11001000.00000000.00000000.00000001 и маской 11111111.11111111.11111111.11000000 укажите: а) адрес сети б) адрес первого хоста в) адрес последнего хоста |
| > |
| 1. Укажите какие открытие источники вы читаете/смотрите на тему информационной безопасности (СМИ, журналы, группы в телеграм и др. мессенджерах, ВК, YouTube и т.п.)? |
| > |

**ЗАДАНИЕ № 2 | РЕАЛИЗАЦИЯ МЕР ЗАЩИТЫ ИНФОРМАЦИИ**

В этом задании необходимо описать, как по-вашему реализуются технические меры защиты (встроенные механизмы) в операционных системах Windows, Windows Server и Linux. Перечень мер приведен ниже в соответствии с требованиями ФСТЭК России. В случае отсутствия технической реализации меры, необходимо указывать компенсирующие (организационные) меры, которые помогут нейтрализовать угрозы безопасности информации.

*Пример: для реализации меры АВЗ.1 в операционной системе Windows предусмотрено средство антивирусной защиты, управление которым осуществляется через оснастку «Безопасность Windows».*

| **Код** | **Содержание мер** | **Реализация** |
| --- | --- | --- |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ИАФ.2 | Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УПД.7 | Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УПД.8 | Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УПД.9 | Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УПД.12 | Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УПД.17 | Обеспечение доверенной загрузки средств вычислительной техники | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ОПС.1 | Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ОПС.2 | Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ОПС.4 | Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗНИ.1 | Учет машинных носителей персональных данных | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗНИ.2 | Управление доступом к машинным носителям персональных данных | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗНИ.3 | Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗНИ.4 | Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗНИ.5 | Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗНИ.6 | Контроль ввода (вывода) информации на машинные носители персональных данных | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗНИ.7 | Контроль подключения машинных носителей персональных данных | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗНИ.8 | Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| РСБ.7 | Защита информации о событиях безопасности | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| АВЗ.1 | Реализация антивирусной защиты | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| СОВ.1 | Обнаружение вторжений | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| СОВ.2 | Обновление базы решающих правил | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ОЦЛ.1 | Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ОЦЛ.2 | Контроль целостности персональных данных, содержащихся в базах данных информационной системы | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ОЦЛ.4 | Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама) | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ОЦЛ.5 | Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ОЦЛ.6 | Ограничение прав пользователей по вводу информации в информационную систему | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ОЦЛ.7 | Контроль точности, полноты и правильности данных, вводимых в информационную систему | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ОЦЛ.8 | Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ОДТ.1 | Использование отказоустойчивых технических средств | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ОДТ.2 | Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ОДТ.3 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ОДТ.4 | Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ОДТ.5 | Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗСВ.4 | Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗСВ.5 | Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗСВ.6 | Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗСВ.7 | Контроль целостности виртуальной инфраструктуры и ее конфигураций | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗСВ.8 | Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗТС.1 | Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗТС.5 | Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.1 | Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.2 | Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.3 | Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.4 | Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации) | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.6 | Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.7 | Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.8 | Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.9 | Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.10 | Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.11 | Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.12 | Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.13 | Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.14 | Использование устройств терминального доступа для обработки персональных данных | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.15 | Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.16 | Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.17 | Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.18 | Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.19 | Изоляция процессов (выполнение программ) в выделенной области памяти | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ИНЦ.1 | Определение лиц, ответственных за выявление инцидентов и реагирование на них | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ИНЦ.2 | Обнаружение, идентификация и регистрация инцидентов | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ИНЦ.3 | Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ИНЦ.4 | Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ИНЦ.5 | Принятие мер по устранению последствий инцидентов | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| ИНЦ.6 | Планирование и принятие мер по предотвращению повторного возникновения инцидентов | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УКФ.1 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УКФ.2 | Управление изменениями конфигурации информационной системы и системы защиты персональных данных | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УКФ.3 | Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |
| УКФ.4 | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных | Для Windows:  Для Windows Server:  Для Linux:  Компенсирующие или организационные меры: |

1. Здесь и далее все вопросы относятся к сфере Российского законодательства [↑](#footnote-ref-1)