МБОУ «Комсомольская средняя общеобразовательная школа»

Приказ

04 июля 2017 года № 97/3.

Об утверждении состава и
содержания мер защиты информации.

В соответствии с требованиями Постановления Правительства РФ от 01.11.2012 № 1119, Приказом ФСТЭК России от 18.02.2013 № 21, Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

ПРИКАЗЫВАЮ:

1. Утвердить состав и содержание мер защиты информации, реализуемых с учётом актуальных угроз безопасности сведений конфиденциального характера и применяемых информационных технологий (Приложение 1).

2. Администратору (подразделению) защиты информации информационных систем привести в соответствие организационно-распорядительные документы по защите конфиденциальной информации.

3. Контроль исполнения настоящего приказа оставляю за собой.

Директор школы: О.В.Зоткина

Приложение 1
к Приказу МБОУ «Комсомольская СОШ»
от «04» июля 2017г. № 97/2

СОСТАВ И СОДЕРЖАНИЕ
мер по защите информации в МБОУ «Комсомольская СОШ»

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ

АВС – антивирусные средства

Администратор защиты (безопасности) информации – лицо, ответственное за защиту АС от несанкционированного доступа к информации;

АП – абонентский пункт - автоматизированная система, подключаемая к Сети с помощью коммуникационного оборудования и предназначенная для работы абонента Сети;

АРМ – автоматизированное рабочее место - программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида;

АС – автоматизированная система

АСЗИ – автоматизированная система в защищенном исполнении

ВТСС – вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях;

Информационные сети общего пользования – вычислительные (информационно-телекоммуникационные) сети, открытые для пользования всем физическим и юридическим лицам, в услугах которых этим лицам не может быть отказано;

ИС – информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

ИСПДн – информационная система персональных данных

КИ – конфиденциальная информация - информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

КОИ – криптографически опасная информация

Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну;

ЛВС – локальная вычислительная сеть - совокупность основных технических средств и систем, осуществляющих обмен информацией между собой и с другими информационными системами, в том числе с ЛВС, через

определенные точки входа/выхода информации, которые являются границей ЛВС;

МЭ – межсетевой экран - это локальное (однокомпонентное) или функционально распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную (информационную) систему и (или) выходящей из неё;

НЖМД – запоминающее устройство (устройство хранения информации) произвольного доступа, основанное на принципе магнитной записи;

НСД – несанкционированный доступ - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых СВТ или автоматизированной (информационной) системы;

Обработка информации - совокупность операций сбора, накопления, ввода-вывода, приема-передачи, записи, хранения, регистрации, уничтожения, преобразования и отображения, осуществляемых над информацией;

Организационно-распорядительная документация (ОРД) – комплекс документов, закрепляющих функции, задачи, цели, а также права и обязанности работников и руководителей по выполнению конкретных действий, необходимость которых возникает в операционной деятельности организации.

Оптический диск – собирательное название для носителей информации, выполненных в виде дисков, чтение с которых ведётся с помощью оптического излучения;

ОС – операционная система

ОТСС – основные технические средства и системы - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации;

ПДн – персональные данные

ПМВ – программно-математическое воздействие

ПО – программное обеспечение - совокупность программ на носителях данных и программных документов, предназначенных для отладки, функционирования и проверки работоспособности автоматизированной (информационной) системы;

ПЭМИН – побочные электромагнитные излучения и наводки

САЗ – система анализа защищенности

СВТ – средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

СЗИ – средства защиты информации

СЗИ от НСД – система защиты информации от НСД - комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации (несанкционированных действий с ней) в автоматизированной (информационной) системе;

СЗПДн – система (подсистема) защиты персональных данных

СКЗИ – средства криптографической защиты информации

СОВ – система обнаружения вторжений

ТС – техническое средство

УБПДн – угрозы безопасности персональных данных

Флеш-накопитель – запоминающее устройство, использующее в качестве носителя электрически стираемую перепрограммируемую энергонезависимую память и подключаемое к компьютеру

ФСБ России – Федеральная служба безопасности Российской Федерации.

ФСТЭК России – Федеральная служба по техническому и экспортному контролю Российской Федерации;

1. УРОВЕНЬ ЗАЩИЩЁННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.1. Тип ИСПДн: иная категория персональных данных (персональные данные не относящиеся к специальным, биометрическим, сотрудникам оператора).

1.2. Тип актуальных угроз: угрозы 3-го типа.

1.2.1. Уровень исходной защищенности ИСПДн

1.2.1.1. Показатели исходной защищённости:

№ п.п.	Технические и эксплуатационные характеристики	Уровень защищённости
1.	По территориальному размещению: локальная ИСПДн, развернутая в пределах одного здания	Высокий
2.	По наличию соединения с сетями общего пользования: ИСПДн, имеющая одноточечный выход в сеть общего пользования	Средний
3.	По встроенным (легальным) операциям с записями баз персональных данных: модификация, передача	Низкий
4.	По разграничению доступа к персональным данным: ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн	Средний
5.	По наличию соединений с другими базами ПДн иных ИСПДн: интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн)	Низкий
6.	По уровню обобщения (обезличивания) ПДн: ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	Низкий
7.	По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: ИСПДн, предоставляющая часть ПДн	Средний

1.2.1.2. Исходная степень защищённости: ИС имеет низкую исходную защищённость: высокий – 14,28% средний – 42,86%, низкий – 42,86%.

1.2.1.3. Коэффициент $Y_1 = 10$.

1.2.2. Угрозы 1-го типа

1.2..2.1. Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе:

системное программное обеспечение: Windows (сертификат по контролю на недокументированные (недекларированные) возможности отсутствует).

1.2.2.2. Частота (вероятность) реализации угрозы: низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (использованы соответствующие средства защиты информации).

1.2.2.3. Коэффициент $Y_2 = 2$.

1.2.2.4. Коэффициент реализуемой угрозы: Y=0,6: возможность реализации угрозы признаётся средним.

1.2.2.5. Оценка опасности: реализация угрозы может привести к незначительным негативным последствиям для субъекта персональных данных: низкая опасность.

1.2.2.6. Вывод: актуальность угрозы: неактуальная (средняя вероятность реализации угрозы, низкая опасность).

1.2.3. Угрозы 2-го типа

1.2.3.1. Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе: программное обеспечение для обеспечение работы сотрудников (сертификат по контролю на недокументированные (недекларированные) возможности отсутствует).

1.2.3.2. Частота (вероятность) реализации угрозы: низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (использованы соответствующие средства защиты информации).

1.2.3.3. Коэффициент $Y_2 = 2$.

1.2.3.4. Коэффициент реализуемой угрозы: Y=0,6: возможность реализации угрозы признаётся средним.

1.2.3.5. Оценка опасности: реализация угрозы может привести к незначительным негативным последствиям для субъекта персональных данных: низкая опасность.

1.2.3.6. Вывод: актуальность угрозы: неактуальная (средняя вероятность реализации угрозы, низкая опасность).

1.3. Объём обрабатываемых персональных данных: более 100000 субъектов персональных данных.

1.4. Уровень защищённости персональных данных: **третий (УЗ3).**

2. КЛАССА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

2.1. Нарушение безопасности конфиденциальности (неправомерные доступ, копирование, предоставление или распространение): **степень возможного ущерба низкая**: возможны незначительные негативные последствия в деятельности, оператор может выполнять возложенные на него функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

2.2. Нарушение безопасности целостности (неправомерные уничтожения или модификация): **степень возможного ущерба низкая**: возможны незначительные негативные последствия в деятельности, оператор может выполнять возложенные на него функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

2.3. Нарушение безопасности доступности (неправомерное блокирование): **степень возможного ущерба низкая**: возможны незначительные негативные последствия в деятельности, оператор может выполнять возложенные на него функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

2.4. Уровень значимости: **низкий.**

2.5. Масштаб информационной системы: **региональный** (система функционирует на территории субъекта Российской Федерации).

2.6. Класс защищённости информационной системы: **К3.**

3. БАЗОВЫЙ НАБОР МЕР ЗАЩИТЕ ИНФОРМАЦИИ

3.1. Идентификация и аутентификация субъектов доступа и объектов доступа

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности)

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
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

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)

3.2. Управление доступом субъектов доступа к объектам доступа

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)

3.3. Ограничение программной среды

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов

3.4. Защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных)

Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
ЗНИ.1	Учет машинных носителей информации
ЗНИ.2	Управление доступом к машинным носителям информации
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

3.5. Регистрация событий безопасности

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
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
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе
РСБ.7	Защита информации о событиях безопасности

3.6. Антивирусная защита

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

3.7. Обнаружение (предотвращение) вторжений

Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
Требования отсутствуют	

3.8. Контроль (анализ) защищенности персональных данных

Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе

3.9. Обеспечение целостности информационной системы и персональных данных

Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций

3.10. Обеспечение доступности персональных данных

Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
Требования отсутствуют	

3.11. Защита среды виртуализации

Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе

хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Условное обозначение и номер меры	**Содержание мер по обеспечению безопасности персональных данных**
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей

3.12. Защита технических средств

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

Условное обозначение и номер меры	**Содержание мер по обеспечению безопасности персональных данных**
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
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
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

3.13. Защита информационной системы, ее средств, систем связи и передачи данных

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
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
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе
ЗИС.30	Защита мобильных технических средств, применяемых в информационной системе

3.14. Выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них

Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
Требования отсутствуют	

3.15. Управление конфигурацией информационной системы и системы защиты персональных данных

Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных
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
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных

4. АДАПТИРОВАННЫЙ БАЗОВЫЙ НАБОР МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Мера защиты информации ИАФ.6

В информационной системе не осуществляется (запрещена) идентификация и аутентификация пользователей, не являющихся работниками оператора.

Решение: **мера защиты информации исключена.**

4.2. Мера защиты информации УПД.13

В информационной системе запрещена реализация любого удалённого доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети с использованием любых стационарных и (или) мобильных технических средств.

Решение: **мера защиты информации исключена.**

4.3. Мера защиты информации УПД.14

В информационной системе запрещено использование технологий беспроводного доступа пользователей к объектам доступа: стандарты коротковолновой радиосвязи, спутниковой и пакетной радиосвязи.

Решение: **мера защиты информации исключена.**

4.4. Мера защиты информации УПД.15

В информационной системе запрещено использование мобильных технических средств:

– съемные машинные носители информации, не входящих в ее состав (находящихся в личном использовании): 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).

Решение: **мера защиты информации исключена.**

4.5. Мера защиты информации ЗСВ.1

В информационной системе не используется (запрещена) виртуальная инфраструктура: среда виртуализации (программное обеспечение, служебные данные компонентов виртуальной инфраструктуры) и аппаратное обеспечение (аппаратные средства, необходимые для функционирования среды виртуализации, в том числе средства резервного копирования и защиты информации).

Решение: **мера защиты информации исключена.**

4.6. Мера защиты информации ЗСВ.2

В информационной системе не используется (запрещена) виртуальная инфраструктура: среда виртуализации (программное обеспечение, служебные данные компонентов виртуальной инфраструктуры) и аппаратное обеспечение (аппаратные средства, необходимые для функционирования среды виртуализации, в том числе средства резервного копирования и защиты информации).

Решение: **мера защиты информации исключена.**

4.7. Мера защиты информации ЗСВ.3

В информационной системе не используется (запрещена) виртуальная инфраструктура: среда виртуализации (программное обеспечение, служебные данные компонентов виртуальной инфраструктуры) и аппаратное обеспечение (аппаратные средства, необходимые для функционирования среды виртуализации, в том числе средства резервного копирования и защиты информации).

Решение: **мера защиты информации исключена.**

4.8. Мера защиты информации ЗСВ.9

В информационной системе не используется (запрещена) виртуальная инфраструктура: среда виртуализации (программное обеспечение, служебные данные компонентов виртуальной инфраструктуры) и аппаратное обеспечение (аппаратные средства, необходимые для функционирования среды виртуализации, в том числе средства резервного копирования и защиты информации).

Решение: **мера защиты информации исключена.**

4.9. Мера защиты информации ЗСВ.10

В информационной системе не используется (запрещена) виртуальная инфраструктура: среда виртуализации (программное обеспечение, служебные данные компонентов виртуальной инфраструктуры) и аппаратное обеспечение (аппаратные средства, необходимые для функционирования среды виртуализации, в том числе средства резервного копирования и защиты информации).

Решение: **мера защиты информации исключена.**

4.10. Мера защиты информации ЗИС.5

В информационной системе не используются (запрещено) использование видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно.

Решение: **мера защиты информации исключена.**

4.11. Мера защиты информации ЗИС.20

В информационной системе не используются (запрещены) беспроводные соединения: 802.11xWi-Fi, 802.15.1 Bluetooth, 802.22WRAN, IrDA и т.п.

Решение: **мера защиты информации исключена.**

4.12. Мера защиты информации ЗИС.30

В информационной системе не используются (запрещены) 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).

Решение: **мера защиты информации исключена.**

5. УТОЧНЁННЫЙ АДАПТИРОВАННЫЙ БАЗОВЫЙ НАБОР МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Условное обозначение и номер меры	Меры по обеспечению безопасности персональных данных, направленные на нейтрализацию актуальных угроз безопасности персональных данных	Вид итоговой отчётности
ИАФ.1	Нейтрализуется при использовании СЗИ от НСД	Протокол испытаний
ИАФ.3	Нейтрализуется при использовании СЗИ от НСД и применении организационных мероприятий	Протокол испытаний, ОРД
ИАФ.4	Нейтрализуется при использовании СЗИ от НСД и применении организационных и охранно-режимных мероприятий	Протокол испытаний, ОРД
ИАФ.5	Нейтрализуется при использовании СЗИ от НСД и применении организационных мероприятий	Протокол испытаний, ОРД
УПД.1	Нейтрализуется при использовании СЗИ от НСД и применении организационных мероприятий	Протокол испытаний, ОРД
УПД.2	Нейтрализуется при использовании СЗИ от НСД	Протокол испытаний
УПД.3	Нейтрализуется при использовании СЗИ от НСД	Протокол испытаний
УПД.4	Нейтрализуется при использовании СЗИ от НСД и применении организационных мероприятий	Протокол испытаний, ОРД
УПД.5	Нейтрализуется при использовании СЗИ от НСД	Протокол испытаний
УПД.6	Нейтрализуется при использовании СЗИ от НСД	Протокол испытаний
УПД.10	Нейтрализуется при использовании СЗИ от НСД	Протокол испытаний
УПД.11	Нейтрализуется при использовании СЗИ от НСД	Протокол испытаний
УПД.16	Нейтрализуется при использовании СЗИ от НСД, МЭ и применении организационных и охранно-режимных мероприятий	Протокол испытаний, ОРД
ОПС.3	Нейтрализуется при применении организационных мероприятий	ОРД
ЗНИ.1	Нейтрализуется при использовании СЗИ от НСД и применении организационных мероприятий	Протокол испытаний, ОРД

Условное обозначение и номер меры	Меры по обеспечению безопасности персональных данных, направленные на нейтрализацию актуальных угроз безопасности персональных данных	Вид итоговой отчётности
ЗНИ.2	Нейтрализуется при использовании СЗИ от НСД и применении организационных мероприятий	Протокол испытаний, ОРД
ЗНИ.8	Нейтрализуется при использовании СЗИ от НСД и применении организационных и охранно-режимных мероприятий	Протокол испытаний, ОРД
РСБ.1	Нейтрализуется при использовании СЗИ от НСД, антивируса, МЭ и применении организационных мероприятий	Протокол испытаний, ОРД
РСБ.2	Нейтрализуется при использовании СЗИ от НСД, антивируса, МЭ	Протокол испытаний
РСБ.3	Нейтрализуется при использовании СЗИ от НСД, антивируса, МЭ	Протокол испытаний
РСБ.4	Нейтрализуется при использовании СЗИ от НСД, антивируса, МЭ	Протокол испытаний
РСБ.5	Нейтрализуется при использовании СЗИ от НСД, антивируса, МЭ и применении организационных мероприятий	Протокол испытаний, ОРД
РСБ.6	Нейтрализуется при применении организационных мероприятий	ОРД
РСБ.7	Нейтрализуется при использовании СЗИ от НСД, антивируса, МЭ и применении организационных мероприятий	Протокол испытаний, ОРД
АВЗ.1	Нейтрализуется при использовании антивируса	Протокол испытаний
АВЗ.2	Нейтрализуется при использовании антивируса и применении организационных мероприятий	Протокол испытаний, ОРД
АНЗ.1	Нейтрализуется при использовании СЗИ и применении организационных мероприятий	Протокол испытаний
АНЗ.2	Нейтрализуется при использовании СЗИ и применении организационных мероприятий	Протокол испытаний, ОРД
АНЗ.3	Нейтрализуется при использовании внутренней системы контроля СЗИ и применении организационных мероприятий	Протокол испытаний, ОРД
АНЗ.4	Нейтрализуется при применении организационных мероприятий	ОРД

Условное обозначение и номер меры	Меры по обеспечению безопасности персональных данных, направленные на нейтрализацию актуальных угроз безопасности персональных данных	Вид итоговой отчётности
АНЗ.5	Нейтрализуется при применении организационных мероприятий	ОРД
ОЦЛ.3	Нейтрализуется при применении организационных мероприятий	ОРД
ЗТС.2	Нейтрализуется применением организационных и охранно-режимных мероприятий	ОРД
ЗТС.3	Нейтрализуется при применении организационных и охранно-режимных мероприятий	ОРД
ЗТС.4	Нейтрализуется при применении организационных и охранно-режимных мероприятий	ОРД
ЗИС.3	Нейтрализуется при использовании МЭ, СКЗИ и применении организационных мероприятий	Протокол испытаний, ОРД
УКФ.1	Нейтрализуется при применении организационных и охранно-режимных мероприятий	ОРД
УКФ.2	Нейтрализуется при применении организационных и охранно-режимных мероприятий	ОРД
УКФ.3	Нейтрализуется при применении организационных и охранно-режимных мероприятий	ОРД
УКФ.4	Нейтрализуется при применении организационных и охранно-режимных мероприятий	ОРД

6. ДОПОЛНЕНИЕ УТОЧНЕННОГО АДАПТИРОВАННОГО БАЗОВОГО НАБОРА МЕР ЗАЩИТЫ ИНФОРМАЦИИ

6.1. Федеральным законом Российской Федерации, указами Президента Российской Федерации, постановлениямм Правительства Российской Федерации, нормативными актами органа государственной власти, органа местного самоуправления или организации, определяющими порядок создания и эксплуатации информационных систем, **не установлены** дополнительные требования к защите информации, выполнение которых не предусмотрено Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. N 17.

6.2. Меры защиты информации, включенные в уточненный адаптированный базовый набор мер защиты информации, достаточны для защиты информационных систем.

7. ПРИМЕНЕНИЕ КОМПЕНСИРУЮЩИХ МЕР ЗАЩИТЫ ИНФОРМАЦИИ

7.1. Сформированный набор мер защиты информации не требует дополнительного применения компенсирующих мер защиты информации.