МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КРАСНОДАРСКОГО КРАЯ

УТВЕРЖДАЮ

Первый заместитель министра
образования и науки
Краснодарского края

_____/С.В. Пронько

Рекомендации по подключению к региональной государственной информационной системе «Автоматизированная система управления сферой образования Краснодарского края»

2025

1. ТЕРМИНЫ И СОКРАЩЕНИЯ

ГИС Краснодарского края	-	Информационная система, созданная, приобретенная и (или) накапливаемая с привлечением средств бюджета Краснодарского края, а также иным установленным законом способом
ГОСТ	-	Государственный стандарт
ИОГВ Краснодарского края	-	Исполнительные органы государственной власти Краснодарского края
ИС	-	Информационная система
Оператор информационной системы	-	Внутренний пользователь РМС ОГВ, осуществляющий деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных[1]
Разработчик ИС	-	Юридическое лицо, осуществляющее на договорной основе (или иным установленным законом способом) функции по разработке и (или) сопровождению ГИС Краснодарского края
РМС ОГВ	-	Региональная мультисервисная сеть органов государственной власти Краснодарского края
Участники информационного взаимодействия	-	Муниципальные органы управления образованием и образовательные организации
ФСБ России	-	Федеральная служба безопасности Российской Федерации
ФСТЭК России	-	Федеральная служба по техническому и экспортному контролю Российской Федерации
ЦОД РМС ОГВ	-	Центр обработки данных региональной мультисервисной сети органов государственной власти Краснодарского края

2. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящие рекомендации по подключению к региональной государственной информационной системе «Автоматизированная система управления сферой образования Краснодарского края» (далее – Рекомендации) определяют общий порядок подключения участников информационного взаимодействия к региональной государственной информационной системы «Автоматизированная система управления сферой образования Краснодарского края» министерства образования и науки Краснодарского края (далее – АСУ СО, Система). Серверный сегмент АСУ СО, реализующий функционал Системы, аттестован на соответствие

---

[1] В случаях, если иное не установлено федеральным законодательством, оператором информационной системы является собственник используемых для обработки, содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы

требованиям безопасности информации.

Оператором АСУ СО является министерство образования и науки Краснодарского края (далее – Министерство).

Настоящие Рекомендации предназначены для муниципальных органов управления образованием, образовательных организаций и контролирующих органов – участников информационного взаимодействия, осуществляющих подключение (взаимодействие) к серверному сегменту АСУ СО в целях исполнения должностных обязанностей.

Рекомендации не предназначены:

— для организаций, являющихся разработчиками ИС, либо осуществляющих техническую поддержку, сопровождение, модернизацию Системы.

— для обучающихся и родителей (законных представителей) обучающихся.

Рекомендации разработаны на основании следующих нормативных правовых и методических документов:

1. Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

2. Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

3. Постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

4. Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

5. Приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Список изменяющих документов»;

6. Приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

7. Методического документа ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах»;

8. Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утверждённое Приказом ФСБ России от 9 февраля 2005 г. № 66;

9. Модели угроз безопасности информации серверного сегмента региональной государственной информационной системы «Автоматизированная система управления сферой образования Краснодарского края» от 2 мая 2024 г.;

10. Модели угроз безопасности информации для сегмента конечных пользователей региональной государственной информационной системы

«Автоматизированная система управления сферой образования Краснодарского края» от 2 мая 2024 г.

Согласно Акту классификации АСУ СО от 15 октября 2021 г. установлен для серверного сегмента второй уровень защищенности (УЗ2) и второй класс защищенности (К2), для пользовательского сегмента АСУ СО установлен третий уровень защищенности (УЗ3) и третий класс защищенности (К3) персональных данных, при их обработке в АСУ СО.

Аттестатом соответствия № 1645.00004.2025 от 21 марта 2025 г. подтверждается выполнение требований безопасности информации, предъявляемых к второму классу защищенности государственных информационных систем (К2), а также второму уровню защищенности персональных данных при их обработке в информационной системе (УЗ 2).

Подключение к серверному сегменту АСУ СО осуществляется через региональную мультисервисную сеть органов государственной власти Краснодарского края (далее – РМС ОГВ) с применением средств криптографической защиты информации ViPNet. Доступ возможен через ViPNet-сети №№ 2467, 2312, 2464, 15428, 11244, 12523, 5160, 1519, 1770.

В соответствии с постановлением Главы администрации (Губернатора) Краснодарского края от 26 августа 2008 г. № 840 «О региональной мультисервисной сети органов государственной власти Краснодарского края» подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники к РМС ОГВ производится:

— с использованием средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю;

— подключаемые к РМС ОГВ информационные системы должны соответствовать (иметь аттестат соответствия) требованиям по защите информации, установленным Федеральной службой по техническому и экспортному контролю для соответствующего класса защищенности государственных информационных систем и уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных.

Для возможности подключения к аттестованному на соответствие требованиям безопасности информации серверному сегменту АСУ СО участник информационного взаимодействия должен подтвердить, что автоматизированные рабочие места (далее – АРМ), пользователей , с которых планируется осуществлять подключение к АСУ СО (пользовательский сегмент АСУ СО) прошли аттестационные испытания на соответствие требованиям, предъявляемым к третьему классу государственных информационных систем (К3), а также третьему уровню защищенности персональных данных при их обработке в информационной системе (УЗ 3).

3. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

3.1. Требования к системе защиты информации

В соответствии с Техническим заданием на создание подсистемы защиты

информации региональной государственной информационной системы «Автоматизированная система управления сферой образования Краснодарского края» и Техническим проектом подсистемы защиты информации региональной государственной информационной системы «Автоматизированная система управления сферой образования Краснодарского края» система защиты информации пользовательского сегмента должна обеспечивать реализацию следующих мер защиты информации:

– 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;

– ИАФ.5 – защита обратной связи при вводе аутентификационной информации;

– 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;

– 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.15 – регламентация и контроль использования в информационной системе мобильных технических средств;

– ОПС.3 – установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;

– ЗНИ.1 – учет машинных носителей информации;

– ЗНИ.2 – управление доступом к машинным носителям информации;

– ЗНИ.3 – контроль перемещения машинных носителей информации за пределы контролируемой зоны;

– ЗНИ.6 – контроль ввода (вывода) информации на машинные носители информации;

– ЗНИ.7 – контроль подключения машинных носителей информации;

– ЗНИ.8 – уничтожение (стирание) или обезличивание информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания;

– 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;

– АВЗ.1 – реализация антивирусной защиты;

– АВЗ.2 – обновление базы данных признаков вредоносных компьютерных программ (вирусов);

– СОВ.1 – обнаружение вторжений;

– СОВ.2 – обновление базы решающих правил;

– 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;

– АНЗ.5 – контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализация правил разграничения доступа, полномочий пользователей в информационной системе;

– ОЦЛ.3 – обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций;

– ЗТС.2 – организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования;

– ЗИС.3 – обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи;

– ЗТС.3 – Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены;

– ЗТС.4 – размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;

– ЗИС.3 – обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи;

– ЗИС.30 – защита мобильных технических средств, применяемых в информационной системе;

– 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.

3.2. Требования к организационному обеспечению системы защиты информации

Система защиты информации пользовательского сегмента при подключении к АСУ СО должна обеспечивать нейтрализацию следующих угроз безопасности информации, определенных в Модели угроз безопасности информации серверного сегмента информационной системы «Автоматизированная система управления сферой образования Краснодарского края» министерства образования и науки Краснодарского края:

– УБИ.003 Угроза анализа криптографических алгоритмов и их реализации;

– УБИ.004 Угроза аппаратного сброса пароля BIOS;

– УБИ.006 Угроза внедрения кода или данных;
– УБИ.007 Угроза воздействия на программы с высокими привилегиями;
– УБИ.008 Угроза восстановления аутентификационной информации;
– УБИ.009 Угроза восстановления предыдущей уязвимой версии BIOS;
– УБИ.012 Угроза деструктивного изменения конфигурации/среды окружения программ;
– УБИ.013 Угроза деструктивного использования декларированного функционала BIOS;
– УБИ.014 Угроза длительного удержания вычислительных ресурсов пользователями;
– УБИ.015 Угроза доступа к защищаемым файлам с использованием обходного пути;
– УБИ.017 Угроза доступа/перехвата/изменения HTTP cookies;
– УБИ.018 Угроза загрузки нештатной операционной системы;
– УБИ.019 Угроза заражения DNS-кеша;
– УБИ.022 Угроза избыточного выделения оперативной памяти;
– УБИ.023 Угроза изменения компонентов системы;
– УБИ.025 Угроза изменения системных и глобальных переменных;
– УБИ.026 Угроза искажения XML-схемы;
– УБИ.027 Угроза искажения вводимой и выводимой на периферийные устройства информации;
– УБИ.028 Угроза использования альтернативных путей доступа к ресурсам;
– УБИ.030 Угроза использования информации идентификации/ аутентификации, заданной по умолчанию;
– УБИ.031 Угроза использования механизмов авторизации для повышения привилегий;
– УБИ.032 Угроза использования поддельных цифровых подписей BIOS;
– УБИ.033 Угроза использования слабостей кодирования входных данных;
– УБИ.034 Угроза использования слабостей протоколов сетевого/локального обмена данными;
– УБИ.036 Угроза исследования механизмов работы программы;
– УБИ.037 Угроза исследования приложения через отчёты об ошибках;
– УБИ.039 Угроза исчерпания запаса ключей, необходимых для обновления BIOS;
– УБИ.045 Угроза нарушения изоляции среды исполнения BIOS;
– УБИ.049 Угроза нарушения целостности данных кеша;
– УБИ.053 Угроза невозможности управления правами пользователей BIOS;
– УБИ.062 Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера;
– УБИ.063 Угроза некорректного использования функционала программного обеспечения;
– УБИ.067 Угроза неправомерного ознакомления с защищаемой информацией;

– УБИ.068 Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;

– УБИ.069 Угроза неправомерных действий в каналах связи;

– УБИ.071 Угроза несанкционированного восстановления удалённой защищаемой информации;

– УБИ.072 Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS;

– УБИ.074 Угроза несанкционированного доступа к аутентификационной информации;

– УБИ.086 Угроза несанкционированного изменения аутентификационной информации;

– УБИ.087 Угроза несанкционированного использования привилегированных функций BIOS;

– УБИ.088 Угроза несанкционированного копирования защищаемой информации;

– УБИ.089 Угроза несанкционированного редактирования реестра;

– УБИ.090 Угроза несанкционированного создания учётной записи пользователя;

– УБИ.091 Угроза несанкционированного удаления защищаемой информации;

– УБИ.093 Угроза несанкционированного управления буфером;

– УБИ.095 Угроза несанкционированного управления указателями;

– УБИ.098 Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб;

– УБИ.099 Угроза обнаружения хостов;

– УБИ.100 Угроза обхода некорректно настроенных механизмов аутентификации;

– УБИ.103 Угроза определения типов объектов защиты;

– УБИ.104 Угроза определения топологии вычислительной сети;

– УБИ.109 Угроза перебора всех настроек и параметров приложения;

– УБИ.111 Угроза передачи данных по скрытым каналам;

– УБИ.115 Угроза перехвата вводимой и выводимой на периферийные устройства информации;

– УБИ.116 Угроза перехвата данных, передаваемых по вычислительной сети;

– УБИ.118 Угроза перехвата привилегированного процесса;

– УБИ.121 Угроза повреждения системного реестра;

– УБИ.122 Угроза повышения привилегий;

– УБИ.123 Угроза подбора пароля BIOS;

– УБИ.124 Угроза подделки записей журнала регистрации событий;

– УБИ.127 Угроза подмены действия пользователя путём обмана;

– УБИ.128 Угроза подмены доверенного пользователя;

– УБИ.129 Угроза подмены резервной копии программного обеспечения BIOS;

– УБИ.130 Угроза подмены содержимого сетевых ресурсов;

– УБИ.131 Угроза подмены субъекта сетевого доступа;

– УБИ.132 Угроза получения предварительной информации об объекте защиты;

– УБИ.139 Угроза преодоления физической защиты;

– УБИ.143 Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;

– УБИ.144 Угроза программного сброса пароля BIOS;

– УБИ.145 Угроза пропуска проверки целостности программного обеспечения;

– УБИ.149 Угроза сбоя обработки специальным образом изменённых файлов;

– УБИ.150 Угроза сбоя процесса обновления BIOS;

– УБИ.152 Угроза удаления аутентификационной информации;

– УБИ.153 Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов;

– УБИ.154 Угроза установки уязвимых версий обновления программного обеспечения BIOS;

– УБИ.155 Угроза утраты вычислительных ресурсов;

– УБИ.156 Угроза утраты носителей информации;

– УБИ.157 Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;

– УБИ.158 Угроза форматирования носителей информации;

– УБИ.160 Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации;

– УБИ.167 Угроза заражения компьютера при посещении неблагонадёжных сайтов;

– УБИ.168 Угроза «кражи» учётной записи доступа к сетевым сервисам;

– УБИ.170 Угроза неправомерного шифрования информации;

– УБИ.171 Угроза скрытного включения вычислительного устройства в состав бот-сети;

– УБИ.172 Угроза распространения «почтовых червей»;

– УБИ.174 Угроза «фарминга»;

– УБИ.175 Угроза «фишинга»;

– УБИ.177 Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью;

– УБИ.178 Угроза несанкционированного использования системных и сетевых утилит;

– УБИ.179 Угроза несанкционированной модификации защищаемой информации;

– УБИ.185 Угроза несанкционированного изменения параметров настройки средств защиты информации;

– УБИ.186 Угроза внедрения вредоносного кода через рекламу, сервисы и контент;

– УБИ.187 Угроза несанкционированного воздействия на средство защиты информации;

– УБИ.188 Угроза подмены программного обеспечения;

– УБИ.189 Угроза маскирования действий вредоносного кода;

– УБИ.190 Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет;

– УБИ.191 Угроза внедрения вредоносного кода в дистрибутив программного обеспечения;

– УБИ.192 Угроза использования уязвимых версий программного обеспечения;

– УБИ.193 Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика;

– УБИ.197 Угроза хищения аутентификационной информации из временных файлов cookie;

– УБИ.198 Угроза скрытной регистрации вредоносной программой учетных записей администраторов;

– УБИ.208 Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники;

– УБИ.212 Угроза перехвата управления информационной системой;

– УБИ.217 Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения.

В целях выполнения требований нормативных правовых документов Российской Федерации, нормативно-методических и руководящих документов ФСТЭК России и ФСБ России, для пользовательского сегмента должна быть разработана организационно-распорядительная документация, необходимая для эксплуатации системы защиты информации.

Разрабатываемая организационно-распорядительная документация в общем случае должна регламентировать следующие вопросы обработки и защиты информации (в том числе персональных данных):

– порядок учета и эксплуатации информационных ресурсов и средств обработки информации;

– порядок предоставления доступа к информационным ресурсам и средствам обработки информации;

– порядок внесения изменений в программное обеспечения и аппаратную часть средств обработки информации;

– порядок действий в ходе эксплуатации информационных систем, аттестованных по требованиям безопасности информации;

– правила и процедуры антивирусной защиты информации;

– правила и процедуры использования аутентификационной информации;

– правила и процедуры обеспечения отказоустойчивости технических средств информационных систем;

– правила и процедуры резервного копирования и восстановления защищаемой информации;

– правила и процедуры обеспечения сетевой безопасности информационных систем;

– правила и процедуры аудита информационной безопасности;

– правила и процедуры управления инцидентами информационной безопасности;

– правила и процедуры использования средств криптографической защиты информации.

Указанные организационно-распорядительные документы должны разрабатываться с учетом требований Приказа ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

3.3. Требования к составу системы защиты информации

В соответствии с Техническим проектом подсистемы защиты информации региональной государственной информационной системы «Автоматизированная система управления сферой образования Краснодарского края» министерства образования и науки Краснодарского края в состав системы защиты информации пользовательского сегмента должны входить следующие сертифицированные средства защиты информации:

– средство защиты информации от несанкционированного доступа;

– средство межсетевого экранирования;

– средство антивирусной защиты информации;

– средство обнаружения (предотвращения) вторжений;

– средство анализа защищенности;

– средство криптографической защиты информации при её передаче по каналам связи.

3.4. Требования к аттестации пользовательского сегмента

Аттестация пользовательского сегмента должна проводится с целью подтверждения выполнения требований безопасности информации, предъявляемым к классу защищенности К3 (для государственных информационных систем), УЗ3 (для информационных систем, в которых осуществляется обработка персональных данных).

Работы по проведению аттестационных испытаний должны осуществляться следующими методами проверок и испытаний:

– экспертно-документальный – проверка соответствия сегмента системы установленным требованиям на основании экспертной оценки полноты и достаточности представленных документов по обеспечению мероприятий по защите информации;

– инструментальный – контроль с применением тестов, проводящийся с целью подтверждения реализации функций защиты информации от НСД, соответствующих установленному классу защищенности сегмента системы.

Экспертно-документальный метод проверки включает в себя:

– анализ и оценку исходных данных и документации по защите информации на объекте информатизации;

– проверка соответствия представленных Заказчиком исходных данных реальным условиям размещения, монтажа и эксплуатации технических средств:

- проверка соответствия контролируемой зоны представленной документации;
- проверка соответствия расположения средств обработки информации представленной документации;

– проверка технологического процесса обработки, передачи и хранения защищаемой информации;

– анализ информационных потоков, определение состава технических средств, используемых для обработки, передачи и хранения защищаемой информации;

– проверка и оценка достаточности и полноты сведений, определяющих состояние организации работ и выполнения организационно-технических требований по защите информации;

– проверка наличия и оценка достаточности и полноты документов, позволяющих правильно классифицировать сегмент системы;

– оценка полноты и уровня разработки организационно-распорядительной, проектной и эксплуатационной документации;

– оценка уровня подготовки кадров и распределения ответственности за выполнение требований по защите информации.

Инструментальный метод проверки включает в себя испытания сегмента системы на соответствие требованиям по защите информации от несанкционированного доступа, в том числе от разрушающих программных воздействий, нарушающих целостность информации или работоспособность технических средств и от компьютерных вирусов.

До проведения аттестационных испытаний должна быть согласована и утверждена программа и методики проведения аттестационных испытаний сегмента системы.

По результатам аттестационных испытаний должны предоставляться следующие документы:

– акт обследования сегмента системы;

– протокол проведения испытаний сегмента системы на соответствие требованиям по защите от несанкционированного доступа к защищаемым ресурсам;

– заключение по результатам аттестации сегмента системы на соответствие требованиям по безопасности информации;

– аттестат соответствия сегмента системы требованиям безопасности информации.

Проведение аттестации должно осуществляться с учетом требований ГОСТ РО 0043-004-2013, ГОСТ РО 0043-003-2012 и Приказа ФСТЭК России 29 апреля 2021 года № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

4. ТРЕБОВАНИЯ К ИСПОЛНИТЕЛЮ, ОСУЩЕСТВЛЯЮЩЕМУ АТТЕСТАЦИОННЫЕ ИСПЫТАНИЯ

В соответствии со статьей 12 Федерального закона от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» исполнитель обязан обладать следующими лицензиями:

1. Лицензия Федеральной службы по техническому и экспортному контролю Российской Федерации на осуществление деятельности по технической защите конфиденциальной информации, выданную на основании Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 03 февраля 2012 г. № 79, с включением в указанную лицензию следующих видов деятельности:

– п.4, пп.(е). Услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).

– п.4, пп (г) аттестационные испытания и аттестация на соответствие требованиям по защите информации средств и систем информатизации.

2. Лицензия ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

Заместитель начальника отдела
проектного сопровождения
и информационной безопасности А.В. Платонова