Приложение № 11
к распоряжению Администрации
городского округа Химки
Московской области
от 30.09.2021 № 56-р

**Требования к сегменту**

соответствующему типовому сегменту
информационной системы
«Государственная информационная система «Единая информационная система обеспечения выполнения функций ЦИОГВ и ГО Московской области: аккредитации, лицензионной и разрешительной деятельности, планирования и учета результатов контрольных мероприятий, в том числе учета выявленных административных правонарушений»
Министерства государственного управления, информационных технологий и связи Московской области
**при условии соблюдения которых**
**на сегмент может распространяться действие Аттестата соответствия**

19937100.460650.076ТС-3018-1

## Содержание

## Перечень принятых сокращений

В данном документе используются следующие сокращения:

| | | |
|---|---|---|
| **АРМ** | – | автоматизированное рабочее место |
| **БД** | – | база данных |
| **БИ** | – | безопасность информации |
| **ЗИ** | – | защита информации |
| **ИБ** | – | информационная безопасность |
| **ИР** | – | информационный ресурс |
| **ИС** | – | информационная система |
| **КЗ** | – | контролируемая зона |
| **КС** | – | криптосредство |
| **ЛВС** | – | локальная вычислительная сеть |
| **НСД** | – | несанкционированный доступ; |
| **ОЗУ** | – | оперативное запоминающее устройство |
| **ОРД** | – | организационно-распорядительный документ |
| **ОС** | – | операционная система |
| **ПО** | – | программное обеспечение |
| **РВС** | – | распределенная вычислительная сеть |
| **СВТ** | – | средство вычислительной техники |
| **СБ** | – | система безопасности |
| **СКЗИ** | – | средство криптографической защиты информации |
| **СПД** | – | сеть передачи данных |
| **СрЗИ** | – | средство защиты информации |
| **ССОП** | – | сеть связи общего пользования |
| **СФК** | – | среда функционирования |
| **ФСБ России** | – | Федеральная служба безопасности Российской Федерации |
| **ФСТЭК России** | – | Федеральная служба по техническому и экспортному контролю |

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения:

**Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Безопасность критической информационной инфраструктуры** – состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак.

**Значимый объект критической информационной инфраструктуры –** объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры.

**Вирус (компьютерный, программный)** – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**Доступ в операционную среду компьютера** – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

**Доступ к информации** – возможность получения информации и ее использования.

**Защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Идентификация –** присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Информационная система**– совокупность содержащихся в базах данных информации и обеспечивающих их обработку информационных технологий и технических средств.

**Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Источник угрозы безопасности информации** – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Контролируемая зона** – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

**Конфиденциальность информации –** обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта информации или наличия иного законного основания.

**Компьютерный инцидент** – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

**Критическая информационная инфраструктура** – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

**Межсетевой экран** – локальное (однокомпонентное) или функционально-распределённое программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

**Нарушитель безопасности** – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при их обработке техническими средствами в информационных системах информации.

**Недекларированные возможности** – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

**Несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

**Обработка информации** – действия (операции) с информацией, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение информации.

**Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку информации, а также определяющие цели и содержание обработки персональных данных.

**Объекты критической информационной инфраструктуры** – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

**Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

**Пользователь** – лицо, участвующее в функционировании объекта критической информационной инфраструктуры или использующее результаты его функционирования.

**Правила разграничения доступа** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Ресурс** – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**Средства вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Субъект доступа (субъект)** – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Субъекты критической информационной инфраструктуры** – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

**Технические средства** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ЗИ (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

**Технический канал утечки информации** – совокупность носителя информации (средства обработки), физической среды распространения

информативного сигнала и средств, которыми добывается защищаемая информация.

**Типовые сегменты (сегменты одного типа) -** сегменты, реализующие полную технологию обработки информации, в которых установлены одинаковые категорий значимости (классы защищенности), одинаковые угрозы безопасности информации, реализованы одинаковые проектные решения по информационной системе и ее системе безопасности.

**Угрозы безопасности** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение защищаемой информации, а также иных несанкционированных действий при их обработке в информационной системе.

**Уничтожение информации –** действия, в результате которых становится невозможным восстановить содержание информации в информационной системе информации и (или) в результате которых уничтожаются материальные носители информации.

**Уязвимость** – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

**Целостность информации** – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

## 1 Общие положения

В соответствии с абз. 3 п. 17.3 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных

информационных системах, утверждённых приказом ФСТЭК России от 11.02.2013 г. № 17 (далее – Приказ № 17), сегмент считается соответствующим сегменту ИС, в отношении которого были проведены аттестационные испытания, если для указанных сегментов установлены одинаковые классы защищённости, угрозы БИ, реализованы одинаковые проектные решения по ИС и её СБ.

Настоящий документ определяет технические и организационные требования для подключения АРМ и серверов к СБ объекта критической информационной инфраструктуры Единой информационной системы оказания государственных и муниципальных услуг (далее – ЕИС ОУ) Московской области Министерства государственного управления, информационных технологий и связи Московской области в качестве сегмента, соответствующего типовому сегменту ЕИС ОУ, прошедшему аттестационные испытания.

Настоящий документ определяет условия и порядок распространения аттестата соответствия требованиям безопасности информации ЕИС ОУ, выданного ООО «Сэйл АйТи», на вновь вводимый сегмент ЕИС ОУ, соответствующий типовым сегментам ЕИС ОУ, прошедшим аттестационные испытания.

## 2 Описание типовых сегментов ЕИС ОУ

В ЕИС ОУ при проведении аттестационных испытаний был выделен следующий набор типовых сегментов:

- сегмент 1 – типовой сегмент «Сервер СУБД»;

- сегмент 2 – типовой сегмент «Сервер приложений»;

- сегмент 3 – типовой сегмент «АРМ пользователя информационной системы – W»;

- сегмент 4 – типовой сегмент «АРМ пользователя информационной системы – L»;

- сегмент 5 – типовой сегмент «АРМ администратора информационной системы».

Таблица 1 – Сведения о назначении типовых сегментов ЕИС ОУ

| № п/п | Типовой сегмент | Назначение типового сегмента |
|---|---|---|
| 1. | «Сервер СУБД» | Предназначен для хранения баз данных на сервера ЕИС ОУ, расположенных в ЦОД ДПМО |
| 2. | «Сервер приложений» | Предназначен для хранения и предоставления доступа к информации ограниченного доступа операторам |
| 3. | «АРМ пользователя информационной системы – W» | Предназначен для обработки информации операторами с АРМ под управлением ОС Windows |
| 4. | «АРМ пользователя информационной системы – L» | Предназначен для обработки информации операторами с АРМ под управлением ОС Linux |
| 5. | «АРМ администратора информационной системы» | Предназначен для управления ЕИС ОУ, в том числе системой безопасности ЕИС ОУ администраторами ЕИС ОУ |

Результаты классификации ЕИС ОУ и типовых сегментов ЕИС ОУ приведены в таблицах 2, 3 соответственно.

Таблица 2 – Результаты классификации ЕИС ОУ

| Объект | Категория значимости | Класс защищённости | Уровень защищенности | Тип актуальных угроз БИ |
|---|---|---|---|---|
| ЕИС ОУ | третья категория значимости (К3) | третий класс защищённости (К3) | третий уровень защищенности (УЗ3) | Третий |

Таблица 3 –

Таблица 4 – Результаты классификации типовых сегментов ЕИС ОУ

| Типовой сегмент | Категория значимости | Класс защищённости | Уровень защищенности | Тип актуальных угроз БИ |
|---|---|---|---|---|
| «Сервер СУБД» | третья категория значимости (К3) | третий класс защищённости (К3) | третий уровень защищенности (УЗ3) | Третий |
| «Сервер приложений» | третья категория значимости (К3) | третий класс защищённости (К3) | третий уровень защищенности (УЗ3) | Третий |
| «АРМ пользователя информационной системы – W» | третья категория значимости (К3) | третий класс защищённости (К3) | третий уровень защищенности (УЗ3) | Третий |
| «АРМ пользователя информационной системы – L» | третья категория значимости (К3) | третий класс защищённости (К3) | третий уровень защищенности (УЗ3) | Третий |
| «АРМ администратора информационной системы» | третья категория значимости (К3) | третий класс защищённости (К3) | Обработка ПДн не осуществлется | Третий |

Перечни актуальных угроз БИ типовых сегментов ЕИС ОУ представлены в модели угроз БИ при их обработке в ЕИС ОУ. Схема проектных решений по СБ в ЕИС ОУ иллюстрирована на рисунке 1.

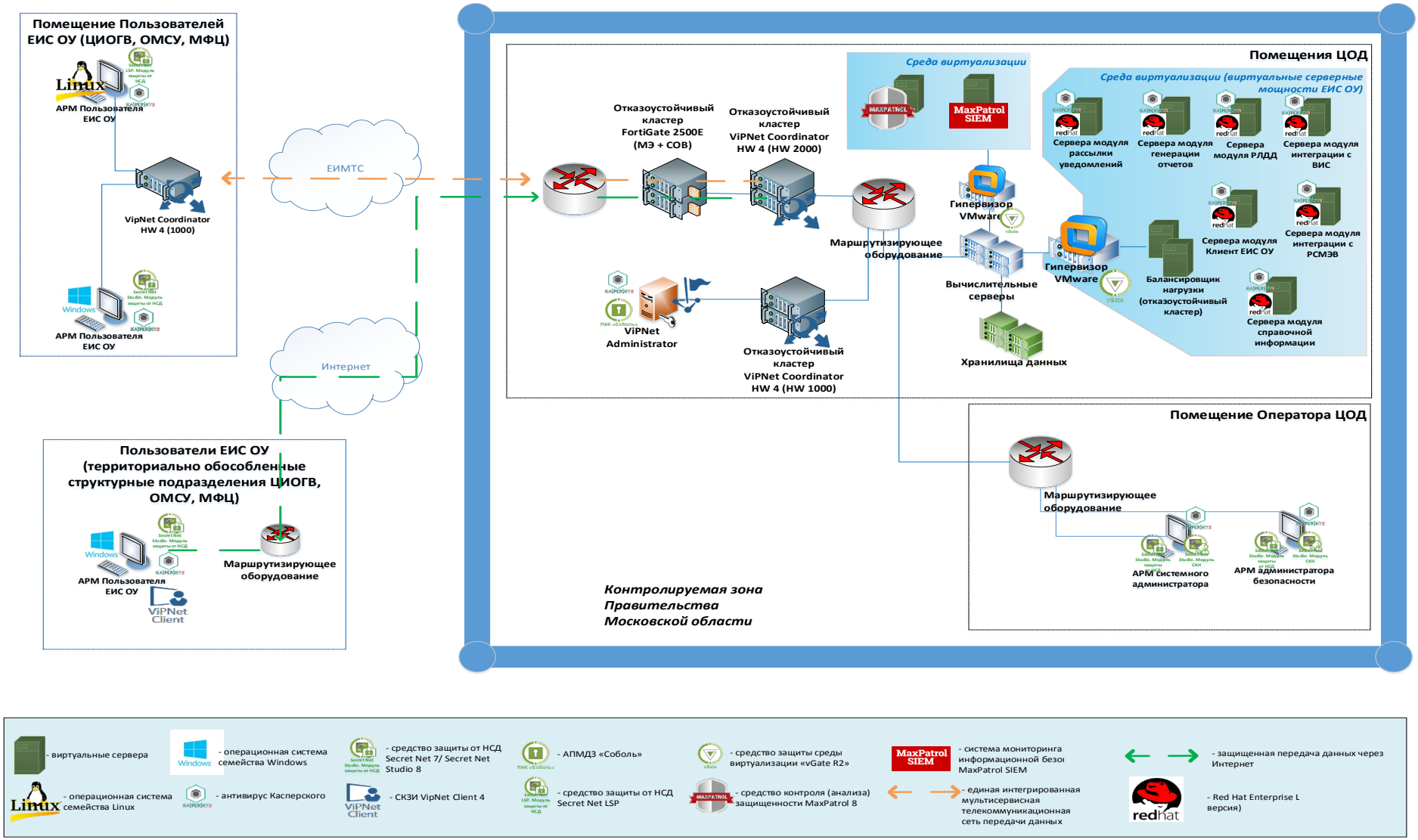


Рисунок 1 – Схема проектных решений по СБ в ЕИС ОУ

## 3 Технические требования для защищённого подключения АРМ (сервер) типовых сегментов к ЕИС ОУ

Для защищённого подключения АРМ (сервер) типовых сегментов к ЕИС ОУ требуется:

- в соответствии с таблицей 1 определить роль пользователя, подключаемого АРМ (сервера) к ЕИС ОУ;

- на основе роли пользователя, подключаемого АРМ (сервера) к СБ ЕИС ОУ по таблице 4 настоящего документа определить типовой сегмент ЕИС ОУ в который будет подключаться АРМ (сервер);

- в соответствии с таблицами 2 и 3 определить максимальные категорию значимости, класс и уровень защищённости, которые необходимо обеспечить в подключаемом АРМ (сервере);

- по таблице 4 определить проектные решения по СБ в выбранном типовом сегменте;

- провести установку на подключаемый АРМ (сервер) и настройку средств защиты информации в соответствии с Руководством администратора безопасности ЕИС ОУ и Описанием порядка и параметров настройки средств защиты информации системы безопасности ЗО КИИ «Единая информационная система оказания государственных и муниципальных услуг Московской области» Министерства государственного управления, информационных технологий и связи Московской области;

- для подключаемого АРМ (сервера) реализовать меры защиты информации, принятые в целях нейтрализации угроз БИ в соответствующем типовом сегменте ЕИС ОУ, приведённые в таблице 6.

Таблица 5 – Описание проектных решений по ЕИС ОУ и её СБ в отдельных типовых сегментах ЕИС ОУ в рамках технологии обработки информации в этих сегментах

| № п/п | Типовой сегмент ЕИС ОУ | Описание проектных решений по ЕИС ОУ* | Описание проектных решений по СБ ЕИС ОУ* |
|---|---|---|---|
| 1. | «Сервер СУБД» | Предназначен для хранения баз данных на серверах ЕИС ОУ, расположенных в ЦОД ДПМО | Средство антивирусной защиты Kaspersky Endpoint Security 10 Сертификат соответствия ФСТЭК России № 3025;<br>Система защиты информации от несанкционированного доступа Secret Net LSP Сертификат соответствия ФСТЭК России № 2790 |
| 2. | «Сервер приложений» | Предназначен для хранения и предоставления доступа к информации ограниченного доступа операторам | Средство антивирусной защиты Kaspersky Endpoint Security 10 Сертификат соответствия ФСТЭК России № 3025;<br>Система защиты информации от несанкционированного доступа Secret Net LSP Сертификат соответствия ФСТЭК России № 2790 |
| 3. | «АРМ пользователя информационной системы – W» | Предназначен для обработки информации операторами с АРМ под управлением ОС Windows | Средство антивирусной защиты Kaspersky Endpoint Security 10 Сертификат соответствия ФСТЭК России № 3025;<br>Система защиты информации от несанкционированного доступа Secret Net Studio 8 Сертификат соответствия ФСТЭК России № 3745;<br>Средство межсетевого экранирования VipNet (VipNet 4 Сертификат соответствия ФСТЭК России № 3727 / ViPNet Coordinator HW 4 Сертификат соответствия ФСТЭК России № 3692 |
| 4. | «АРМ пользователя информационной системы – L» | Предназначен для обработки информации операторами с АРМ под управлением ОС Linux | Средство антивирусной защиты Kaspersky Endpoint Security 10 Сертификат соответствия ФСТЭК России № 3025; |

| № п/п | Типовой сегмент ЕИС ОУ | Описание проектных решений по ЕИС ОУ* | Описание проектных решений по СБ ЕИС ОУ* |
|---|---|---|---|
| | | | Система защиты информации от несанкционированного доступа Secret Net LSP Сертификат соответствия ФСТЭК России № 2790;<br>Средство межсетевого экранирования VipNet Coordinator HW 4 Сертификат соответствия ФСТЭК России № 3692 |
| 5. | «АРМ администратора информационной системы» | Предназначен для управления ЕИС ОУ, в том числе системой безопасности ЕИС ОУ администраторами ЕИС ОУ | Средство антивирусной защиты Kaspersky Endpoint Security 10 Сертификат соответствия ФСТЭК России № 3025;<br>Система защиты информации от несанкционированного доступа Secret Net Studio 8 Сертификат соответствия ФСТЭК России № 3745 |

*приведены проектные решения уровня ЕИС ОИ и СБ ЕИС ОУ (описание проектных решений ЦОД ДПМО и СЗИ ЦОД ДПМО приведено в проектной документации на ЦОД ДПМО)

Таблица 6 – Реализованные наборы мер по защите информации в типовых сегментах ЕИС ОУ

| **Типовой сегмент** | **Итоговый набор мер защиты информации*** |
|---|---|
| Типовой сегмент «Сервер СУБД» | ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6, УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.10, УПД.11, ОПС.3, ЗНИ.1, ЗНИ.2, ЗНИ.5, ЗНИ.8, РСБ.1, РСБ.2, РСБ.3, РСБ.4, РСБ.7, АВЗ.1, АВЗ.2, АНЗ.3, АНЗ.4, ОЦЛ.3, ЗТС.2, ЗТС.3,ЗТС.4, ЗИС.5 |
| Типовой сегмент «Сервер приложений» | ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6, УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.10, УПД.11, ОПС.3, ЗНИ.1, ЗНИ.2, ЗНИ.5, ЗНИ.8, РСБ.1, РСБ.2, РСБ.3, РСБ.4, РСБ.7, АВЗ.1, АВЗ.2, АНЗ.3, АНЗ.4, ОЦЛ.3, ЗТС.2, ЗТС.3,ЗТС.4, ЗИС.5 |
| Типовой сегмент «АРМ пользователя информационной системы – W» | ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6, УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.10, УПД.11, УПД.13, ОПС.3, ЗНИ.1, ЗНИ.2, ЗНИ.5, ЗНИ.8, РСБ.1, РСБ.2, РСБ.3, РСБ.4, РСБ.6, РСБ.7, АВЗ.1, АВЗ.2, АНЗ.3, АНЗ.4, ОЦЛ.3, ЗТС.2, ЗТС.3,ЗТС.4, ЗИС.3, ЗИС.5 |
| Типовой сегмент «АРМ пользователя информационной системы – L» | ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6, УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.10, УПД.11, УПД.13, ОПС.3, ЗНИ.1, ЗНИ.2, ЗНИ.5, ЗНИ.8, РСБ.1, РСБ.2, РСБ.3, РСБ.4, РСБ.6, РСБ.7, АВЗ.1, АВЗ.2, АНЗ.3, АНЗ.4, ОЦЛ.3, ЗТС.2, ЗТС.3,ЗТС.4, ЗИС.3, ЗИС.5 |
| Типовой сегмент «АРМ администратора информационной системы» | ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6, УПД.1, УПД.2, УПД.3, УПД.4, УПД.5, УПД.6, УПД.10, УПД.11, УПД.13, ОПС.3, ЗНИ.1, ЗНИ.2, ЗНИ.5, ЗНИ.8, РСБ.1, РСБ.2, РСБ.3, РСБ.4, РСБ.6, РСБ.7, АВЗ.1, АВЗ.2, АНЗ.3, АНЗ.4, ОЦЛ.3, ЗТС.2, ЗТС.3,ЗТС.4, ЗИС.5 |

*набор мер, выполняемый в рамках СБ ЕИС ОУ (не содержит меры, реализуемые на уровне СЗИ ЦОД ДПМО)

## 4. Организационные требования для защищённого подключения АРМ (серверов) типовых сегментов ЕИС ОУ

4.1. Все пользователи (администраторы) подключаемого АРМ (сервера) типового сегмента к СБ ЕИС ОУ обязаны ознакомиться с техническими и организационно-распорядительными документами (см. таблицу 6) соответствующего типового сегмента (таблица 1). При возникновении трудностей в понимании положений такой документации работникам необходимо пройти соответствующее обучение (в области обеспечения безопасности персональных данных, защиты государственных информационных систем, защиты объектов КИИ, работы с криптографическими средствами, конфигурирования активного сетевого оборудования и др.).

4.2. На подключаемом АРМ (сервере) типового сегмента к СБ ЕИС ОУ должны быть реализованы организационные меры, приведённые в таблице 5 настоящего документа.

4.3. Кроме того, для подключаемого АРМ (сервера) типового сегмента к СБ ЕИС ОУ в соответствии с таблицей 6 должна быть разработана (размножены, доработаны, скорректированы, актуализированы) техническая и организационно-распорядительная документация.

Таблица 7 – Требования к наличию документации в типовых сегментах ЕИС ОУ

| № п/п | Наименование документа | Необходимость наличия (разработки) в типовом сегменте |
|---|---|---|
| 1 | Технический паспорт сегмента ЕИС ОУ | + |
| 2 | Инструкция по защите информации пользователям ЕИС ОУ[1] | |
| 3 | Руководство пользователя СБ ЗО КИИ ЕИС ОУ | + |
| 4 | Руководство администратора СБ ЗО КИИ ЕИС ОУ | + |
| 5 | Инструкция по организации антивирусной защиты[1] | |
| 6 | Инструкция по парольной защите в ЕИС ОУ[1] | |
| 7 | Акт соответствия Сегмента ЕИС ОУ Сегменту в отношении, которого были проведены аттестационные испытания по требованиям безопасности информации | + |
| 8 | Список пользователей Сегмента ЕИС ОУ | + |
| 9 | Акт классификации Сегмента ЕИС ОУ по требованиям защиты информации для каждого Сегмента ЕИС ОУ | + |
| 10 | Описание разрешительной системы доступа пользователей к Сегменту ЕИС ОУ для каждого Сегмента | + |

[1] Допускается использовать документы, разработанные для ЕИСОУ в целом, а не для каждого ее сегмента