

УТВЕРЖДАЮ

Директор ГКУ МО ЦБ МО

А.А. Осотов

М.П.

«29» 2024 г.



РЕГЛАМЕНТ

подключения к информационной системе

«Бухгалтерия, кадровый учет и документооборот»

Государственного казенного учреждения Московской области

«Централизованная бухгалтерия Московской области»

Москва 2024

Оглавление

Сокращения и определения.....	3
1. Общие положения.....	3
2. Порядок организации подключения	5
3. Схемы подключения к ИС	7
4. Требования к реализации системы защиты информации и защищенного взаимодействия	9
5. Ответственность.....	9
Приложение к Регламенту	10

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

АРМ – автоматизированное рабочее место.

Внешние пользователи – участники информационного взаимодействия, осуществляющие подключение к информационной системе «Бухгалтерия, кадровый учет и документооборот» Государственного казенного учреждения Московской области «Централизованная бухгалтерия Московской области» с использованием внешних информационно-телекоммуникационных сетей, не входящих в контролируемую зону, в которой функционируют программные и технические средства ИС «Бухгалтерия, кадровый учет и документооборот».

ЕИМТС – единая интегрированная мультисервисная телекоммуникационная сеть передачи данных.

ИС – информационная система.

Оператор ИС – оператор информационной системы «Бухгалтерия, кадровый учет и документооборот» Государственного казенного учреждения Московской области «Централизованная бухгалтерия Московской области».

СКЗИ – средства криптографической защиты информации.

Учреждение – обособляемая(ое) организация или учреждение.

ФСТЭК России – Федеральная служба по техническому и экспортному контролю.

ФСБ России – Федеральная служба безопасности Российской Федерации.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Регламент подключения внешних пользователей к информационной системе «Бухгалтерия, кадровый учет и документооборот» (далее соответственно – Регламент, ИС «Бухгалтерия, кадровый учет и документооборот») определяет общий состав, содержание и порядок выполнения участниками информационного взаимодействия работ по защите информации при их подключении к ИС «Бухгалтерия, кадровый учет и документооборот».

1.2. Регламент разработан в соответствии с:

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

Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее - Федеральный закон от 27.07.2006 г. № 152-ФЗ);

постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

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

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

приказом ФСТЭК России от 29 апреля 2021 г. № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;

Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 г. (ДСП);

Методическим документом «Методика оценки угроз безопасности информации», утвержденным ФСТЭК России 5 февраля 2021 г.;

приказом ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

приказом ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

Методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (утверждены руководством 8 Центра ФСБ России от 31 марта 2015 г. № 149/7/2/6-432);

нормативно-методическими документами Московской области.

1.3. Регламент устанавливает порядок, способы подключения и правила осуществления защищенного взаимодействия между ИС «Бухгалтерия, кадровый учет и документооборот» и обслуживаемыми учреждениями, включая обязанности сторон.

1.4. Оператором ИС «Бухгалтерия, кадровый учет и документооборот» является Государственное казенное учреждение Московской области «Централизованная бухгалтерия Московской области».

1.5. Контактные данные Оператора ИС: cbmo_iso@mosreg.ru.

1.6. Основной целью Регламента является определение необходимых мероприятий по обеспечению информационной безопасности, проводимых участниками информационного взаимодействия при подключении к ИС «Бухгалтерия, кадровый учет и документооборот».

1.7. Организация защищенного взаимодействия с информационными системами ИС «Бухгалтерия, кадровый учет и документооборот» осуществляется:
с помощью ЕИМТС;

по технологии виртуальных защищенных сетей, с использованием средств криптографической защиты информации ViPNet сети № 2131.

1.8. Регламент (изменения, дополнения, приложения) публикуется в форме электронного документа в сети Интернет на сайте: <https://cbmo.mosreg.ru/docs>.

2. ПОРЯДОК ОРГАНИЗАЦИИ ПОДКЛЮЧЕНИЯ

2.1. Для подключения обслуживаемой организации к ИС «Бухгалтерия, кадровый учет и документооборот» необходимо выполнить следующие действия:

заключить с Государственным казенным учреждением Московской области «Централизованная бухгалтерия Московской области» договор на обслуживание;

определить перечень подключаемых к ИС «Бухгалтерия, кадровый учет и документооборот» АРМ;

выбрать схему подключения к ИС «Бухгалтерия, кадровый учет и документооборот» в соответствии с разделом 3 настоящего Регламента;

подключиться к сети ViPNet сети № 2131 или к ЕИМТС;

обеспечить защиту конфиденциальности и целостности передаваемой по каналам связи информации;

выполнить обязательные организационные мероприятия, необходимые при эксплуатации СКЗИ в соответствии с требованиями нормативных документов ФСБ России и документацией на СКЗИ;

обеспечить выполнение требований ст. 18.1, ст. 19 Федерального закона от 27.07.2006 г. № 152-ФЗ;

на подключаемых АРМ выполнить организационные и технические меры защиты информации, соответствующие 3-му уровню защищенности персональных данных в информационных системах;

провести оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИС персональных данных;

направить Оператору ИС через МСЭД или на электронную почту (пункт 1.5) уведомление о готовности к подключению к ИС «Бухгалтерия, кадровый учет и документооборот» за подписью руководителя Учреждения с указанием выбранной

схемы подключения (далее – Уведомление) по форме согласно приложению к настоящему Регламенту;

провести подключение и проверить работоспособность подключения к ИС «Бухгалтерия, кадровый учет и документооборот»;

периодически проводить контроль выполнения мероприятий по обеспечению защиты информации.

2.2. В случае изменения схемы подключения необходимо провести повторное подключение.

2.3. В случае выявления инцидентов информационной безопасности, повлекших неправомерную или случайную передачу (предоставление, распространение, доступ) персональных данных, в результате которого произошло нарушение прав субъектов персональных данных, участники информационного взаимодействия уведомляют через МСЭД или на электронную почту (пункт 1.5) друг друга в течение 24 часов с момента выявления инцидента.

2.4. В случае изменения сведений, указанных в Уведомлении, направить Оператору ИС через МСЭД или на электронную почту (пункт 1.5) актуальные сведения в течение 5 рабочих дней с момента изменения.

3. СХЕМЫ ПОДКЛЮЧЕНИЯ К ИС

Схема подключения № 1

Внешние пользователи производят подключение к ИС «Бухгалтерия, кадровый учет и документооборот» с АРМ при помощи программного СКЗИ ViPNet Client for Windows или ViPNet Client for Linux (Рисунок 1).

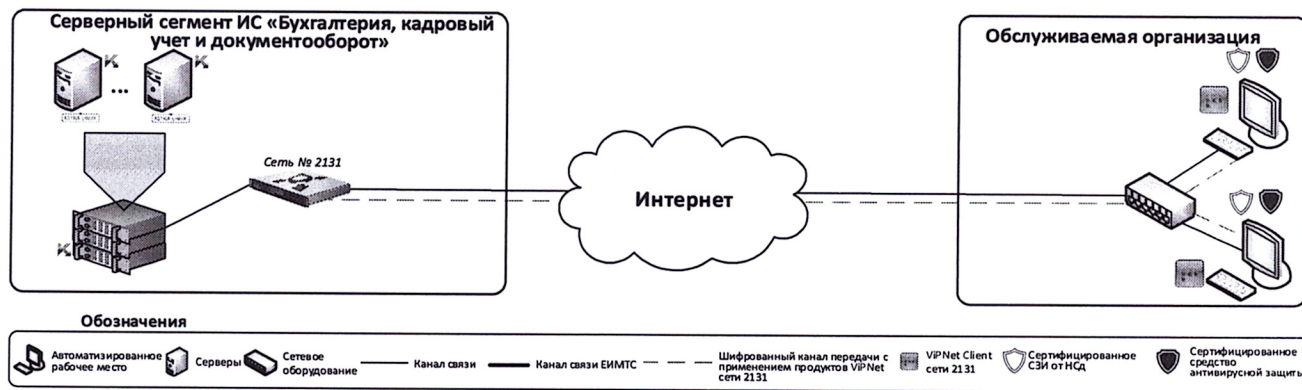


Рисунок 1

Схема подключения № 2

Внешние пользователи производят подключение к ИС «Бухгалтерия, кадровый учет и документооборот» с АРМ при помощи программно-аппаратного СКЗИ ViPNet Coordinator (Рисунок 2).

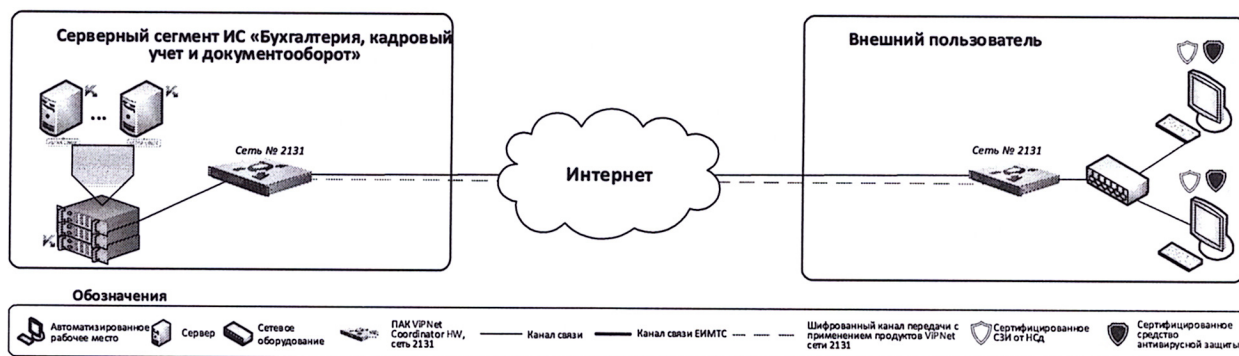


Рисунок 2

Схема подключения № 3

Внешние пользователи производят подключение к ИС «Бухгалтерия, кадровый учет и документооборот» с АРМ, находящихся в составе ЕИМТС (Рисунок 3).

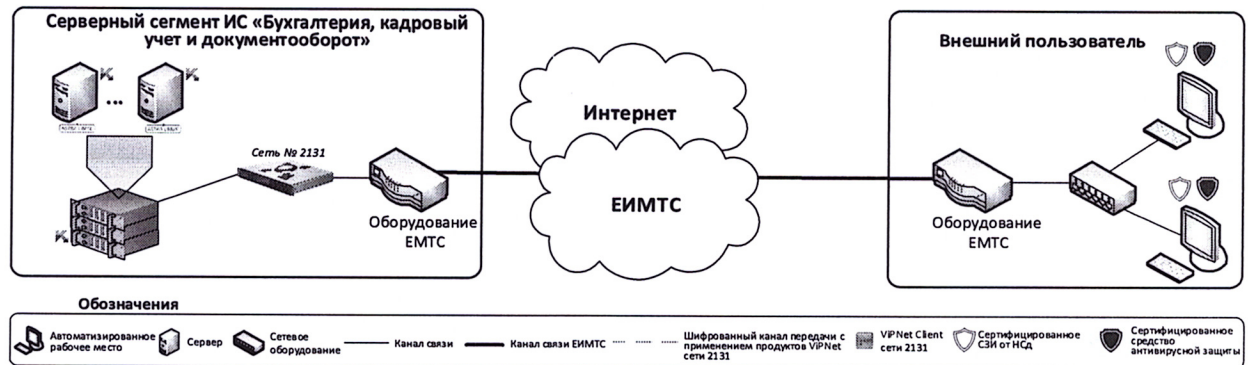


Рисунок 3

4. ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ И ЗАЩИЩЕННОГО ВЗАИМОДЕЙСТВИЯ

В целях организации защищенного информационного взаимодействия и обеспечения требований по защите информации участники информационного взаимодействия должны обеспечить реализацию следующих организационных мероприятий:

4.1. Организационные мероприятия, включают:

4.1.1. Назначение ответственного за организацию обработки защищаемой информации;

4.1.2. Назначение ответственного за обеспечение безопасности защищаемой информации;

4.1.3. Определение перечней сотрудников, осуществляющих обработку защищаемой информации и имеющих доступ к обрабатываемой защищаемой информации;

4.1.4. Определение перечня мер по обеспечению безопасности помещений, в которых размещены информационные системы защищаемой информации и сохранности носителей защищаемой информации;

4.1.5. Определение перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием СКЗИ.

Не допускается взаимодействие АРМ внешних пользователей с ИС «Бухгалтерия, кадровый учет и документооборот» при неполной или некорректной реализации защищенного подключения, невыполнении всех необходимых требований по обеспечению информационной безопасности, отсутствию или некорректной настройке технических средств защиты информации.

5. ОТВЕТСТВЕННОСТЬ

5.1. За неисполнение или ненадлежащее исполнение обязательств, предусмотренных настоящим Регламентом, Учреждение и Оператор ИС несут ответственность в соответствии с законодательством Российской Федерации, законодательством Московской области.

5.2. Учреждение и Оператор ИС не несут ответственность за возможные временные задержки по исполнению требований настоящего Регламента, возникшие по вине лиц, предоставляющих услуги связи, а также вследствие обстоятельств непреодолимой силы.

Приложение
к Регламенту

Уведомление о готовности к подключению

В соответствии с Регламентом подключения к информационной системе «Бухгалтерия, кадровый учет и документооборот» Государственного казенного учреждения Московской области «Централизованная бухгалтерия Московской области» (далее – Регламент) сообщаю следующие сведения:

Полное наименование организации:	
Сокращенное наименование организации:	
Юридический адрес организации:	
ФИО руководителя, должность:	
Выбранная схема подключения	
Для схемы 1 и схемы 2. Количество участвующих во взаимодействии программных или программно-аппаратных продуктов ViPNet со стороны подключаемой организации (указать количество: ViPNet Coordinator, ViPNet Client for Linux, ViPNet Client for Windows и другие):	
Контактные данные ответственного за подключение (ФИО, телефон, адрес электронной почты):	

и прошу организовать подключение **[наименование организации]** к ресурсам информационной системе «Бухгалтерия, кадровый учет и документооборот».

Выполнение требований по защите информации, указанных в Регламенте, подтверждаю. Мероприятия по оценке эффективности принимаемых мер по обеспечению безопасности персональных данных выполнены.

[должность руководителя организации]

[И.О. Фамилия]