САМОРЕГУЛИРУЕМАЯ ОРГАНИЗАЦИЯ АУДИТОРОВ
АССОЦИАЦИЯ «СОДРУЖЕСТВО»
член Международной Федерации Бухгалтеров (IFAC)
(ОГРН 1097799010870, ИНН 7729440813, КПП 772901001)
119192, г. Москва, Мичуринский проспект, дом 21, корпус 4.
т: +7 (495) 734-22-22, ф: +7 (495) 734-04-22, www.auditor-sro.org, info@auditor-sro.org

ПРОТОКОЛ № 9
заседания Комитета по ИТ и кибербезопасности Саморегулируемой организации аудиторов Ассоциации «Содружество»

г. Москва **20 декабря 2024 года**

Форма заседания: Очная

Члены Комитета, принявшие участие в заседании: Стрий Л.В., Богров Е.Г., Орлов А.В., Бареев Т.Ф., Комиссарова О.В., Брюханов М.Ю., Кушнарев А.С, Зубков А.С., Винокуров Д.М., Полавская Н.В.

Итого в заседании Комитета по ИТ и кибербезопасности (далее - Комитет) участвует 9 из 10 человек, что составляет 90% голосов.
Кворум для принятия решений имеется.
Председатель заседания – Стрий Л.В.

Повестка дня:
Утвердить ответ на Обращение №564МТ201124 от 20 ноября 2024 г.

Решение, поставленное на голосование:
Утвердить ответ на Обращение №564МТ201124 от 20 ноября 2024 г. с учетом поступивших предложений.

Результаты голосования по вопросу:
ЗА – 9 чел.
ПРОТИВ – 0 чел.
ВОЗДЕРЖАЛСЯ – 1 чел.
Решение принято

Подсчет голосов производила Председатель Комитета Л.В. Стрий.

К настоящему протоколу прилагаются:
1. Ответ (Приложение 1)

Председатель Комитета **Л.В. Стрий**

Приложение 1

Комитет по ИТ и кибербезопасности СРО ААС
Ответ на Обращение №564МТ201124 от 20 ноября 2024 г.

При использовании сервера для обработки информации, связанной с аудиторской деятельностью, необходимо соблюдать требования федеральных законов и подзаконных актов, регулирующих защиту персональных данных и конфиденциальной информации (аудиторской тайны):

- Указ Президента РФ от 06.03.1997 N 188 "Об утверждении Перечня сведений конфиденциального характера";
- Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Федеральный закон от 30.12.2008 N 307-ФЗ (ред. от 08.08.2024) "Об аудиторской деятельности";
- Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных";
- Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Положение Банка России от 17.10.2022 N 808-П "О требованиях к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций, обязательных для лиц, оказывающих профессиональные услуги на финансовом рынке, к обеспечению бюро кредитных историй защиты информации, указанной в статье 4 Федерального закона "О кредитных историях", при ее обработке, хранении и передаче сертифицированными средствами защиты, а также к сохранности информации, полученной в процессе деятельности кредитного рейтингового агентства";
- Приказ ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";
- Приказ ФСБ России от 10.07.2014 N 378 "Об утверждении Состава 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".

На практике это означает, что аудиторская организация обязана обеспечить:

- Защиту данных при ее обработке и передаче по открытым каналам связи;
- Ограничение доступа к аудиторской тайне;
- Физическую и техническую защиту серверного оборудования.

Требования к дата-центру.

Дата-центр, в котором планируется размещение серверов, должен соответствовать следующим требованиям:

- Наличие лицензий, предусмотренных ФЗ №126-ФЗ «О связи», если предоставляются услуги связи;
- наличие аттестатов соответствия уровню защищенности персональных данных определенных для категории обрабатываемых персональных данных субъектов (физических лиц), вида обработки по форме отношений между субъектами и организацией, количества субъектов, а также типов угроз актуальных для информационной системы в составе арендуемых облачных или выделенных серверов, если в информационной системе ведется обработка персональных данных, аудиторской тайны или иной конфиденциальной информации;
- Наличие лицензии на деятельность по технической защите конфиденциальной информации (ФСТЭК) у лица, выполняющего работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации;
- наличие лицензии ФСБ на криптографию у лица, осуществляющего создание защищенной с помощью средств шифрования информационной системы;
- сертификатов соответствия требованиям ФСТЭК и ФСБ, если сервер обрабатывает персональные данные, аудиторскую тайну или иную конфиденциальную информацию;
- Соответствие стандартам отказоустойчивости, например, Tier III или Tier IV (не обязательно, но рекомендуется);
- Наличие систем физической защиты серверных помещений (контроль доступа, видеонаблюдение, системы пожаротушения).

Кроме того, важно учитывать, что дата-центр должен предоставлять гарантию конфиденциальности данных и отвечать за соблюдение законодательства в части защиты информации.

Дополнительные меры защиты.

Аудиторской организации рекомендуется:

1. Заключить с дата-центром договор, в котором будут прописаны обязательства по защите данных, включая:
   - Обеспечение резервного копирования;
   - Ограничение доступа третьих лиц к данным и оборудованию;
   - Гарантии конфиденциальности и ответственности за утечку данных.
2. Использовать Применять сертифицированные средства криптографической защиты информации при организации каналов до дата-центра, такие как (VPN и шифрование каналов связи).
3. Регулярно проводить аудит инфраструктуры информационной системы и проверять соблюдение дата-центром установленных требований.

Таким образом, размещение сервера аудиторской организации в дата-центре возможно, как в случае аренды площадей для собственного оборудования, так и в случае аренды серверов. В обоих вариантах необходимо учитывать требования российского законодательства к защите персональных данных, аудиторской тайны и конфиденциальной информации.