Типовые требования
по подключению пользователей к информационным системам, размещенным в инфраструктуре Республиканского центра обработки данных

Чебоксары, 2022 г.

1. Общие положения

Настоящие требования разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», и определяют требования по подключению пользователей к информационным системам, размещенным в инфраструктуре Республиканского центра обработки данных (далее – РЦОД) в части информационной безопасности.

2. **Термины, используемые в настоящем Регламенте, их определения**

2.1. Республиканский центр обработки данных (далее - РЦОД) представляет собой технологически и территориально обособленные серверные комплексы, включая рабочие станции, предназначенные для обслуживающего персонала РЦОД, и технологическое оборудование, обеспечивающее функционирование серверов (стойки, источники бесперебойного питания, коммутационное оборудование и кабельные системы).

2.2. Органом исполнительной власти Чувашской Республики, уполномоченным на обеспечение функционирования и модернизацию Республиканского центра обработки данных, определено Министерство информационной политики и массовых коммуникаций Чувашской Республики (далее - Уполномоченный орган).

2.3. Оператором РЦОД является бюджетное учреждение Чувашской Республики «Центр информационных технологий» Министерства информационной политики и массовых коммуникаций Чувашкой Республики (далее - Оператор).

2.4. Пользователи РЦОД - органы исполнительной власти Чувашской Республики и иные государственные органы Чувашской Республики, органы местного самоуправления, юридические лица, зарегистрированные на территории Чувашской Республики, размещающие в РЦОД серверы, информационные системы и информационные ресурсы, не содержащие сведения, составляющие государственную тайну (далее также соответственно - серверы, информационные системы и информационные ресурсы) (далее - Пользователь).

2.5. Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (далее - ИС).

2.6. Оператор информационной системы (далее – Оператор ИС) – владелец информационной системы, разместивший ИС в информационной инфраструктуре РЦОД.

3. **Типовые требования по подключению пользователей к информационным системам, размещенным в инфраструктуре Республиканского центра обработки данных**

3.1. В целях организации защищенного информационного взаимодействия с ИС, размещенной в РЦОД, оператор ИС обеспечивает реализацию организационных и технических мероприятий по обеспечению безопасности персональных данных и иной информации ограниченного доступа (далее - защищаемая информация) при её обработке на АРМ пользователей.

3.2. Организационные мероприятия по обеспечению защиты информации должны включать:

- назначение должностных лиц, ответственных за обеспечение информационного взаимодействия с ИС (пользователей ИС);
- организацию режима обеспечения безопасности помещений, в которых размещены технические и программные средства, участвующие в обработке защищаемой информации, а также помещений, где используются или хранятся средства защиты информации и СКЗИ, носители защищаемой информации, в том числе носители персональных данных, носители ключевой, аутентифицирующей и парольной информации (далее - защищаемое помещение);
- обеспечение сохранности носителей персональных данных и иной защищаемой информации;
- принятие мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами;
- принятие мер, направленных на обеспечение защиты информации и безопасности персональных данных при их обработке в информационных системах.

3.3. Обеспечиваемый режим безопасности защищаемых помещений должен исключать возможность неконтролируемого проникновения или пребывания в данных помещениях, лиц, не имеющих права доступа в защищаемые помещения. Организация обеспечения режима безопасности защищаемых помещений достигается путем:

- оснащения защищаемых помещений входными дверьми с замками, обеспечения постоянного закрытия дверей защищаемых помещений на замок и их открытия только для санкционированного прохода, а также опечатывания защищаемых помещений по окончании рабочего дня или оборудование защищаемых помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии защищаемых помещений;
- утверждения правил доступа в защищаемые помещения в рабочее и нерабочее время, а также в нештатных ситуациях;
- утверждения перечня лиц, имеющих право доступа в защищаемые помещения.

В целях организации режима обеспечения безопасности помещений рекомендуется разработать и утвердить соответствующий документ, определяющий меры по обеспечению безопасности защищаемых помещений.

3.4. В целях принятия мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, необходимо разработать, утвердить и поддерживать в актуальном состоянии документы, определяющие:

- ответственного за организацию обработки персональных данных;
- регламент (инструкцию) ответственного за организацию обработки персональных данных;
- политику в отношении обработки персональных данных;

- формы документов, необходимых в целях выполнения требований законодательства Российской Федерации в области обработки персональных данных;
- перечень лиц, доступ которых к персональным данным и иной защищаемой информации, обрабатываемой в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.

3.5. В целях принятия мер, направленных на обеспечение зашиты информации и безопасности персональных данных при их обработке в информационных системах, необходимо разработать, утвердить и поддерживать в актуальном состоянии документы, определяющие:

- ответственного за обеспечение безопасности защищаемой информации при её обработке в информационных системах;
- регламент (инструкцию) ответственного за обеспечение безопасности защищаемой информации при её обработке в информационных системах;
- перечень мер, направленных на выполнение требований законодательства Российской Федерации в области защиты персональных данных с использованием средств криптографической защиты информации.

3.6. Технические меры защиты информации должны реализовываться посредством применения сертифицированных средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности.

3.7. Технические мероприятия по обеспечению защиты информации должны включать:

- установку и настройку средств антивирусной защиты информации;
- установку и настройку СКЗИ;
- установку и настройку средств защиты информации от несанкционированного доступа.
- установку и настройку средств межсетевого экранирования;
- опечатывание корпуса АРМ номерными пломбами с возможностью контроля вскрытия с периодическим визуальным контролем фактов нарушения пломб;
- установка пароля администратора на доступ к базовой системы ввода-вывода (BIOS/UEFI). Организовать контроль доступа пользователей к процессу загрузки операционной системы посредством запрета альтернативной загрузки операционной системы (в том числе – с внешних носителей), отключить возможность выбора источников во время загрузки в настройках базовой системе ввода-вывода (BIOS/UEFI).

3.8. На АРМ пользователей, должны быть установлены и настроены сертифицированные на соответствие требованиям по безопасности информации средства защиты информации и СКЗИ.

3.9. Перечень рекомендуемых вариантов подключения пользователей к информационным системам, размещенным в инфраструктуре Республиканского центра обработки данных, приведен в Приложении № 1.

3.10. Перечень рекомендуемых средств защиты информации приведен в Приложении № 2.

3.11. По результатам выполнения выше указанных мер Оператору ИС необходимо предоставить Оператору РЦОД Акт о готовности подключения пользователей к информационной системе, размещенной в РЦОД. Типовая форма представлена в Приложении № 3.

Приложение № 1

Перечень рекомендуемых вариантов подключения пользователей к информационным системам, размещенным в инфраструктуре Республиканского центра обработки данных

Вариант подключения № 1. Подключение отдельного АРМ.

Подключение отдельного АРМ пользователя к ИС, размещенным в РЦОД, осуществляется с помощью установленного средства криптографической защиты информации «Континент TLS-клиент. Версия 2», сертифицированного ФСБ России по классу КС1/КС2.

На АРМ пользователя должны быть установлены и настроены программные средства:

1. лицензионная операционная система: ОС Windows;
2. средство криптографической защиты информации: «Континент TLS-клиент. Версия 2»;
3. сертифицированное средство антивирусной защиты на соответствие требованиям по безопасности информации;
4. средство защиты информации от несанкционированного доступа с модулем межсетевого экранирования.

Вариант подключения № 2. Подключение отдельного АРМ.

Подключение отдельного АРМ пользователя к ИС, размещенным в РЦОД, осуществляется с помощью установленного программного комплекса ViPNet Client 4 (версия 4.5), сертифицированного ФСБ России.

На АРМ пользователя должны быть установлены и настроены программные средства:

1. лицензионная операционная система: ОС Windows, Linux;
2. средство криптографической защиты информации: программный комплекс ViPNet Client 4 (версия 4.5);
3. сертифицированное средство антивирусной защиты на соответствие требованиям по безопасности информации;
4. средство защиты информации от несанкционированного доступа.

Вариант подключения № 3. Подключение нескольких АРМ, размещенных в пределах единой контролируемой зоны.

Подключение АРМ пользователей к ИС, размещенным в РЦОД, осуществляется с помощью установленного СКЗИ программно-аппаратного комплекса «ViPNet Coordinator HW 4», сертифицированного ФСБ России.

На АРМ пользователя должны быть установлены и настроены программные средства:

1. лицензионная операционная система: ОС Windows / ОС Linux;
2. сертифицированное средство антивирусной защиты на соответствие требованиям по безопасности информации;
3. средство защиты информации от несанкционированного доступа.

Вариант подключения № 4. Подключение нескольких АРМ, размещенных в пределах единой контролируемой зоны.

Подключение АРМ пользователей к ИС, размещенным в РЦОД, осуществляется с помощью установленного СКЗИ «МагПро КриптоПакет», сертифицированного ФСБ России. Необходимо установить сертифицированное средство межсетевого экранирования на границе сети.

На АРМ пользователя должны быть установлены и настроены программные средства:

1. лицензионная операционная система: ОС Windows / ОС Linux;
2. сертифицированное средство антивирусной защиты на соответствие требованиям по безопасности информации;
3. средство защиты информации от несанкционированного доступа.

Приложение № 2

Перечень рекомендуемых средств защиты информации.

Средства антивирусной защиты информации для ОС Windows:

1. программное изделие «Kaspersky Endpoint Security для Windows» (версия 11.6.0.394);
2. программное обеспечение «Dr. Web Enterprise Security Suite».

Средства антивирусной защиты информации для ОС Linux:

1. программное изделие «Kaspersky Endpoint Security 11 для Linux»;
2. программное обеспечение «Dr. Web Enterprise Security Suite».

Средство защиты информации от несанкционированного доступа ОС Windows:

1. средство защиты информации Secret Net Studio 8;
2. система защиты информации от несанкционированного доступа «Dallas Lock 8.0-К.

Средство защиты информации от несанкционированного доступа для ОС Linux:

1. средство защиты информации Secret Net LSP;
2. система защиты информации от несанкционированного доступа «Dallas Lock Linux.

Приложение № 3

УТВЕРЖДАЮ

«___» _____ 20__ г. Руководитель _____

Акт № _____
о готовности подключения пользователей к информационной системе _____, размещенной в РЦОД

Комиссия _____,
(наименование организации)
в составе:

Председатель комиссии: - _____
Члены комиссии: - _____
- _____

составила настоящий акт о том, что проведена проверка выполнения требований в соответствии с Типовыми требованиями по подключению пользователей к информационным системам, размещенным в инфраструктуре Республиканского центра обработки данных, в том числе проверка:

1. Наличия разработанных и принятых организационных документов по вопросам информационной безопасности и обеспечения защиты персональных данных в соответствии с федеральными законами «Об информации, информационных технологиях и о защите информации», «О персональных данных» и принимаемыми в соответствии с ними нормативными правовыми актами, методическими и руководящими документами в области защиты информации.

2. Организации режима обеспечения безопасности помещений, в которых размещены автоматизированные рабочие места, предназначенные для обеспечения информационного взаимодействия с информационной системой _____, технические и программные средства, участвующие в обработке информации при взаимодействии с ИС, а также помещений, где используются или хранятся средства защиты информации, средства криптографической защиты информации, носители защищаемой информации, персональных данных, ключевой, аутентифицирующей и парольной информации.

3. Подготовленности лиц, ответственных за обеспечение информационного взаимодействия с ИС, знания ими основных положений законодательства в области защиты информации и обеспечения безопасности персональных данных, требований 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, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 года № 152.

4. Готовности АРМ пользователей ИС, технических и программных средств, участвующих в обработке информации при взаимодействии с ИС, а также проверка настроек

и корректности функционирования следующих средств защиты информации и средств криптографической защиты информации, установленных на АРМ пользователя ИС:

средства криптографической защиты информации:

_____,
наименование СКЗИ (например, СКЗИ «Континент TLS VPN Клиент» версии 2)

средства антивирусной защиты информации:

_____,
наименование средства антивирусной зашиты (например, Kaspersky Endpoint Security 11 для Windows)

средства защиты информации от несанкционированного доступа:

_____,
наименование средства зашиты информации (например, Secret Net Studio)

средства межсетевого экранирования:

_____,
наименование средства зашиты информации

Заключение комиссии:

принятые организационные и технические меры по обеспечению информационной безопасности

_____
(наименование организации)

соответствуют Типовым требованиям по подключению пользователей к информационным системам, размещенным в инфраструктуре Республиканского центра обработки данных, автоматизированные рабочие места для подключения и обработки информации в информационной системе _____ готовы.

Представители комиссии:

_____	_____
(подпись члена комиссии)	(Ф.И.О. члена комиссии)
_____	_____
(подпись члена комиссии)	(Ф.И.О. члена комиссии)
_____	_____
(подпись члена комиссии)	(Ф.И.О. члена комиссии)