

Министерство финансов Чувашской Республики

УТВЕРЖДАЮ:

Заместитель министра финансов
Чувашской Республики


И.Н. Смирнов

«23» декабря 2020 г.

Регламент организации информационного взаимодействия внешних пользователей и информационных систем сторонних организаций с информационной системой «Минфин» Министерства финансов Чувашской Республики

Содержание

СОДЕРЖАНИЕ.....	2
АННОТАЦИЯ	3
ПРИНЯТЫЕ СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ.....	4
ВВЕДЕНИЕ.....	5
1. ОБЩИЕ ПОЛОЖЕНИЯ	6
2. УДАЛЕННЫЙ ДОСТУП ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ.....	7
2.1 ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ПОДКЛЮЧЕНИЯ ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ	7
2.2 ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ И ЗАЩИЩЕННОГО ВЗАИМОДЕЙСТВИЯ	9
2.3 ПОРЯДОК ПОДКЛЮЧЕНИЯ АРМ ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ ВОЗМОЖНОСТИ ВКЛЮЧЕНИЯ ИХ В ЗАЩИЩЕННУЮ ИНФОРМАЦИОННУЮ СИСТЕМУ ИС «МИНФИН»	10
3. ВЗАИМОДЕЙСТВИЕ С ИНФОРМАЦИОННЫМИ СИСТЕМАМИ СТОРОННИХ ОРГАНИЗАЦИЙ (ВНЕШНИМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ)	12
3.1 ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ	12
3.2 ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ И ЗАЩИЩЕННОГО ВЗАИМОДЕЙСТВИЯ	12
3.3 ПОРЯДОК ОРГАНИЗАЦИИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ.....	13
ПРИЛОЖЕНИЕ №1.....	14
ПРИЛОЖЕНИЕ №2.....	15
ПРИЛОЖЕНИЕ №3.....	16

Аннотация

Данный документ регламентирует процесс организации информационного взаимодействия внешних пользователей и информационных систем сторонних организаций с информационной системой «Минфин» (далее – ИС «Минфин»).

Принятые сокращения и определения

АРМ	- автоматизированные рабочие места
СЗИ от НСД	- средства защиты информации от несанкционированного доступа
ПКИ	- парольно-ключевая информация
Внешние пользователи	- внешние пользователи ИС «Минфин»
Оператор	- Министерство финансов Чувашской Республики
Регламент	- Регламент взаимодействия внешних пользователей и информационных систем сторонних организаций с информационной системой «Минфин»
РЦОД	- Республиканский центр обработки данных, уполномоченным органом исполнительной власти Чувашской Республики по обеспечению функционирования и модернизации которого является Министерство цифрового развития, информационной политики и массовых коммуникаций Чувашской Республики

Введение

Регламент определяет типы информационного взаимодействия, варианты организаций информационного взаимодействия, общий состав, содержание и порядок выполнения работ при организации защищенного информационного взаимодействия с ИС «Минфин».

Регламент разработан в соответствии с Приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Основной целью Регламента является определение типов информационного взаимодействия и обязательного плана работ при организации информационного взаимодействия, необходимого для выполнения требований по обеспечению информационной безопасности в ИС «Минфин».

1. Общие положения

В соответствии с Приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и другими нормативными актами, применяемыми для ИС «Минфин» информационное взаимодействие с ИС «Минфин» должно осуществляться по защищенному каналу связи. На средствах вычислительной техники, осуществляющих информационное взаимодействие, должны быть установлены и корректно настроены средства защиты информации.

Для ИС «Минфин» определены следующие типы информационного взаимодействия:

- удаленный доступ внешних пользователей;
- взаимодействие с информационными системами сторонних организаций (внешние информационные системы).

В целях реализации технических требований разработаны типовые схемы информационного взаимодействия внешних пользователей, информационных систем сторонних организаций, а также регламентирован способ организации информационного взаимодействия с ИС «Минфин».

2. Удаленный доступ внешних пользователей

Настоящим Регламентом определяется схема подключения Внешних пользователей к следующим информационным ресурсам ИС «Минфин»:

- районная база данных программного комплекса «Бюджет-СМАРТ Про»;
- республиканская база данных программного комплекса «Бюджет-СМАРТ Про»;
- база данных программного комплекса «Проект-СМАРТ Про»;
- районная база данных программного комплекса «Хранилище-КС»;
- республиканская база данных программного комплекса «Хранилище-КС»;
- база данных программного комплекса «Свод-СМАРТ» (поэтапное подключение).

2.1 Требования к организации подключения внешних пользователей

Организация подключения Внешних пользователей должна осуществляться в соответствии с:

- ✓ требованиями нормативно-правовых актов Российской Федерации в сфере защиты информации;
- ✓ требованиями нормативно-технических и методических документов уполномоченных органов исполнительной власти Российской Федерации в сфере обеспечения безопасности информации (ФСТЭК России, ФСБ России);
- ✓ требованиями настоящего Регламента.

До начала выполнения работ по подключению Внешних пользователей к ИС «Минфин» схема защищенного взаимодействия должна быть согласована с Оператором.

2.1.1 Схема защищенного взаимодействия №1 (Схема подключения №1)

Для обработки защищаемой информации должен использоваться АРМ, на котором установлены сертифицированные ФСТЭК России по требованиям безопасности информации:

- ✓ средство защиты от несанкционированного доступа;
- ✓ средство межсетевого экранирования;
- ✓ средство антивирусной защиты.

Функции средства криптографической защиты информации должен выполнять программный комплекс ViPNet Client, имеющий действующий сертификат соответствия ФСБ России, подключаемый к ViPNet-сети № 2921 Министерства цифрового развития, информационной политики и массовых коммуникаций Чувашской Республики.

2.1.2 Схема защищенного взаимодействия №2 (Схема подключения №2)

Для обработки защищаемой информации должны использоваться АРМ, на которых установлены сертифицированные ФСТЭК России по требованиям безопасности информации:

- ✓ средство защиты от несанкционированного доступа;
- ✓ средство антивирусной защиты.

Функции средства криптографической защиты информации и средства межсетевого экранирования должен выполнять программно-аппаратный комплекс ViPNet Coordinator HW, имеющий действующие сертификаты соответствия ФСБ России и ФСТЭК России, подключаемый к ViPNet-сети № 2921 Министерства цифрового развития, информационной политики и массовых коммуникаций Чувашской Республики.

2.1.3. Обобщенная схема информационного взаимодействия ИС «Минфин» с АРМ внешних пользователей

Обобщенная схема информационного взаимодействия ИС «Минфин» с АРМ внешних пользователей представлена на рисунке 1, где:

- ✓ 1 вариант отражает схему подключения №1;
- ✓ 2 вариант отражают схему подключения №2.

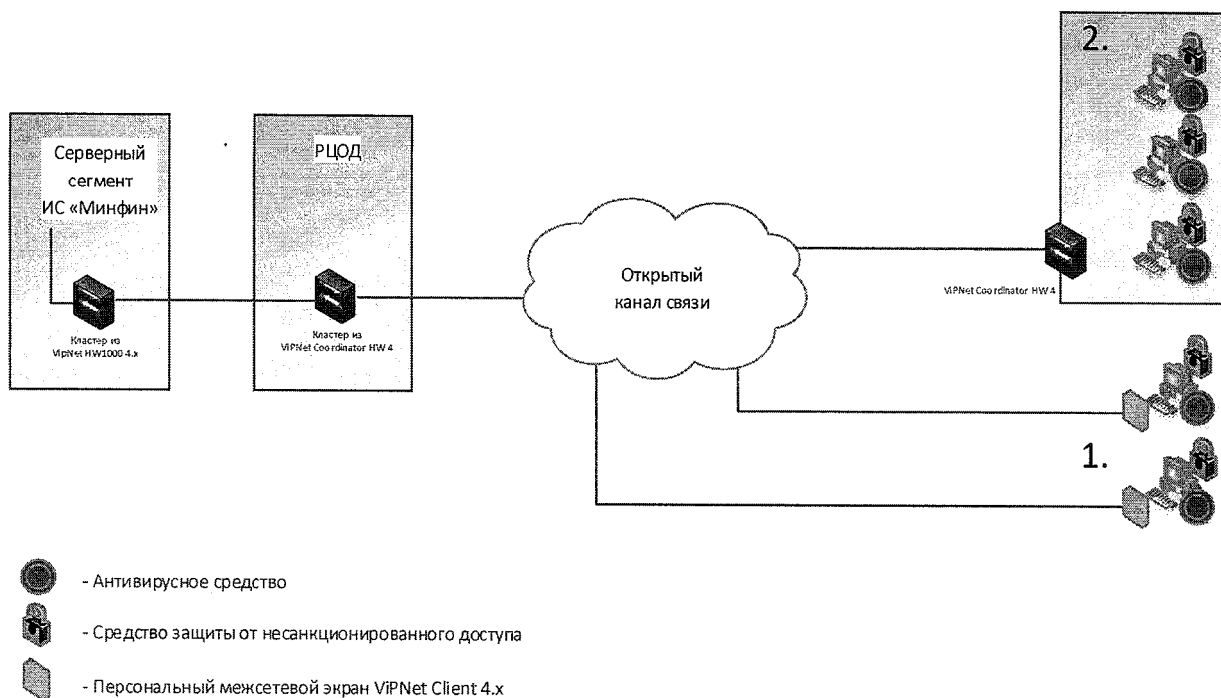


Рисунок 1

2.2 Требования к реализации системы защиты информации и защищенного взаимодействия

Для возможности реализации защищенного взаимодействия АРМ внешних пользователей с ИС «Минфин», а так же обеспечения надлежащего уровня защиты информации на АРМ внешних пользователей должны выполняться следующие требования:

- ✓ техническое обеспечение безопасности информации согласно настоящему документу, включающее в себя:
 - обеспечение безопасного межсетевого взаимодействия;
 - обеспечение защиты конфиденциальности и целостности передаваемой по каналам связи информации;
 - обеспечение комплексной защиты информации, обрабатываемой на АРМ внешних пользователей;
- ✓ выполнение обязательных организационных мероприятий, необходимых при эксплуатации средств защиты информации, в том числе средств криптографической защиты, в соответствии с требованиями нормативных правовых документов, включающие в себя:
 - проведение инструктажей пользователей АРМ;
 - разработку документации по защите информации (минимальный типовой комплект представлен в приложении №1);

○ выполнение организационных требований нормативно-правовых актов в сфере защиты информации.

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

2.3 Порядок подключения АРМ внешних пользователей для возможности включения их в защищенную информационную систему ИС «Минфин»

Для АРМ Внешних пользователей реализация обязательных требований достигается путем применения порядка следующих технических и организационных мер:

- ✓ согласование схемы подключения с Оператором и получение ПКИ (в сроки, установленные Оператором);
- ✓ приобретение средств защиты информации и прав на их использование;
- ✓ установка и настройка средств защиты информации в соответствии с выбранной схемой подключения;
- ✓ оформление акта установки с указанием перечня установленных средств защиты информации;
- ✓ проведение инструктажа пользователям подключаемых АРМ;
- ✓ корректировка организационных и технических мер, применяемых на рабочих местах Внешних пользователей согласно актуальным требованиям по обеспечению безопасности информации, в том числе разработка и/или доработка организационно-распорядительной документации и технических паспортов;
- ✓ проведение комиссией Внешних пользователей, назначенной приказом (примерная форма приказа представлена в приложении №2), оценку полноты выполнения мер, необходимых к применению согласно нормативным правовым актам по защите информации;

- ✓ проверка Внешними пользователями возможности корректного функционирования подключаемых АРМ для возможности выполнения должностных обязанностей сотрудников;
- ✓ оформление акта оценки полноты выполнения мер по защите информации (типовая форма представлена в приложении №3);
- ✓ опытная эксплуатация АРМ Внешних пользователей;
- ✓ проведение контроля (периодического или инициированного ответственным за обеспечение безопасности информации) эффективности системы защиты информации в информационной среде Внешних пользователей.

3. Взаимодействие с информационными системами сторонних организаций (внешними информационными системами)

Настоящим Регламентом определяется схема информационного взаимодействия ИС «Минфин» с информационными системами сторонних организаций (внешними информационными системами).

В информационном взаимодействии с внешними информационными системами участвуют следующие программные комплексы ИС «Минфин»:

- ✓ ПК «Свод-СМАРТ»;
- ✓ ПК «Бюджет-СМАРТ Про».

3.1 Требования к организации информационного взаимодействия

Организация информационного взаимодействия должна осуществляться в соответствии с:

- ✓ требованиями нормативно-правовых актов Российской Федерации в сфере защиты информации;
- ✓ требованиями нормативно-технических и методических документов уполномоченных органов исполнительной власти Российской Федерации в сфере обеспечения безопасности информации (ФСТЭК России, ФСБ России);
- ✓ требованиями настоящего Регламента.

Для реализации информационного взаимодействия внешних информационных систем с ИС «Минфин» между сетью Оператора, внешними информационными системами и РЦОД должен быть организован межсетевой защищенный обмен.

3.2 Требования к реализации системы защиты информации и защищенного взаимодействия

Реализация информационного взаимодействия информационных систем сторонних организаций (внешних информационных систем) с ИС «Минфин» возможна только в случае выполнения оператором внешней

информационной системы или лицом, уполномоченным на основании заключенного договора обеспечивать защиту информации, требований по обеспечению защиты информации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации, а также требований настоящего Регламента.

Не допускается взаимодействие информационных систем сторонних организаций (внешних информационных систем) с ИС «Минфин» при неполной или некорректной реализации требований по обеспечению защиты информации.

3.3 Порядок организации информационного взаимодействия

Порядок организации информационного взаимодействия информационных систем сторонних организаций (внешних информационных систем) с ИС «Минфин»:

- ✓ предоставление оператором внешней информационной системы документа, подтверждающего выполнение требований по обеспечению защиты информации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации (Аттестат соответствия, контроль эффективности принятых мер);
- ✓ оформление соглашения об информационном взаимодействии;
- ✓ определение узлов взаимодействия и их конфигурирование.

Типовой комплект документации, необходимой к разработке для выполнения требований по обеспечению безопасности информации при подключении к защищенной сети с целью осуществления информационного взаимодействия с ИС «Минфин»

- ✓ Приказ об ответственном за обеспечение безопасности информации при подключении к ИС «Минфин»;
- ✓ Приказ об утверждении перечня сотрудников, осуществляющих обработку информации при подключении к ИС «Минфин»;
- ✓ Инструкция ответственного за обеспечение безопасности информации при подключении к ИС «Минфин»;
- ✓ Инструкция пользователей, осуществляющих обработку информации при подключении к ИС «Минфин»;
- ✓ Приказ об обеспечении безопасности помещений, в которых осуществляется обработка информации при подключении к ИС «Минфин»;
- ✓ Приказ об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты (назначение ответственного пользователя криптосредств; утверждение инструкции ответственного пользователя криптосредств; утверждение перечня сотрудников, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности информации; утверждение инструкции пользователей криптосредств; утверждение формы журнала поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов; утверждение формы лицевого счета пользователя криптосредств).

Примерная форма Приказа «О комиссии по оценке полноты выполнения мер по защите информации при взаимодействии с информационной системой «Минфин»

ПРИКАЗ

В целях выполнения требований по обеспечению информационной безопасности в соответствии с нормативными правовыми актами Российской Федерации в области защиты информации и методическими документами уполномоченных органов исполнительной власти Российской Федерации в сфере обеспечения безопасности информации п р и к а з ы в а ю:

1. Создать комиссию по оценке полноты выполнения мер по защите информации при информационном взаимодействии с информационной системой «Минфин», (далее – Комиссия) в составе:

Председатель комиссии:

Члены комиссии:

2. Комиссии обеспечить проведение работ по оценке полноты выполнения мер по защите информации, необходимых к применению согласно нормативным правовым актам по защите информации, Регламента организации информационного взаимодействия внешних пользователей и информационных систем сторонних организаций с информационной системой «Минфин» Министерства финансов Чувашской Республики.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Приложение №3

УТВЕРЖДАЮ

Руководитель _____

« ____ » _____ 20__ г.

**Акт оценки полноты выполненных мер по защите информации при
информационном взаимодействии с информационной системой
«Минфин»**

Комиссия _____,
(наименование организации)

в составе:

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

составила настоящий акт о том, что проведена проверка выполнения требований Регламента организации информационного взаимодействия внешних пользователей и информационных систем сторонних организаций с информационной системой «Минфин» (далее – ИС «Минфин») Министерства финансов Чувашской Республики от _____ года (далее – Регламент) участником информационного взаимодействия

(наименование организации)

при подключении к ИС «Минфин», в том числе:

1. Наличие разработанных и принятых организационных документов по вопросам информационной безопасности и обеспечения защиты персональных данных в соответствии с нормативными правовыми актами Российской Федерации в сфере защиты информации, нормативно-техническими и методическими документами уполномоченных органов исполнительной власти Российской Федерации в сфере обеспечения безопасности информации (ФСТЭК России, ФСБ России).

2. Организации режима обеспечения безопасности помещений, в которых размещены автоматизированные рабочие места (далее – АРМ), технические и программные средства, предназначенные для обеспечения информационного взаимодействия с ИС «Минфин», а также помещений, где используются или хранятся средства защиты информации, средства

криптографической защиты информации, носители защищаемой информации, ключевой, аутентифицирующей и парольной информации.

3. Подготовленности лиц, ответственных за обеспечение информационного взаимодействия с ИС «Минфин», 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, технических и программных средств, участвующих в обработке информации при взаимодействии с ИС «Минфин», а также проверка настроек и корректности функционирования средств защиты информации и средств криптографической защиты информации.

Заключение комиссии:

принятые организационные и технические меры по обеспечению информационной безопасности _____

(наименование организации)

соответствуют требованиям Регламента, АРМ для подключения и информационного взаимодействия с ИС Минфин готовы.

Председатель комиссии:

(подпись)

(Ф.И.О.)

Члены комиссии:

(подпись члена комиссии)

(Ф.И.О. члена комиссии)

(подпись члена комиссии)

(Ф.И.О. члена комиссии)