МИНИСТЕРСТВО ФИНАНСОВ ЧУВАШСКОЙ РЕСПУБЛИКИ

УТВЕРЖДАЮ:

Заместитель министра финансов
Чувашской Республики

_____ **Г.В. Павлова**

«04» АПРЕЛЯ 2023 г.

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

г. Чебоксары
2023

Содержание

СОДЕРЖАНИЕ 2
ПРИНЯТЫЕ СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ 3
ВВЕДЕНИЕ 4
1. ОБЩИЕ ПОЛОЖЕНИЯ 5
2. УДАЛЕННЫЙ ДОСТУП ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ 6
2.1 ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ПОДКЛЮЧЕНИЯ ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ 6
2.2 ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ И ЗАЩИЩЕННОГО ВЗАИМОДЕЙСТВИЯ 8
2.3 ПОРЯДОК ПОДКЛЮЧЕНИЯ АРМ ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ ВОЗМОЖНОСТИ ВКЛЮЧЕНИЯ ИХ В ЗАЩИЩЕННУЮ ИНФОРМАЦИОННУЮ СИСТЕМУ ИС «МИНФИН» 9
3. ВЗАИМОДЕЙСТВИЕ С ИНФОРМАЦИОННЫМИ СИСТЕМАМИ СТОРОННИХ ОРГАНИЗАЦИЙ (ВНЕШНИМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ) 11
3.1 ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ 11
3.2 ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ И ЗАЩИЩЕННОГО ВЗАИМОДЕЙСТВИЯ 11
3.3 ПОРЯДОК ОРГАНИЗАЦИИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ 12
ПРИЛОЖЕНИЕ №1 13
ПРИЛОЖЕНИЕ №2 14
ПРИЛОЖЕНИЕ №3 15

Принятые сокращения и определения

АРМ	Автоматизированное рабочее место
Внешние пользователи	Внешние пользователи ИС «Минфин»
ИС «Минфин»	Информационная система «Минфин» Министерства финансов Чувашской Республики
Оператор	Министерство финансов Чувашской Республики
СЗИ	Средство защиты информации
СЗИ от НСД	Средство защиты информации от несанкционированного доступа
СКЗИ	Средство криптографической защиты информации
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
УЦ АУ «ЦИТ» Минцифры Чувашии	Удостоверяющий центр Автономного учреждения «Центр информационных технологий» Министерства цифрового развития, информационной политики и массовых коммуникация Чувашской Республики (http://uc-cit.cap.ru/)

Введение

Настоящий 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», приказом Федеральной службы по техническому и экспортному контролю от России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказом ФСБ России от 10 июля 2014 года № 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».

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»:

– база данных программного комплекса «Бюджет-СМАРТ Про»;
– база данных программного комплекса «Проект-СМАРТ Про»;
– база данных программного комплекса «Хранилище-КС»;
– база данных программного комплекса «Свод-СМАРТ».

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 антивирусной защиты.

Функции средства криптографической защиты информации должен выполнять программный комплекс ViPNet Client 4 (ViPNet Client 4U for Linux), имеющий действующий сертификат соответствия ФСБ России, подключаемый к ViPNet-сети №2921 АУ «ЦИТ» Минцифры Чувашии.

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 АУ «ЦИТ» Минцифры Чувашии.

2.1.3 Схема защищенного взаимодействия №3 (Схема подключения №3)

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;

Для организации защищенного информационного взаимодействия с использованием средства криптографической защиты информации необходимо использовать:

- ✓ сертификат ключа проверки электронной подписи, изготовленный УЦ АУ «ЦИТ» Минцифры Чувашии, который не является квалифицированным сертификатом и применяется только для установки защищенного канала связи;
- ✓ СКЗИ «КриптоПро CSP» версии 4.0 и выше и/или СКЗИ «Континент TLS Клиент».

СКЗИ «Континент TLS Клиент» рекомендуется устанавливать для организации защищенного информационного взаимодействия с ИС Минфин в случаях:

- ✓ применения на АРМ специализированного прикладного программного обеспечения для работы в ИС Минфин;
- ✓ применения СКЗИ «Континент TLS Клиент» без стороннего криптопровайдера (СКЗИ «КриптоПро CSP» версии 4.0 и выше). В данном варианте СКЗИ «Континент VPN Клиент» используется с криптопровайдером «Код Безопасности CSP», входящим в состав СКЗИ «Континент TLS Клиент».

** - СЗИ от НСД не устанавливается в случае использования операционной системы, имеющей сертификат соответствия ФСТЭК России.*

СКЗИ, используемые для обеспечения защищенного информационного взаимодействия с ИС «Минфин», должны соответствовать требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС1 или выше и иметь действующие сертификаты соответствия.

На АРМ рекомендуется применять лицензионную операционную систему, для которой производителем выпускаются обновления безопасности.

Средство антивирусной защиты должно обладать действующим сертификатом соответствия ФСБ России и/или ФСТЭК России, либо сертификатами соответствия с подтверждением оказания технической поддержки производителем такого средства антивирусной защиты.

Реализация антивирусной защиты должна предусматривать:

- применение средств антивирусной защиты на АРМ;
- установку, конфигурирование и управление средствами антивирусной защиты;
- проведение периодических проверок компонентов АРМ на наличие вредоносных компьютерных программ;
- проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов;
- оповещение об обнаружении вредоносных компьютерных программ;
- определение и выполнение действий по реагированию на обнаружение объектов, подвергшихся заражению вредоносными компьютерными программами;
- регулярное, не реже 1 раза в день, обновление антивирусных баз;
- обновление версий программного обеспечения средств антивирусной защиты по мере их выпуска производителем;
- периодическую проверку работоспособности средств антивирусной защиты.

Все средства защиты информации должны эксплуатироваться в строгом соответствии с требованиями эксплуатационной и технической документации к ним.

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:
  - o обеспечение безопасного межсетевого взаимодействия;
  - o обеспечение защиты конфиденциальности и целостности передаваемой по каналам связи информации;
  - o 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:
  - o проведение инструктажей пользователей АРМ;
  - o разработку документации по защите информации (минимальный типовой комплект представлен в приложении №1);
  - o 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«Бюджет-СМАРТ Про»;
- ✓ ПК «Проект-СМАРТ Про»;
- ✓ ПК «Хранилище-КС»;
- ✓ ПК«Свод-СМАРТ».

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.

Применяемые организационные и технические меры защиты информации должны удовлетворять требованиям, установленным для 3 класса защищенности государственных информационных систем и требованиям, установленным для 4 уровня защищенности персональных данных.

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 требованиям по защите информации не ниже 3 класса защищенности государственных информационных систем и 4 уровня защищенности персональных данных, протокол контроля уровня защиты информации на аттестованном объекте информатизации);
- ✓ оформление соглашения об информационном взаимодействии;
- ✓ определение узлов взаимодействия и их конфигурирование.

Приложение №1

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).

Приложение №2

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. Наличия 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 по схеме подключения № _____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)