Министерство социальной политики и труда Удмуртской Республики
(Минсоцполитики УР)

Удмурт Элькунысь мерлыко политикая но ужъя министерство
(УЭ мерполитикмин)

ПРИКАЗ

«14» июня 2019 г. № 167

г. Ижевск

Об утверждении Инструкции о порядке допуска сотрудников Министерства социальной политики и труда Удмуртской Республики к самостоятельной работе со средствами криптографической защиты информации

В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Инструкцией 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, утверждённой приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 года № 152 п р и к а з ы в а ю:

1. Утвердить прилагаемую Инструкцию о порядке допуска сотрудников Министерства социальной политики и труда Удмуртской Республики к самостоятельной работе со средствами криптографической защиты информации.

2. Признать утратившим силу приказ Министерства социальной, семейной и демографической политики Удмуртской Республики от 30 декабря 2015 года № 348 «Об утверждении Инструкции о порядке допуска сотрудников Министерства социальной, семейной и демографической политики Удмуртской Республики к самостоятельной работе со средствами криптографической защиты информации».

3. Контроль за исполнением настоящего приказа возложить на заместителя министра Белоусову М.Е.

Министр Т.Ю. Чуракова

УТВЕРЖДЕНА

приказом Министерства
социальной политики и труда
Удмуртской Республики
от «14» июня 2019 года № 167

ИНСТРУКЦИЯ
о порядке допуска сотрудников Министерства социальной политики и труда Удмуртской Республики к самостоятельной работе со средствами криптографической защиты информации

1. Настоящая Инструкция определяет порядок допуска сотрудников Министерства социальной политики и труда Удмуртской Республики (далее – Министерство) к самостоятельной работе со средствами криптографической защиты информации (далее – СКЗИ).

2. Инструкция разработана в соответствии с требованиями:

Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

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, утверждённой приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 года № 152;

Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утверждённого приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66;

Требований к защите персональных данных при их обработке в информационных системах персональных данных, утверждённых постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119;

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, утверждённых приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378.

3. Администратор безопасности за эксплуатацию СКЗИ должен пройти обучение в организации, осуществляющей образовательную деятельность по дополнительным профессиональным программам в области информационной безопасности, согласованных с Федеральной службой по техническому и экспортному контролю.

4. Сотрудники Министерства для получения допуска к самостоятельной работе с СКЗИ:

проходят обучение по Программе подготовки к самостоятельной работе со средствами криптографической защиты информации (далее – Программа) в соответствии с приложением 1 к настоящей Инструкции;

сдают тесты на допуск к самостоятельному использованию средств криптографической защиты информации (далее – тестирование) в соответствии с приложениями 2, 3 к настоящей Инструкции.

5. Администратор безопасности за эксплуатацию СКЗИ:

проводит практические занятия с сотрудниками Министерства в соответствии с Программой;

организует проведение тестирования сотрудников Министерства;

на основании тестирования принимает решение о допуске сотрудников Министерства к самостоятельной работе с СКЗИ.

6. К самостоятельной работе с СКЗИ допускаются сотрудники Министерства, прошедшие подготовку по Программе и тестирование.

7. Документом, подтверждающим подготовку к самостоятельной работе с СКЗИ, является акт ввода в эксплуатацию СКЗИ. К акту ввода в эксплуатацию СКЗИ приобщаются результаты тестирования.

8. Ответственность за полноту и качество подготовки сотрудников Министерства к тестированию возлагается на администратора безопасности за эксплуатацию СКЗИ.

9. Достоверность результата тестирования контролируется Технической комиссией по защите информации Министерства.

Приложение 1
к Инструкции о порядке допуска сотрудников Министерства социальной политики и труда Удмуртской Республики к самостоятельной работе со средствами криптографической защиты информации

ПРОГРАММА
подготовки к самостоятельной работе со средствами криптографической защиты информации

№ п/п	Изучаемые вопросы	Кол-во часов, ч.	Форма подготовки/ форма контроля
1	2	3	4
1	Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	1	Самоподго-товка
2	Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»	1	Самоподго-товка
3	Федеральный закон от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»	1	Самоподго-товка
4	Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утверждённая приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 года № 152	1	Самоподго-товка
5	Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утверждённое приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66	2	Самоподго-товка
6	Требования к защите персональных данных при их обработке в информационных системах персональных данных, утверждённых постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119.	1	Самоподго-товка
7	Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации,	1	Самоподго-товка

1	2	3	4
	необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утверждённые приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378		
8	СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы»	1	Самоподготовка
9	Эксплуатационная и техническая документация на используемые средства криптографической защиты информации	2	Самоподготовка
10	Инструкция по обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах Министерства социальной политики и труда Удмуртской Республики	2	Самоподготовка
11	Инструкция о порядке допуска сотрудников Министерства социальной политики и труда Удмуртской Республики к самостоятельной работе со средствами криптографической защиты информации	1	Самоподготовка
12	Правила работы со средствами криптографической защиты информации и криптографическими ключами	2	Практическое занятие
13	Работа с криптографическими ключами. Установка сертификата криптографического ключа. Демонстрация возможностей средств криптографической защиты информации. Установка и настройка средств криптографической защиты информации. Функциональные возможности ключевых носителей информации	2	Практическое занятие
14	Оценка знаний по правилам работы со средствами криптографической защиты информации	1	Тестирование
	Итого	**19**	

Приложение 2
к Инструкции о порядке допуска сотрудников Министерства социальной политики и труда Удмуртской Республики к самостоятельной работе со средствами криптографической защиты информации

ТЕСТ
на допуск к самостоятельному использованию средств криптографической защиты информации

Вопрос 1. VipNetClient [Деловая почта] предназначена для:
- ○ регистрации электронных документов;
- ○ организации защищенной передачи электронных документов по открытым каналам связи;
- ○ регистрации сайтов, посещаемых через InternetExplorer.

Вопрос 2. Когда в графе «Атрибуты» главного окна VipNetClient появляется признак «ПШО», то это означает что:
- ○ письмо отправлено;
- ○ письмо доставлено;
- ○ письмо прочитано.

Вопрос 3. Основные возможности VipNetClient [Монитор]:
- ○ обмен сообщениями/конференция, файловый обмен, деловая почта, проверка;
- ○ соединения с узлом и информирование о статусе пользователя, открыть сетевой ресурс файловый обмен;
- ○ обмен сообщениями/конференция, файловый обмен.

Вопрос 4. Какие действия необходимо выполнить с неработоспособными криптографическими ключами пользователям СКЗИ?
- ○ уничтожить;
- ○ передать администратору безопасности за эксплуатацию СКЗИ;
- ○ перезаписать на ключевой носитель.

Вопрос 5. При увольнении или прекращении использования СКЗИ сотрудник, имеющий доступ к ключевым носителям или к ключевой информации на данных носителях, обязан:
- ○ сдать СКЗИ, эксплуатационную и техническую документацию к ним, криптографические ключи;
- ○ незамедлительно уведомлять ответственного за эксплуатацию СКЗИ;
- ○ уничтожить СКЗИ, эксплуатационную и техническую документацию к ним, криптографические ключи.

Вопрос 6. Какой кнопкой в VipnetClient выбрать получателя для отправки письма?

○  ○  ○ 

Вопрос 7. Как проверить соединение с узлом через VipNetClient [Монитор]?

- ○ выбрать сетевой узел и нажать клавишу «F5»;
- ○ отправить письмо;
- ○ таких возможностей нет в программе VipNetClient [Монитор].

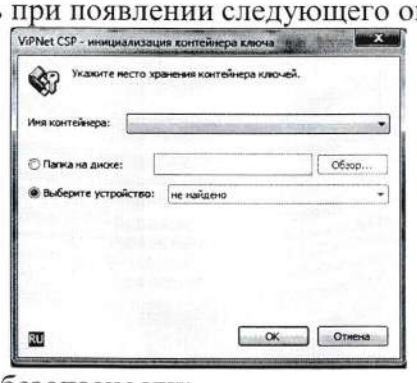
Вопрос 8. Пользователю СКЗИ запрещается:

- ○ работать с ключевыми носителями информации;
- ○ расшифровывать и подписывать электронные документы;
- ○ осуществлять несанкционированное копирование криптографических ключей; вскрывать корпуса ключевого носителя; использовать ключевые носители для работы на других АРМ; передавать ключевые носители лицам, к ним не допущенным; записывать на ключевой носитель с криптографическими ключами постороннюю информацию.

Вопрос 9. Для чего предназначена программа VipNet [Монитор]?

- ○ для выполнения функции персонального сетевого экрана и шифрования ip-трафика компьютера;
- ○ для обеспечения обмена конвертами и файлами с другими сетевыми узлами;
- ○ для контроля сетевой активности на каждом компьютере.

Вопрос 10. Что нужно сделать при появлении следующего окна в VipNetClient



- ○ позвонить администратору безопасности;
- ○ вставить eToken в usb-порт;
- ○ нажать ОК.

Результат тестирования:

Фамилия, имя, отчество сотрудника	**Результат тестирования**		**Дата тестирования**	**Администратор безопасности за эксплуатацию СКЗИ**	
	Количество правильных ответов	**Сдан / Не сдан**		**Фамилия, имя, отчество**	**Подпись**

Приложение 3
к Инструкции о порядке допуска сотрудников Министерства социальной политики и труда Удмуртской Республики к самостоятельной работе со средствами криптографической защиты информации

ТЕСТ
на допуск к самостоятельному использованию средств криптографической защиты информации

Вопрос 1. Основное предназначение программы КриптоПро CSP:
- ○ для копирования юридически значимых документов;
- ○ для обеспечение процесса придания электронным документам юридической значимости посредством использования ЭП а также конфиденциальности и контроля целостности шифрованной информации;
- ○ для выхода в локальную сеть.

Вопрос 2. Каким образом осуществляется хранение криптографических ключей?
- ○ в закрываемых на замок шкафах;
- ○ у начальника структурного подразделения Министерства;
- ○ в закрываемых на замок металлических шкафах (сейфах) в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Вопрос 3. На время отсутствия пользователей СКЗИ должны:
- ○ удаляться;
- ○ быть не активны (выключен монитор);
- ○ при наличии технической возможности быть выключены, отключены от линии связи и убраны в опечатываемые хранилища.

Вопрос 4. Какие действия необходимо выполнить с неработоспособными криптографическими ключами пользователям СКЗИ?
- ○ уничтожить;
- ○ передать администратору безопасности за эксплуатацию СКЗИ;
- ○ перезаписать на ключевой носитель.

Вопрос 5. При увольнении или прекращении использования СКЗИ сотрудник, имеющий доступ к ключевым носителям или к ключевой информации на данных носителях, обязан:
- ○ сдать СКЗИ, эксплуатационную и техническую документацию к ним, криптографические ключи;
- ○ незамедлительно уведомлять ответственного за эксплуатацию СКЗИ;
- ○ уничтожить СКЗИ, эксплуатационную и техническую документацию к ним, криптографические ключи.

Вопрос 6. Для чего используются криптографические ключи?
- ○ для обеспечения конфиденциальности, авторства и целостности электронных документов;
- ○ для включения компьютера;
- ○ для хранения документов.

Вопрос 7. При сбоях или отказах ключевых носителей с криптографическими ключами в экстренных случаях пользователь СКЗИ может:

○ использовать ключевые носители с криптографическими ключами другого сотрудника;
○ вскрыть конверт с резервными криптографическими ключами с последующим уведомлением администратора безопасности за эксплуатацию СКЗИ о факте вскрытия конверта с криптографическими ключами;
○ сменить пароль на ключевом носителе.

Вопрос 8. Как просмотреть сертификаты в контейнере?

○ открыть вкладку «Безопасность»;
○ открыть вкладку «Дополнительно»;
○ открыть вкладку «Сервис».

Вопрос 9. Как проверить что eToken правильно подключен в usb-порт?

○ с помощью программы Крипто Про CSP;
○ с помощью программы PKI Client;
○ с помощью программы Nero 2016 Platinum.

Вопрос 10. Что подтверждает юридическую значимость электронной подписи в документе?

○ сертификат ключа проверки электронной подписи;
○ открытый ключ проверки электронной подписи;
○ договор оказания услуг.

Результат тестирования:

Фамилия, имя, отчество сотрудника	**Результат тестирования**		**Дата тестирования**	**Администратор безопасности за эксплуатацию СКЗИ**	
	Количество правильных ответов	**Сдан / Не сдан**		**Фамилия, имя, отчество**	**Подпись**