АДМИНИСТРАЦИЯ ВОЛЧИХИНСКОГР РАЙОНА АЛТАЙСКОГО КРАЯ

РАСПОРЯЖЕНИЕ

27.08.2020 № 60-р

с. Волчиха

О назначении ответственного
пользователя криптосредств

В целях соблюдения Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ, Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа ФСБ России от 10.07.2014 № 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 защищённости».

1. Утвердить:

1.1. Программу подготовки к самостоятельной работе со средствами криптографической защиты информации (Приложение 1).

1.2. Состав комиссии по допуску к самостоятельной работе со средствами криптографической защиты информации (Приложение 2).

1.3. Порядок работы со средствами криптографической защиты информации (Приложение 3).

1.4. Порядок размещения специального оборудования, охраны и организации режима в выделенных (режимных) помещениях Администрации Волчихинского района (Приложение 4).

1.5. Список лиц, допущенных к работе со средствами криптографической защиты информации (Приложение 5).

1.6. Список помещений, выделенных для использования средств криптографической защиты информации и хранения ключевых документов к ним (Приложение 6).

1.7. Форму Журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (Приложение 7).

1.8. Порядок заполнения «Журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов» (Приложение 8).

1.9. Форму Журнала учета и уничтожения носителей с ключевой информацией (Приложение 9).

1.10. Форму Журнала выдачи носителей с ключевой информацией (Приложение 10).

1.11. Форму Журнала регистрации ключей от режимных помещений (Приложение 11).

1.12. Форму Журнала учета хранилищ (Приложение 12).

1.13. Форму Журнала регистрации выдачи сдачи ключей от режимных помещений (Приложение 13).

1.14. Форму Журнала регистрации выдачи сдачи ключей от хранилищ (Приложение 14).

1.15. Форму Лицевых счетов пользователей средств криптографической защиты информации (Приложение 15).

1.16. Форму Акта ввода в эксплуатацию средств криптографической защиты информации (Приложение 16).

1.17. Порядок восстановления связи в случае компрометации действующих ключей к средствам криптографической защиты информации (Приложение 17).

1.18. Форму Заключения о допуске к самостоятельной работе с средствами криптографической защиты информации (Приложение 18).

1.19. Форму Журнала технического (аппаратного) (Приложение 19).

2. Назначить Ответственным пользователем криптосредств заведующего сектором информационного обеспечения управления делами Балакиреву О.В. Соответствующие изменения внести в должностную инструкцию. Во время отсутствия заведующего сектором информационного обеспечения обязанности Ответственного пользователя криптосредств возлагать на ведущего специалиста-секретаря административной комиссии Качесову Е.О.

3. Возложить на Ответственного пользователя криптосредств обязанности (внести соответствующие изменения в должностную инструкцию):

3.1. По вводу в эксплуатацию средств криптографической защиты информации.

3.2. По ведению:

– журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов;

– журнала учета и уничтожения носителей с ключевой информацией;

– журнала выдачи носителей с ключевой информацией;

– журнала регистрации ключей от режимных помещений;

– журнала учета хранилищ;

– лицевых счетов пользователей средств криптографической защиты информации;

– журнала регистрации выдачи/сдачи ключей от хранилищ.

– журнала регистрации выдач/сдачи ключей от режимных помещений.

4. Всем сотрудникам, которым необходимо осуществлять работу со средствами криптографической защиты информации, пройти обучение в соответствии с утвержденной программой.

5. Комиссии по допуску к самостоятельной работе со средствами криптографической защиты информации провести оценку готовности сотрудника к работе и в случае положительной оценки выдать заключение о допуске к самостоятельной работе с СКЗИ.

6. Управляющему делами Шевич Н.А. ознакомить всех сотрудников Администрации Волчихинского района, допущенных к работе со средствами криптографической защиты информации с распоряжением.

7. Контроль за исполнением распоряжения оставляю за собой.

Глава района Е.В. Артюшкина

Приложение 1
к распоряжению Администрации
района
от 27.08.2020 № 60-л

ПЛАН
обучения правилам защиты информации
в Администрации Волчихинского района

№ п/п	Изучаемые вопросы (темы)	Кол-во часов	Форма (метод) подготовки	Преподаватель
Раздел 1	Изучение законодательной базы			
1	Федеральный закон от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	1	Самоподготовка	
2	Федеральный закон от 27 июля 2006г. № 152-ФЗ «О персональных данных»	1	Самоподготовка	
3	Федеральный закон от 06 апреля 2011г. № 63-ФЗ «Об электронной подписи»	1	Самоподготовка	
4	Приказ ФСТЭК России от 18 февраля 2013г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»	1	Самоподготовка	
5	Постановление Правительства Российской Федерации от 15 сентября 2008г. № 687 «Об утверждении Положения об	1	Самоподготовка	

№ п/п	Изучаемые вопросы (темы)	Кол-во часов	Форма (метод) подготовки	Преподаватель
	особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»			
6	Постановление Правительства Российской Федерации от 01 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	1	Самоподготовка	
Форма контроля: устный опрос				
Раздел 2	Изучение локальных нормативных актов и эксплуатационной документации			
1	Эксплуатационно-техническая документация на используемые СЗИ (СЗИ от НСД, ПМЭ, антивирусное программное обеспечение)	8	Самоподготовка	
2	Регламент по работе пользователя в информационных системах	2	Самоподготовка	
3	Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных	2	Самоподготовка	
4	Порядок проведения антивирусного контроля в информационных системах	2	Самоподготовка	
5	Порядок организации и проведения работ по защите информации в информационных системах	2	Самоподготовка	
6	Порядок организации парольной защиты	2	Самоподготовка	

№ п/п	Изучаемые вопросы (темы)	Кол-во часов	Форма (метод) подготовки	Преподаватель
	в информационных системах			
Форма контроля: устный опрос				
Раздел 3	Практическая часть			
1	Работа на АРМ с установленными СЗИ от НСД (порядок запуска системы, смены пароля, действия в случае срабатывания СЗИ от НСД)	1	Тренинг	
2	Работа на АРМ с установленным антивирусным программным обеспечением (использование внешних носителей, работа в локальной сети, сети Интернет, отправка данных)	1	Тренинг	
Форма контроля: практический контроль				

Приложение 2
к распоряжению Администрации района
от 27.08.2020 № 607

СОСТАВ КОМИССИИ
по допуску к самостоятельной работе со средствами криптографической защиты информации в Администрации Волчихинского района

Для допуска сотрудников Администрации Волчихинского района Алтайского края к самостоятельной работе со средствами криптографической защиты информации (СКЗИ) назначается комиссия в составе:

Председатель комиссии:

– Артюшкина Е.В, председатель комиссии- глава района.

Члены комиссии:

– Шевич Н.А. , заместитель председателя комиссии – управляющий делами;

– Балакирева О.В. член комиссии – заведующий сектором информационного обеспечения управления делами.

В случае отсутствия Артюшкиной Е.В., председателя комиссии обязанности председателя комиссии возлагать на заместителя председателя комитета Шевич Н.А., заместителя председателя комиссии СКЗИ.

По результатам работ комиссия предоставляет главе Волчихинского района для утверждения Заключение о допуске к самостоятельной работе с СКЗИ (для каждого пользователя СКЗИ составляется отдельное Заключение).

Приложение 3
к распоряжению Администрации района
от 27.08.2010 № 60-л

ПОРЯДОК
работы со средствами криптографической защиты информации в в Администрации Волчихинского района

1. Обозначения и сокращения

АИБ – администратор информационной безопасности;
ИБ – информационная безопасность;
НКИ – носители ключевой информации;
СКЗИ – средства криптографической защиты информации;
ПЭВМ – персональная электронная вычислительная машина;
ЭП – электронная подпись.

2. Понятия и определения

2.1. Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

2.2. Сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

2.3. Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи.

2.4. Средство криптографической защиты информации – средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

3. Общие положения

3.1. Настоящий Порядок по работе с СКЗИ в Администрации Волчихинского йона (далее – Порядок) определяет:

– правила обращения с СКЗИ и криптографическими ключами;

– основные обязанности, права и ответственность Пользователя СКЗИ (далее Пользователя);

– действия при компрометации ключей и восстановлении конфиденциальной язи;

– специальные требования по обработке информации с использованием СКЗИ;

3.2. Пользователь должен выполнять все требования настоящего Порядка, равила, изложенные в эксплуатационной документации на СКЗИ, а также другие кументы, регламентирующие порядок работы с СКЗИ.

3.3. Данный Порядок разработан в соответствии с требованиями следующих рмативных документов:

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Постановления Правительства Российской Федерации от 01.11.2012 № 1119 Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и держания организационных и технических мер по обеспечению безопасности рсональных данных при их обработке в информационных системах персональных нных с использованием средств криптографической защиты информации, обходимых для выполнения установленных Правительством Российской дерации требований к защите персональных данных для каждого из уровней щищенности».

3.4. Требования настоящего Порядка распространяется на всех специалистов дминистрации Волчихинского района(далее – Администрация района), спользующих СКЗИ.

3.5. Все сотрудники Администрации района, начинающие работу с СКЗИ, бязаны пройти обучение в соответствии с программами подготовки к мостоятельной работе с используемыми СКЗИ.

4. Общий порядок работы с СКЗИ

4.1. На все поступающие СКЗИ, ключевые дискеты должен вестись оэкземплярный учет в «Журнале поэкземплярного учета СКЗИ, эксплуатационной технической документации к ним». Единицей поэкземплярного учета СКЗИ для рограммных СКЗИ является инсталляционная дискета или компакт-диск (CD-

ROM). Выдаваемые Пользователям СКЗИ должны иметь учетные номера. Все СКЗИ реализуются (распространяются) вместе с правилами пользования ими.

4.2. Передачу СКЗИ производит ответственный пользователь криптосредств Пользователю под роспись в «Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним». Установка (инсталляция) СКЗИ осуществляется в соответствии с требованиями документации на СКЗИ.

4.3. Рабочие места, оснащенные СКЗИ и предназначенные для создания информации о ключах (рабочие места Администратора безопасности) должны быть оснащены специально выделенными ПЭВМ.

4.4. Установка (переустановка) программных средств рабочего места производится Ответственным пользователем криптосредств с лицензионных инсталляционных комплектов. Перед установкой должна быть проведена проверка на отсутствие вирусов и программных «закладных» устройств.

4.5. Ответственными специалистами периодически должен проводиться контроль сохранности СКЗИ, а также всего используемого совместно с СКЗИ программного обеспечения для предотвращения внесения программно-аппаратных «закладных» устройств и программ вирусов.

4.6. Должны быть приняты организационные меры с целью исключения возможности несанкционированного копирования СКЗИ.

4.7. Ключевые дискеты СКЗИ и тестовые ключи должны храниться в металлическом шкафу (сейфе) отдельно от других документов. При вскрытии металлического шкафа (сейфа) должна быть проверена целостность замков. В случае нарушения целостности печатей или замков ответственный специалист обязан немедленно доложить об этом главе района. Рабочие и резервные носители ключевой информации, предназначенные для использования в случае компрометации рабочей ключевой информации, должны храниться в разных местах (металлических шкафах, сейфах).

4.8. Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования). Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), Data Key, Smart Card, Touch Memory и т.п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

4.9. Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по

уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

4.10. Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к СКЗИ уничтожают путем сжигания или с помощью любых бумагорезательных машин.

4.11. СКЗИ уничтожают (утилизируют) в соответствии с требованиями Положения ПКЗ-2005 по решению обладателя конфиденциальной информации, владеющего СКЗИ.

4.12. Подлежащие уничтожению (утилизации) СКЗИ должны быть изъяты из аппаратных средств, с которыми они функционировали. При этом СКЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ процедура удаления программного обеспечения СКЗИ и они полностью отсоединены от аппаратных средств.

4.13. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций СКЗИ, а также совместно работающее с СКЗИ оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.) разрешается использовать после уничтожения СКЗИ без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

4.14. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введенная и хранящаяся в СКЗИ или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия криптоключам. Хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

5. Основные обязанности Пользователя

5.1. Пользователь обязан:

– соблюдать требования по обеспечению безопасности функционирования СКЗИ согласно документации к средствам защиты;

– обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей;

– сдать носители ключевой информации при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

– сдать носители ключевой информации по окончании срока действия сертификата ключа, а также в случае компрометации ключа;

– немедленно уведомлять АИБа о компрометации криптографических ключей;

– немедленно уведомлять АИБа о фактах утраты или недостачи СКЗИ, НКИ;

– в пределах своей компетенции предоставлять информацию комиссии, проводящей служебные расследования по фактам компрометации, а также выявления причин нарушения установленных требований информационной безопасности при функционировании СКЗИ.

6. Права Пользователя

6.1. Пользователь имеет право:

– вносить предложения Руководству по совершенствованию СКЗИ;

– повышать уровень квалификации по использованию СКЗИ.

7. Порядок обращения с СКЗИ

7.1. Монтаж и установка СКЗИ осуществляются АИБом.

7.2. Установка и ввод в эксплуатацию, а также эксплуатация СКЗИ должна осуществляться в соответствии с эксплуатационной и технической документацией к этим средствам.

7.3. Для хранения носителей ключевой информации помещения обеспечиваются сейфами (металлическими шкафами), оборудуются охранной сигнализацией и по убытии сотрудников закрываются, сдаются под охрану.

7.4. Дубликаты ключей от сейфов (а также значения кодов – при наличии кодовых замков) пользователей должны храниться в сейфе руководителя подразделения в упаковках, опечатанных личными печатями пользователей. Несанкционированное изготовление дубликатов ключей ЗАПРЕЩЕНО. В случае утери ключа механизм (секрет) замка (либо сам сейф) должен быть заменён.

7.5. К эксплуатации СКЗИ допускаются лица, прошедшие соответствующую подготовку и изучившие правила пользования данным СКЗИ.

8. Порядок обращения с ключами

8.1. Выработанные секретные криптоключи хранятся исключительно в электронном виде на цифровых носителях информации, которые получают статус

НКИ.

8.2. Владельцы ключей несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту НКИ от несанкционированного использования.

8.3. Для хранения носителей ключевой информации Пользователь должен быть обеспечен личным сейфом. В случае отсутствия индивидуального сейфа по окончании рабочего дня Пользователь обязан сдавать НКИ лицу, ответственному за хранение.

8.4. Категорически запрещается:

– осуществлять несанкционированное и безучётное копирование ключевых данных;

– хранить НКИ вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность;

– передавать НКИ каким бы то ни было лицам, кроме Владельца ключа;

– во время работы оставлять НКИ без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ);

– хранить на НКИ какую-либо информацию, кроме ключевой;

– использовать в помещениях, где применяются СКЗИ, личные технические средства, позволяющие осуществлять копирование ключевой информации.

8.5. Не позднее 10 дней до окончания срока действия сертификата криптоключей Пользователь предоставляет АИБу, заявление на изготовление нового ключа.

8.6. После ввода в действие нового ключа Пользователь обязан предоставить АИБу, ключ, выведенный из действия для уничтожения ключевой информации с носителя.

8.7. Использование криптоключей, которые выведены из действия, запрещено.

9. Действия при компрометации действующих ключей и восстановлении конфиденциальной связи

9.1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию Владельца и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

– утрата (хищение) НКИ, в том числе – с последующим их обнаружением;

– увольнение (переназначение) специалистов, имевших доступ к ключевой информации;

– передача секретных ключей по линии связи в открытом виде;

– нарушение правил хранения криптоключей;

– вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);

– несанкционированное или безучётное копирование ключевой информации;

– все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

9.2. При наступлении любого из перечисленных выше событий владелец ключа должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) АИБу, лично, по телефону, электронной почте или другим доступным способом. В любом случае владелец ключа обязан убедиться, что его сообщение получено и прочтено адресатом.

9.3. При подтверждении факта компрометации действующих ключей Пользователь обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей и сдачу их АИБу в течение 3 рабочих дней.

9.4. Для восстановления конфиденциальной связи после компрометации действующих ключей Пользователь получает у АИБа новые ключи ЭП на основании предоставленного Заявления на изготовления криптоключа.

10. Ответственность Пользователя

10.1. Пользователь несет персональную ответственность за:

– за правильность эксплуатации и сохранность СКЗИ носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями;

– сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с СКЗИ;

– сохранение в тайне содержания закрытых ключей СКЗИ и средств ЭП;

– утрату и некорректность эксплуатации СКЗИ и закрытых ключей;

– за то, чтобы на компьютере, на котором установлены СКЗИ и средства ЭП, не были установлены и не эксплуатировались программы (в том числе, вирусы), которые могут нарушить функционирование программных СКЗИ и средств ЭП;

– в случае несвоевременного сообщения о факте компрометации ключей Пользователь, допустивший компрометацию ключей, несет ответственность в полном объеме за ущерб, причиненный им другим Пользователям Системы.

10.2. В случае неисполнения или ненадлежащего выполнения требований настоящего Порядка Пользователь ключа может быть привлечен к дисциплинарной и/или административной ответственности в соответствии с действующим Законодательством Российской Федерации.

Приложение 4
к распоряжению Администрации
района
от 27.08.2020 № 60-р

ПОРЯДОК
по размещению специального оборудования, охраны и организации режима в выделенных (режимных) помещениях в Администрации Волчихинского района

1. Перечень используемых определений, обозначений и сокращений

Доступ к информации – возможность получения информации и ее использования.

Контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств.

Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) – шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь – лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Режимные помещения – помещения, где установлены криптосредства или хранятся ключевые документы к ним.

Шифровальные (криптографические) средства – криптосредства:

1. средства шифрования – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

2. средства имитозащиты – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

3. средства электронной цифровой подписи – аппаратные, программные и аппаратно–программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;

4. средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

5. средства изготовления ключевых документов (независимо от вида носителя ключевой информации);

6. ключевые документы (независимо от вида носителя ключевой информации).

2. Общие положения

2.1. Настоящий Порядок устанавливает правила и общие требования к организации работы специалистов Администрации Волчихинского района (далее – Администрация района), использующих в своей работе криптосредства и имеющих допуск в помещения, в которых установлены данные криптосредства или хранятся ключевые документы к ним.

2.2. Требования данного Порядка обязательны для исполнения всеми сотрудниками Администрации района, использующими в своей работе криптосредства и имеющими допуск в помещения, в которых установлены данные криптосредства или хранятся ключевые документы к ним.

2.3. Ответственным за соблюдение требований данного Порядка является ответственный пользователь криптосредства.

2.4. Размещение оборудования, функционирующего с криптосредствами, охрана и организация режима в помещениях, где установлены криптосредства или

хранятся ключевые документы к ним (далее – режимные помещения), должны обеспечивать сохранность персональных данных, криптосредств и ключевых документов к ним.

2.5. Режимные помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

2.6. Для предотвращения просмотра извне режимных помещений их окна должны быть защищены.

2.7. Режимные помещения должны быть оснащены охранной сигнализацией, связанной со службой охраны. Исправность сигнализации периодически необходимо проверять ответственному пользователю криптосредств с отметкой в журнале проверки исправности и технического обслуживания.

2.8. Размещение и монтаж оборудования, функционирующего с криптосредствами, в режимных помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам.

3. Организация работы с ключами от режимных помещений и металлических хранилищ

3.1. Двери режимных помещений должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников Администрации района и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают специалистам, имеющим право допуска в режимные помещения, под расписку в журнале регистрации ключей от режимных помещений. Дубликаты ключей от входных дверей таких помещений храниться в сейфе ответственного пользователя криптосредствами.

3.2. Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей используются металлические хранилища (сейфы), оборудованных внутренними замками с двумя экземплярами ключей и приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища находиться у сотрудника, ответственного за хранилище. Дубликаты ключей от хранилищ должны храниться в сейфе ответственного пользователя криптосредств. Дубликат ключа от сейфа ответственного пользователя криптосредств в опечатанной упаковке (конверте) должны храниться у управляющего делами под расписку в журнале регистрации ключей от режимных помещений.

3.3. По окончании рабочего дня режимные помещения и установленные в них хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в

соответствующем журнале регистрации выдачи/сдачи ключей от хранилищ ответственному пользователю криптосредств, который хранит эти ключи в личном выделенном хранилище.

Ключи от режимных помещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ режимного помещения, в опечатанном виде должны быть сданы под расписку в журнале регистрации выдачи/сдачи ключей от режимных помещений службы охраны (вахтера) одновременно с передачей под охрану самих режимных помещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей криптосредств, ответственных за эти хранилища.

3.4. При утрате ключа от хранилища или от входной двери в режимное помещение замок необходимо заменить с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Хранение ключевых и других документов из хранилища, от которого утрачен ключ, до замены замка происходит в другом исправном хранилище по согласованию с ответственным пользователем криптосредств.

3.5. В обычных условиях режимные помещения и находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями криптосредств, ответственным пользователем криптосредств или главой Волчихинского района.

3.6. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному пользователю криптосредств или главе Волчихинского района. Прибывший ответственный пользователь криптосредств должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации персональных данных и к замене скомпрометированных криптоключей.

4. Организация пропускного режима в режимные помещения

4.1. Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

4.2. Режим охраны помещений, в том числе правила допуска специалистов и посетителей в рабочее и нерабочее время, устанавливает ответственный пользователь криптосредств.

4.3. Доступ сотрудников Администрации района в режимные помещения осуществляется на основании соответствующих списков допущенных, согласованных с ответственным пользователем криптосредств и утвержденных главой Волчихинского района.

4.4. Доступ сотрудников Администрации Волчихинского района, не включенных в списки, разрешается только с личного разрешения ответственного пользователя криптосредств и только по служебной необходимости.

5. Организация работы с криптосредствами

5.1. Техническое обслуживание оборудования, функционирующего с криптосредствами, и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

5.2. На время отсутствия пользователей криптосредств оборудование, функционирующее с криптосредствами, должно быть выключено и отключено от линии связи. Использование криптосредств посторонними лицами ЗАПРЕЩАЕТСЯ.

5.3. Работа пользователей с криптосредствами регламентируется эксплуатационной документацией на используемые криптосредства.

Приложение 5
к распоряжению Администрации района
от 27.08.2020 № 60-л

СПИСОК ЛИЦ,
допущенных к работе со средствами криптографической защиты информации в Администрации Волчихинского района

№ п/п	Должность	ФИО
1	Начальник отдела учета и отчетности	Шадуро Наталья Николаевна
2	Заведующий сектором по градостроительству	Барсукова Людмила Александровна
3	Главный специалист	Трубе Наталья Владимировна
4	Главный специалист	Черникова Нина Николаевна
5	Ведущий специалист	Скопенцова Нина Владимировна
6	Ведущий специалист	Кнышева Екатерина Матвеевна
7	Заведующий сектором информационного обеспечения управления делами	Балакирева Оксана Владимировна
8	Главный специалист	Зацепина Наталья Юрьевна
9	Главный специалист	Овчарова Юлия Петровна
10	И.о. начальника правового отдела	Лукина Елена Михайловна
11	Главный специалист	Трунова Ольга Васильевна

Приложение 6
к распоряжению Администрации района
от 27.08.2020 № 60-р

СПИСОК ПОМЕЩЕНИЙ,
выделенных для использования СКЗИ и хранения ключевых документов к ним в Администрации Волчихинского района

№ п/п	№ кабинета	Адрес, размещение
1	2	658930, Алтайский край, с.Волчиха, ул. Свердлова,4
2	11	658930, Алтайский край, с.Волчиха, ул. Свердлова,4
3	32	658930, Алтайский край, с.Волчиха, ул. Свердлова,4
4	35	658930, Алтайский край, с.Волчиха, ул. Свердлова,4
5	18	658930, Алтайский край, с.Волчиха, ул. Свердлова,4
6	20	658930, Алтайский край, с.Волчиха, ул. Свердлова,4

Приложение 7
к распоряжению Администрации района
от 27.08.2020 № 60-к

ФОРМА
журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов в Администрации Волчихинского района

Начат «____» _____ 202_ г.
Окончен «____» _____ 202_ г.
На _____ листах

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ
1	2	3	4	5	6	7

Отметка о выдаче	Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Дата и расписка в получении	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
8	9	10	11	12	13	14	15

Приложение 8
к распоряжению Администрации района
от 27.08.2020 № 60-л

ПОРЯДОК
по заполнению журнала поэкземплярного учета
средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов
в Администрации Волчихинского района

1. Общие положения

1.1. К средствам криптографической защиты информации (далее - СКЗИ) относятся как сами программные или аппаратно-программные средства, так и ключевая информация необходимая для их работы и техническая документация на СКЗИ. В соответствии «Инструкцией об организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащих сведений, составляющих государственную тайну», утвержденной приказом Федерального агентства правительственной связи и информации (ФАПСИ) при Президенте Российской Федерации от 13.06.2001 № 152 (далее – Инструкция № 152) все СКЗИ должны браться на поэкземплярный учет и их движение (выдача, установка, передача, уничтожение) должны быть документально отслежены. Для этих целей Ответственный ведет журнал учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (Приложение № 2 к Инструкции № 152).

2. Порядок заполнения журнала

2.1. В данном журнале подлежат регистрации все полученные СКЗИ и выработанные ключевые документы. Сначала выделяется раздел (1-2 страницы) для регистрации аппаратно-программных и программных средств (например КриптоПРО или других, поставленными сторонними организациями). В следующем выделенном разделе регистрируются ключевые документы: выработанные самостоятельно или полученные от других издателей. При учете применяется сквозная нумерация.

2.2. По разделу 1: пример заполнения на программе СКЗИ Криптопро

1. номер по порядку
2. Крипто-Про v.2.0
3. FE40310300

4. 1 (так как лицензионное соглашение подразумевает одну установку)

5. Организация, проводившая установку
6. Указывается дата установки
7. Ф.И.О. лица, на чьем компьютере проведена установка СКЗИ
8. расписка лица п.7
9. Ф.И.О. лица производившего установку СКЗИ
10. дата установки
11. Серийный или инвентарный номер компьютера
12. Дата изъятия (деинсталяции)
13. Ф.И.О. лиц, производивших деинсталляцию СКЗИ
14. Расписки лиц п. 13 за уничтожение деинсталлированного СКЗИ. Под уничтожением понимается удаление (стирание) дистрибутива программы, лицензии и ключа активации, без возможности восстановления. Если осуществляется перенос СКЗИ на новый компьютер, то данная графа не заполняется, а производится регистрация данного СКЗИ под следующим порядковым номером.

2.3. Раздел 2 «Ключевая информация»

Пример заполнения журнала на основе ключа сформированного на дискете 3,5".

1. номер по порядку
2. Ключ электронной подписи (далее - ЭП) Банк-клиент
3. 119111754 (берется из КриптоПро, описано ниже)
4. 1 (Первый экземпляр)
5. изготовлен самостоятельно
6. дата формирования ключа
7. Ф.И.О. владельца ключа (физическое лицо, для которого изготовлен данный ключ)
8. дата и расписка в получении лица п.7

Графы 9, 10, 11 не заполняются

12. Дата уничтожения ключа по окончании срока действия или другим причинам (порча ключа, лишения владельца прав ЭП и т.п.)
13. Ф.И.О. лиц, производивших уничтожение ключа (2 человека, из числа лиц, наделенных правом использования ЭП, включая администратора ИС, использующей ЭП)
14. Подписи лиц, указанных в п.13

Наклейка дискеты должна содержать следующие идентификационные признаки:

Наименование организации	
Уч.№	Экз. № 1
Ключ ЭП АРМ Банк-клиент	
Ф.И.О. владельца ключа	
Серийный № 119111754	

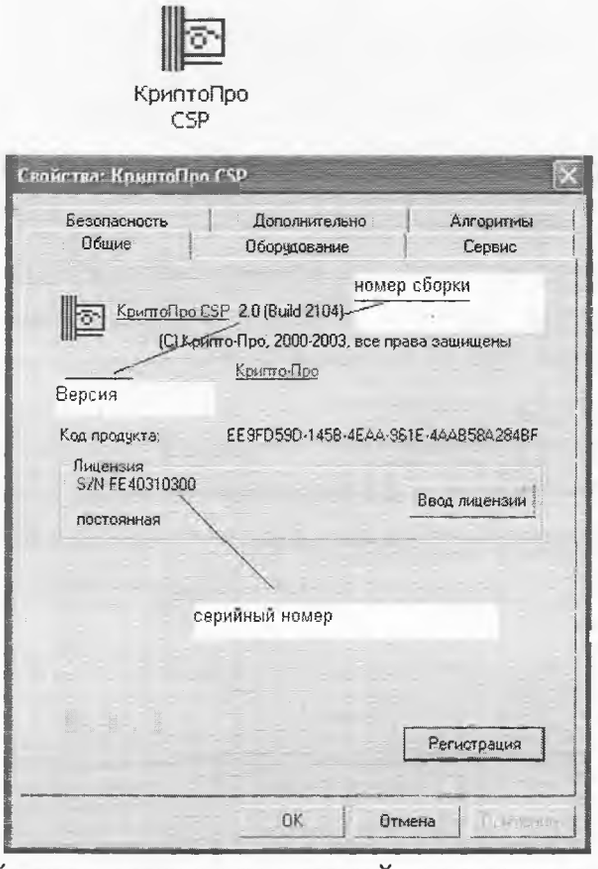
2.4. Согласно правилам пользования Крипто-про, при генерации ключа на дискету, рекомендуется создавать рабочую копию дискеты (порядок копирования подробно изложен в документе «копирование ключей»). При этом созданная резервная дискета учитывается аналогично первоначальной, под следующим порядковым номером, только в графе 4 пишется номер экземпляра «2». В случае

выхода из строя основной дискеты, перед использованием резервной, с нее делается копия, которая учитывается под следующим порядковым номером, а в графе 4 ставиться номер экземпляра «3».

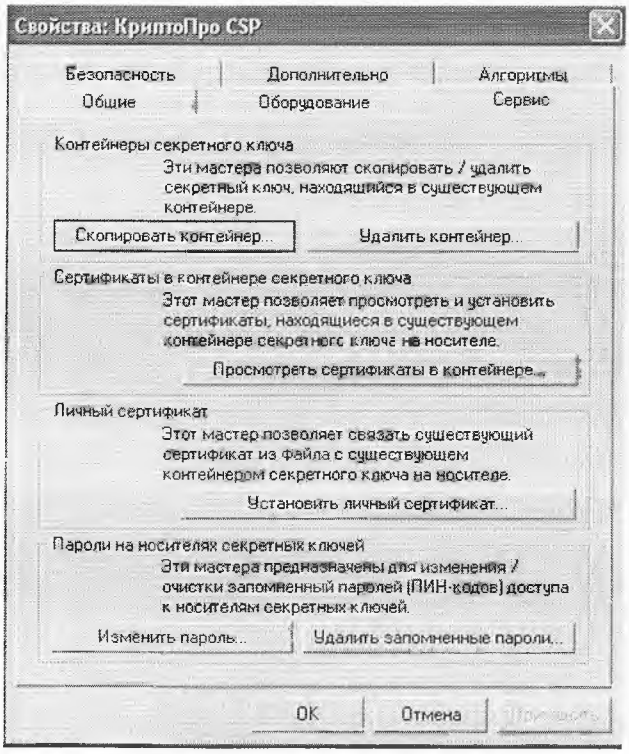
2.5. По окончании срока действия ключа, основная ключевая дискета и резервные копии уничтожаются одновременно.

2.6. При генерации ключа на носитель многократного использования (электронные ключи eToken, ruToken, DS-1995 и т.п.) в графе 4 указывается наименование носителя и его идентификационный номер (определяется при помощи программного обеспечения на данный вид носителя), например ruToken 214978f9.

2.7. Работа с ключевой информацией осуществляется в СКЗИ КриптоПро. Для запуска необходимо нажать Кнопку «ПУСК» - «Настройка» - «Панель управления» и запустить программу со значка



2.8. Удаление контейнеров закрытых ключей, копирование ключей, просмотр контейнеров осуществляется со вкладки «Сервис»



2.9. В случае досрочного прекращения действия закрытого ключа ЭП (смена специалиста, компрометация ключа), закрытый ключ должен быть уничтожен в течении суток с отметкой в журнале учета СКЗИ. Информация об отзыве сертификата также в течении суток направляется в территориальный орган федерального казначейства.

2.10. При плановой смене ключей, по истечении срока их действия, выведенные ключи уничтожаются ответственным пользователем криптосредств Администрации района в течение 4 суток с момента окончания срока действия с отметкой об этом в журнале учета СКЗИ.

Приложение 9
к распоряжению Администрации района
от 27.08.2020 № 60-к

ФОРМА
журнала учета и уничтожения носителей с ключевой информацией
в Администрации Волчихинского района

Начат «____» _____ 202_ г.
Окончен «____» _____ 202_ г.
На _____ листах

Рег. №	Дата формирования ключевой информации	Вид ключевой информации	Дата получения	Наименование органа криптографической защиты	ФИО ответственного пользователя криптосредства	Подпись	№ АКТА/ Дата уничтожения	Подпись по факту уничтожения
1	2	3	4	5	6	7	8	9

Приложение 10
к распоряжению Администрации района
от 27.03.2020 № 607

ФОРМА
журнала выдачи носителей с ключевой информацией
в Администрации Волчихинского района

Начат «____» _____ 202_ г.
Окончен «____» _____ 202_ г.
На _____ листах

№ п/п	Рег. №	Дата выдачи/сдачи	Выдано			Сдано		
			ФИО пользователя носителя с ключевой информацией	подпись пользователя носителя с ключевой информацией	подпись ответственного пользователя носителя с ключевой информацией	ФИО пользователя носителя с ключевой информацией	подпись пользователя носителя с ключевой информацией	подпись ответственного пользователя криптосредств
1	2	3	4	5	6	7	8	9

Приложение 11
к распоряжению Администрации района
от 27.08.2020 № 60-л

ФОРМА
журнал регистрации ключей от режимных помещений/хранилищ
в Администрации Волчихинского района

Начат «____» _____ 202_ г.
Окончен «____» _____ 202_ г.
На _____ листах

№ п/п	Регистрационный номер ключа	Номер экземпляра ключа	Номер (название) режимного помещения/ хранилища	Дата, ФИО, получившего ключ, подпись	Отметки ответственного пользователя криптосредств / руководителя		Сведения об утрате/замене ключа (№ акта, служебной записки и т.п.)
					ФИО	Дата, подпись о получении дубликата ключа	
1	2	3	4	5	6	7	8

Приложение 12
к распоряжению Администрации района
от 27.08.2020 № 60-к

ФОРМА
журнала учета хранилищ в Администрации Волчихинского района

Начат «____» _____ 202_ г.
Окончен «____» _____ 202_ г.
На _____ листах

Учетный номер	Наименование хранилища (сейф, металлический шкаф)	Инвентарный номер	Местонахождение (подразделение, номер комнаты)	Что находится (документы, изделия)	Фамилия ответственного за сейф (шкаф)	Кол-во комплектов ключей и их номера	Расписка ответственного за хранилище в получении ключа и дата	Расписка в приеме ключа и дата
1	2	3	4	5	6	7	8	9

Приложение 13
к распоряжению Администрации района
от 27.08.2020 № 60-л

ФОРМА
журнала регистрации выдачи/сдачи ключей от режимных помещений
в Администрации Волчихинского района

Начат «____» _____ 202_ г.
Окончен «____» _____ 202_ г.
На _____ листах

Дата	Регистрационный номер ключа	Время выдачи	ФИО пользователя	Подпись пользователя	Время сдачи	ФИО пользователя	Подпись пользователя	ФИО, подпись лица, принявшего помещение под охрану
1	2	3	4	5	6	7.	8	9

Приложение 14
к распоряжению Администрации
Волчихинского района
от 27.08.2020 №60-л

ФОРМА
журнала регистрации выдачи/сдачи ключей от хранилищ
в Администрации Волчихинского района

Начат «____» _____ 202_ г.
Окончен «____» _____ 202_ г.
На _____ листах

Дата	Регистрационный номер ключа	Время выдачи	Отметки пользователя		Отметки ответственного пользователя криптосредств		Время сдачи	Отметки пользователя		Отметки ответственного пользователя криптосредств	
			ФИО	Подпись	ФИО	Подпись		ФИО	Подпись	ФИО	Подпись
1	2	3	4	5	6	7	8	9	10	11	12

Приложение 15
к распоряжению Администрации района
от 27.08.2020 № 607

ФОРМА
журнала лицевых счетов пользователей средств
криптографической защиты информации в Администрации Волчихинского района

Начат «____» _____ 202_ г.
Окончен «____» _____ 202_ г.
На _____ листах

№	ФИО пользователя СКЗИ	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Дата ввода в действие	Дата вывода из действия	Примечание
1	2	3	4	5	6	7	8

Приложение 16
к распоряжению Администрации района
от 27.08.2020 № 60-р

ФОРМА
Акта ввода в эксплуатацию
средств криптографической защиты информации

УТВЕРЖДАЮ
Глава района

_____ /Е.В. Артюшкина
«__» _____ 202_г.

АКТ
ввода в эксплуатацию средства криптографической защиты информации

Настоящий акт составлен в том, что _____
(дата)
специалистом_____
(Ф.И.О., должность, наименование организации)
была произведена установка и настройка средства криптографической защиты информации (далее – СКЗИ) _____
(наименование СКЗИ)
Место установки: _____
(адрес, № кабинета)
Пользователь СКЗИ: _____
(Ф.И.О., должность)
Серийный номер ПК: _____

Комплектность и содержание установленного программного средства, обеспечивающего криптографическую защиту информации, соответствует сведениям, указанным в формуляре.

Размещение СКЗИ, хранение ключевых носителей, охрана помещения организованны в установленном порядке.

Обучение правилам работы с СКЗИ и проверка знаний нормативных правовых актов, а также эксплуатационной и технической документации к ним проведены.

Условия для использования СКЗИ, установленные эксплуатационной и технической документации к ним созданы.

Установленное и настроенное ПО находится в работоспособном состоянии.

(должность лица, установившего СКЗИ)	(подпись)	(Ф.И.О.)
(должность пользователя СКЗИ)	(подпись)	(Ф.И.О.)

Должность руководителя (ИП) *ПНО (РП)* *Фамилия И.О. руководителя (ИП)*

Приложение 17
к распоряжению Администрации
района от 27.08.2020 № 60-р

ПОРЯДОК
по восстановлению связи в случае компрометации действующих ключей к средствам криптографической защиты информации в Администрации Волчихинского района

1. Общие положения

1.1. Настоящий Порядок разработан в целях обеспечения восстановления связи в случае компрометации действующих ключей к средствам криптографической защиты информации (далее – СКЗИ) Администрации Волчихинского района (далее – Администрация района).

1.2. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

– потеря ключевых носителей;

– потеря ключевых носителей с их последующим обнаружением;

– увольнение специалистов, имевших доступ к ключевой информации;

– нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа;

– возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;

– нарушение печати на сейфе с ключевыми носителями;

– случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).

1.3. В случае возникновения обстоятельств, указанных в п.1.1 настоящего Порядка, Пользователь обязан немедленно прекратить обмен электронными документами с использованием скомпрометированных закрытых криптографических ключей и сообщить о факте компрометации ответственному за эксплуатацию СКЗИ.

1.4. Смена криптографических ключей проводится в соответствии с

соответствующими положениями «Порядка по работе со средствами криптографической защиты информации в Администрации района».

1.5. Использование СКЗИ может быть возобновлено только после ввода в действие другого криптографического ключа взамен скомпрометированного.

Для этого Пользователь, чей ключевой носитель скомпрометирован, должен написать Заявку на изготовление нового сертификата ключа подписи в соответствии с порядком, установленным в Администрации района.

Ответственный пользователь СКЗИ должен либо создать новый сертификат, либо содействовать получению сертификата в Удостоверяющем центре. После чего необходимо зарегистрировать ключевой носитель в установленном порядке и передать непосредственному пользователю.

1.6. Скомпрометированные ключи подлежат уничтожению в соответствии с порядком, установленным в Администрации района.

Приложение 18
к распоряжению Администрации района
от 27.08.2020 № 60-л

ФОРМА
заключения о допуске к самостоятельной работе с СКЗИ

УТВЕРЖДАЮ
Глава района

_____ /Е.В. Артюшкина
«_____» _____ 202_ г.

Заключение
о допуске к самостоятельной работе с средствами криптографической защиты

Структурное подразделение _____
Должность _____
Фамилия, имя, отчество _____
с «__»_____ 201__г. по «__»_____201__г.

в соответствии с Программой, утвержденной председателем комиссии _____ прошел(ла) подготовку к самостоятельной работе со средствами криптографической защиты информации (далее – СКЗИ) количество часов (29) и сдал(а) зачет с общей оценкой (_____).

По решению комиссии _____ допущен(а) к самостоятельной работе с СКЗИ.

Специалист несет персональную ответственность за

– за правильность эксплуатации и сохранность СКЗИ носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями;

– сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с СКЗИ;

– сохранение в тайне содержания закрытых ключей СКЗИ и средств ЭП;

– утрату и некорректность эксплуатации СКЗИ и закрытых ключей;

– в случае несвоевременного сообщения о факте компрометации ключей Специалист, допустивший компрометацию ключей, несет ответственность в полном объеме за ущерб, причиненный им другим Пользователям Системы.

В случае неисполнения или ненадлежащего выполнения требований «Порядка по работе со средствами криптографической защиты информации в *ПНО (ПП)*» Пользователь ключа может быть привлечен к дисциплинарной и/или административной ответственности в соответствии с действующим Законодательством Российской Федерации.

Председатель комиссии: Артюшкина Е.В

Члены комиссии: Шевич Н.А.

Балакирева О.В.

Приложение 19
к распоряжению Администрации района
от 27.08.2020 № 607

ФОРМА
журнала технического (аппаратного)
в Администрации Волчихинского района

Начат «____» _____ 202_ г.
Окончен «____» _____ 202_ г.
На _____ листах

N п/п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ, в которую введены криптографические ключи	Дата	Подпись пользователя СКЗИ	
1	2	3	4	5	6	7	8	9	10