Администрация сельского поселения «Вотча»

«Волея» сикт овмöдчöминса администрация

ПОСТАНОВЛЕНИЕ
ШУÖМ

от 12 января 2015 года

№ 1/1

с.Вотча, Республика Коми

Об утверждении Инструкций, определяющих политику в отношении обработки персональных данных и мер управления и контроля СКЗИ

В соответствии с требованиями Федерального закона 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», Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,

Администрация сельского поселения «Вотча» ПОСТАНОВЛЯЕТ:

1. Утвердить:

1) Инструкцию пользователя по работе с персональными данными согласно приложению № 1;

2) Инструкцию пользователя локально-вычислительной сети (корпоративной сети) согласно приложению № 2;

3) Инструкцию ответственного за организацию обработки персональных данных согласно приложению № 3;

4) Инструкцию пользователя по обращению со средствами криптографической защиты информации (СКЗИ) согласно приложению № 4;

5) Инструкцию администратора средств криптографической защиты информации (СКЗИ) согласно приложению № 5;

2. Настоящее постановление вступает в силу со дня обнародования.

Глава сельского поселения «Вотча» Е.А. Старцева

Приложение № 1
к постановлению администрации
сельского поселения «Вотча»
от 12 января 2015 г. № 1/1

ИНСТРУКЦИЯ
пользователя по работе с персональными данными

1. Общие положения

1.1 Настоящая Инструкция определяет общие правила работы работников администрации сельского поселения «Вотча» (далее - Администрация) с документами, содержащими персональные данные субъектов персональных данных.

1.2 Пользователем является каждый работник Администрации, участвующий в рамках своих функциональных обязанностей в процессах обработки (автоматизированной, без использования средств автоматизации) персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, носителям информации и средствам защиты.

1.3 Пользователь в своей работе руководствуется настоящей Инструкцией, Положением о персональных данных и другими документами Администрации, регламентирующих организацию обработки персональных данных.

1.4 Методическое руководство работой пользователя осуществляет ответственный за организацию обработки персональных данных.

2. Термины и определения

2.1 Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации (в том числе служебная информация ограниченного распространения и персональные данные).

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

2.3 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.

2.4 Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.5 Информационная система (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. В настоящей Инструкции под информационной также подразумевается автоматизированная система и информационная система персональных данных.

2.6 Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

2.7 Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.8 Автоматизированное рабочее место (АРМ) – программно-технический комплекс, посредством которого пользователь выполняет свои должностные обязанности (персональный компьютер, ноутбук, терминал и т.п.).

2.9 Несанкционированный доступ (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

2.10 Посторонние лица – лица, которые не имеют права самостоятельного доступа в помещение и (или) не имеют права самостоятельного доступа в ИС и (или) не имеют допуска к персональным данным.

2.11 Средство защиты информации от несанкционированного доступа (СЗИ НСД) – программное, техническое или программно-техническое средство, направленное на предотвращение или существенное затруднение несанкционированного доступа к информации.

3. Обязанности пользователя

3.1 Не разглашать персональные данные, которые будут доверены или станут известны в ходе рабочего процесса во время выполнения должностных (договорных) обязанностей.

3.2 Не сообщать устно или письменно, не передавать в каком-либо виде третьим лицам и не раскрывать публично персональные данные без соответствующего разрешения непосредственного руководителя.

3.3 Знать и выполнять требования законодательных актов Российской Федерации, настоящей Инструкции и других внутренних документов, регламентирующих порядок обработки персональных данных.

3.4 Выполнять на АРМ только те процедуры обработки персональных данных, которые определены должностной инструкцией.

3.5 Знать и соблюдать установленные требования по режиму обработки персональных данных, по учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных.

3.6 Использовать для хранения персональных данных только определенные места хранения и учтенные носители персональных данных.

3.7 Незамедлительно, в кратчайшие сроки, сообщать ответственному за организацию обработки персональных данных об утрате или недостаче носителей информации, ключей от помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению информации, содержащей персональные данные, а также о причинах возможной их утечки (несанкционированного доступа);

3.8 При прекращении трудовых отношений (увольнении) все материальные носители, содержащие персональные данные (флеш-накопители, дискеты,

компакт-диски, документы, черновики, распечатки на принтерах, кино- и фотоматериалы, модели, промышленные образцы и пр.), ключи от помещений, хранилищ, сейфов, личные печати передавать ответственному за организацию обработки персональных данных;

3.9 Использовать информационные ресурсы Администрации и переданные в распоряжение технические средства хранения, обработки и передачи информации исключительно для выполнения порученных работ, должностных (договорных) обязанностей.

3.10 Соблюдать требования Инструкции пользователя локально-вычислительной сети (корпоративной сети).

3.11 Пользователи, имеющие выход в Интернет, обязаны соблюдать правила при работе в сетях связи общего пользования и (или) сетях международного информационного обмена.

3.12 Пользователи, работающие с электронной подписью или использующие шифрование, обязаны соблюдать Инструкцию пользователя по обращению со средствами криптографической защиты информации (СКЗИ).

3.13 Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

3.14 Обо всех выявленных нарушениях, связанных с порядком обработки персональных данных, а так же для получений консультаций по вопросам обработки персональных данных, необходимо обращаться к администратору ИС или ответственному за организацию обработки персональных данных.

4. Пользователям запрещается:

4.1 Нарушать установленные в Администрации правила обработки персональных данных.

4.2 Использовать компоненты программного и аппаратного обеспечения Администрации в неслужебных целях.

4.3 Оставлять свое рабочее место без присмотра, предварительно не заблокировав (штатными средствами операционной системы, либо при помощи штатных средств защиты информации от несанкционированного доступа - при их наличии).

4.4 Оставлять без присмотра или неубранными в хранилища (шкаф, сейф) носители или документы, содержащие персональные данные.

4.5 Записывать и хранить персональные данные на неучтенных носителях информации (оптических дисках, гибких магнитных дисках, флеш-накопителях и т.п.).

4.6 Самовольно изменять состав и конфигурацию используемых программных, аппаратных, программно-аппаратных средств, самовольно устанавливать программное обеспечение, отключать/подключать оборудование или изменять режимы его работы.

4.7 Самовольно подключать АРМ или другие средства к ЛВС Администрации, изменять IP-адрес, MAC-адрес и иные настройки сети АРМ.

4.8 Производить действия, направленные на получение несанкционированного доступа к АРМ и серверам, равно как и любым другим узлам ЛВС Администрации или Интернет, в том числе:
а) действия, направленные на нарушение нормального функционирования элементов сети (компьютеров, другого сетевого оборудования или программного обеспечения);
б) установка программного обеспечения, осуществляющего перехват информации (информационных пакетов), адресованной другим пользователям;
в) действия, направленные на получение несанкционированного доступа к информационным ресурсам, в последующем использовании такого доступа;
г) уничтожение, модификация программного обеспечения или данных без согласования с непосредственным руководителем или владельцами этого ресурса;
д) попытки подбора паролей к любым информационным ресурсам методом перебора всех возможных вариантов паролей, либо атак по словарю;
е) умышленные действия по созданию, использованию и распространению вредоносных программ, в том числе направленных на получение несанкционированного доступа к любым информационным и служебным ресурсам (как внутри Администрации так и вне), либо на нарушение целостности и работоспособности этих систем;
ж) действия по сканированию локальной сети с целью определения ее внутренней структуры, списков открытых портов, наличия существующих сервисов и уязвимостей.

4.9 Самовольно изменять параметры средств защиты информации (в том числе и средств антивирусной защиты), а также завершать их работу и (или) самостоятельно их устанавливать.

4.10 Самостоятельно разрабатывать или использовать нерегламентированное (без разрешения непосредственного руководителя (работника отдела общего обеспечения), не относящиеся к выполнению должностных обязанностей) программное обеспечение.

4.11 Разрешать посторонним лицам работать под своей учетной записью в ИС.

4.12 Пересылать персональные данные по каналам связи в открытом виде, в том числе Интернет, по телефону, факсу, электронной почте и т.п. (без использования средств шифрования).

4.13 Получать доступ к персональным данным с рабочих мест, не оборудованными необходимыми средствами защиты информации.

4.14 Получать доступ к сети Интернет любыми способами, кроме как установленными настоящей Инструкцией, например, при помощи несанкционированно установленных на АРМ модемов и т. п.

4.15 Самовольно создавать совместно используемые сетевые ресурсы (папки общего доступа) на своих компьютерах и файловых серверах, несанкционированно удалять или изменять права доступа к ним.

4.16 В случае возникновения любых механических неисправностей в оборудовании осуществлять самостоятельные попытки их устранения.

4.17 Препятствовать должностным лицам при проведении проверок и служебных расследований, связанных с обеспечением безопасности информации.

4.18 Удалять или искажать программы и файлы с персональными данными и иной важной информацией (например, системной, необходимой для функционирования АРМ, ИС).

4.19 Подключать к ЛВС Администрации личные средства вычислительной техники: ноутбуки, карманные компьютеры, смартфоны и т.п., а так же личные носители и накопители информации.

5. Порядок доступа сотрудников в помещения, предназначенные для обработки персональных данных

5.1 Работники имеют доступ в помещения, предназначенные для работы с персональными данными, в рабочее время без ограничений согласно матрице доступа.

5.2 Присутствие других лиц (другие работники Администрации, субъекты персональных данных и т.д.) в данных помещениях допускается в той мере, в какой этого требуют процессы обработки персональных данных, оказания государственных или муниципальных услуг и исполнения своих должностных обязанностей.

5.3 Уборка помещений выполняется обслуживающим персоналом под контролем работников Администрации согласно матрице доступа.

5.4 В нерабочее время помещения должны опечатываться одним из способов:

а) с помощью пломбиратора и проволоки;

б) с помощью пластилина и пломбира под пластилин;

в) с помощью опечатывающего устройства «под нить» и пломбира под пластилин;

г) с помощью штока и пломбира под пластилин.

5.5 Допускается пребывание в помещениях, предназначенных для обработки персональных данных, работников Администрации в нерабочее время согласно матрицы доступа и при обязательной регистрации в журнале выдачи ключей от помещений в выходные и нерабочие дни.

6. Ответственность

6.1 За неисполнение возложенных настоящей Инструкцией функций и требований лицо, имеющее доступ к документам, содержащих персональные данные субъектов персональных данных и имеющего доступ к аппаратным средствам, программному обеспечению, носителям информации и средствам защиты, содержащих персональные данные, несет персональную ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение № 2
к постановлению администрации
сельского поселения «Вотча»
от 12 января 2015 г. № 1/1

ИНСТРУКЦИЯ
пользователя локально-вычислительной сети (корпоративной сети)

1. Общие положения

1.1 Настоящая Инструкция определяет общие правила работы работников администрации сельского поселения «Вотча» (далее - Администрация) в локально-вычислительной сети Администрации и устанавливает единые требования по использованию компьютерного оборудования с целью повышения эффективности и предотвращения ненадлежащего использования этого оборудования.

1.2 Пользователем является каждый работник Администрации, в том числе и участвующий в рамках своих функциональных обязанностей в процессах обработки (автоматизированной, без использования средств автоматизации) персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, носителям информации и средствам защиты.

1.3 С целью оперативного обеспечения пользователей Администрации вычислительными и информационными ресурсами определен круглосуточный режим работы серверов, включая выходные и праздничные дни.

1.4 Пользователь в своей работе руководствуется настоящей Инструкцией, Положением о персональных данных и другими документами Администрации по информационной безопасности.

2. Термины и определения

2.1 Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации (в том числе служебная информация ограниченного распространения и персональные данные).

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

2.3 Локальная вычислительная сеть (ЛВС) – компьютерная сеть, объединяющая в единую информационную систему вычислительные ресурсы всех компьютеров и рабочих станций, использующихся в Администрации. ЛВС Администрации, является составной частью КСПД органов государственной власти Республики Коми и имеет непосредственное подключение к ресурсам ГАУ Республики Коми «Центр информационных технологий» по оптоволоконным каналам связи (администрируется специалистами ГАУ Республики Коми «Центр информационных технологий» в рамках своих полномочий).

2.4 Локальная вычислительная сеть, корпоративная сеть (ЛВС) - совокупность компьютеров, кабелей, сетевых адаптеров, работающих под управлением сетевой операционной системы и прикладного программного обеспечения.

2.5 Функционирование ЛВС обеспечивается специализированным оборудованием, называемым сервером (файловый сервер, сервер приложений и контроллер домена).

2.6 Администратор ЛВС – ответственное лицо, работник, отвечающий за стабильное функционирование серверов и компьютерной сети Администрации.

2.7 Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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

2.9 Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

2.10 Автоматизированное рабочее место (АРМ) – программно-технический комплекс, посредством которого пользователь выполняет свои должностные обязанности (персональный компьютер, ноутбук, терминал и т.п.).

2.11 Компьютерное оборудование (оборудование, техника, периферия) – это серверы, рабочие станции, персональные компьютеры, ноутбуки, нетбуки, КПК, терминалы, принтеры, сканеры, источники бесперебойного питания, маршрутизаторы, коммутаторы, модемы и прочее.

3. Обязанности и права пользователя

3.1 Пользователи обязаны:

а) ознакомиться с настоящей Инструкцией до начала работы с АРМ;

б) пройти регистрацию, инструктаж и получить личные атрибуты доступа (имя, пароль) для работы с оборудованием (в том числе с ограниченным доступом);

в) устанавливать личный пароль доступа (если пользователю предоставлена возможность) в соответствии с правилами компьютерной безопасности (п.7 настоящей Инструкции);

г) использовать АРМ исключительно для исполнения своих должностных обязанностей;

д) бережно относится к составу АРМ, соблюдать правила его эксплуатации;

е) сообщать Администратору ЛВС о замеченных неисправностях АРМ и недостатках в работе общего и специального программного обеспечения;

ж) рационально пользоваться ограниченными разделяемыми ресурсами (дисковой памятью компьютеров общего пользования (сервера), пропускной способностью ЛВС) и расходными материалами;

з) выполнять законные требования Администратора ЛВС;

и) предоставлять доступ к АРМ Администратору ЛВС для проверки исправности и соответствия установленным правилам работы;

к) сообщать о замеченных случаях нарушения компьютерной безопасности (несанкционированный доступ к оборудованию и информации, несанкционированное искажение или уничтожение информации,

несанкционированный доступ к персональным данным или к информационным системам персональных данных и т.д.);
л) использовать информационные ресурсы Администрации и переданные в распоряжение технические средства хранения, обработки и передачи информации исключительно для выполнения порученных работ, должностных (договорных) обязанностей;
м) соблюдать требования парольной политики (п.7 настоящей Инструкции);
н) соблюдать требования антивирусной защиты (Положение об антивирусной защите);
о) пользователи, имеющие выход в Интернет, обязаны соблюдать правила при работе в сетях связи общего пользования и (или) сетях международного информационного обмена;
п) пользователи, работающие с электронной подписью или использующие шифрование, обязаны соблюдать Инструкцию пользователя по обращению со средствами криптографической защиты информации (СКЗИ).

3.2 Пользователям запрещается:
а) использовать программное обеспечение, АРМ и оборудование для деятельности, не обусловленной необходимостью и должностной инструкцией;
б) создавать помехи работе других пользователей, помехи работе компьютеров и сети;
в) включать и выключать оборудование общего пользования, переключать, перемещать, разбирать, изменять конфигурацию АРМ и другого оборудования, кроме случаев прямого указания Администратора ЛВС или ответственного лица (исключения - пожарная опасность, дым из оборудования, или других угроз жизни и здоровью людей, или угроз сохранности имущества);
г) подключать к ЛВС новые компьютеры и оборудование без регистрации и ознакомления Администратора ЛВС;
д) передавать другим лицам свои личные атрибуты доступа (регистрационное имя и пароль) к АРМ, ЛВС, общему и программному обеспечению, информационным ресурсам Администрации;
е) осуществлять доступ к АРМ и ЛВС с использованием чужих личных атрибутов доступа или с использованием чужого сеанса работы;
ж) удалять файлы других пользователей на серверах;
з) осуществлять попытку несанкционированного доступа к компьютерному оборудованию и информации хранящейся на АРМ пользователей и передаваемой по ЛВС;
и) использовать, распространять и хранить программы, предназначенные для осуществления несанкционированного доступа, взлома паролей, для нарушения функционирования компьютерного оборудования и ЛВС, а также компьютерные вирусы и
любые программы ими инфицированные,
к) использовать, распространять и хранить программы сетевого управления, мониторинга и удаленного доступа без специального разрешения Администратора ЛВС;
л) предоставлять доступ к АРМ и ЛВС незарегистрированным пользователям.

3.3. Права пользователей (с обязательным обоснованием и через администратора ЛВС):

а) подавать заявку на получение права доступа к оборудованию и программному обеспечению;
б) подавать заявку на выделение и модернизацию компьютерного оборудования (АРМ пользователя) персонального пользования;
в) вносить предложения по установке бесплатного и приобретению коммерческого программного обеспечения;
г) вносить предложения по приобретению компьютерного оборудования;
д) вносить предложения по улучшению настроек оборудования и программного обеспечения, по улучшению условий труда;
е) вносить предложения по изменению настоящей Инструкции;

4. Пользователям запрещается:

4.1 Оставлять свое рабочее место (АРМ) без присмотра.

4.2 Самовольно подключать АРМ или другие средства к ЛВС Администрации, изменять IP-адрес, MAC-адрес и иные настройки сети АРМ.

4.3 Производить действия, направленные на получение несанкционированного доступа к АРМ и серверам, равно как и любым другим узлам ЛВС Администрации или Интернет, в том числе:
а) действия, направленные на нарушение нормального функционирования элементов сети (компьютеров, другого сетевого оборудования или программного обеспечения);
б) установка программного обеспечения, осуществляющего перехват информации (информационных пакетов), адресованной другим пользователям;
в) действия, направленные на получение несанкционированного доступа к информационным ресурсам, в последующем использовании такого доступа;
г) уничтожение, модификация программного обеспечения или данных без согласования с непосредственным руководителем или владельцами этого ресурса;
д) попытки подбора паролей к любым информационным ресурсам методом перебора всех возможных вариантов паролей, либо атак по словарю;
е) умышленные действия по созданию, использованию и распространению вредоносных программ, в том числе направленных на получение несанкционированного доступа к любым информационным и служебным ресурсам (как внутри Администрации так и вне), либо на нарушение целостности и работоспособности этих систем;
ж) действия по сканированию локальной сети с целью определения ее внутренней структуры, списков открытых портов, наличия существующих сервисов и уязвимостей.

4.4 Самовольно изменять параметры средств защиты информации (в том числе и средств антивирусной защиты), а также завершать их работу и (или) самостоятельно их устанавливать.

4.5 Самостоятельно разрабатывать или использовать нерегламентированное (без разрешения непосредственного руководителя и Администратора ЛВС, не относящиеся к выполнению должностных обязанностей) программное обеспечение.

4.6 Разрешать посторонним лицам работать под своей учетной записью в ИС.

4.7 Пересылать персональные данные по каналам связи в открытом виде, в том числе Интернет, по телефону, факсу, электронной почте и т.п. (без использования средств шифрования).

4.8 Получать доступ к персональным данным с рабочих мест, не оборудованными необходимыми средствами защиты информации.

4.9 Получать доступ к сети Интернет любыми способами, кроме как установленными настоящей Инструкцией, например, при помощи несанкционированно установленных на АРМ модемов и т. п.

4.10 Самовольно создавать совместно используемые сетевые ресурсы (папки общего доступа) на своих компьютерах и файловых серверах, несанкционированно удалять или изменять права доступа к ним.

4.11 В случае возникновения любых механических неисправностей в оборудовании осуществлять самостоятельные попытки их устранения.

4.12 Препятствовать должностным лицам при проведении проверок и служебных расследований, связанных с обеспечением безопасности информации.

4.13 Удалять или искажать программы и файлы с персональными данными и иной важной информацией (например, системной, необходимой для функционирования АРМ, ИС).

4.14 Подключать к ЛВС Администрации личные средства вычислительной техники: ноутбуки, карманные компьютеры, смартфоны и т.п., а так же личные носители и накопители информации.

5. Регистрация пользователей и оборудования

5.1. Регистрация (установка) нового оборудования подключаемого к ЛВС производится только Администратором ЛВС.

5.2. Регистрация нового пользователя производится только Администратором ЛВС, по согласованию с главой сельского поселения «Вотча».

6. Обязанности и права Администратора ЛВС

6.1 Обязанности:

а) совершенствовать работу оборудования и программного обеспечения для повышения эффективности выполнения пользователями их служебных обязанностей;

б) предоставлять пользователям информацию необходимую для работы на компьютерном оборудовании;

в) доводить до сведения пользователей информацию об изменении правил или режима работы оборудования (АРМ);

г) снижать до минимально необходимого время простоя оборудования из-за неполадок и сервисных работ;

д) проводить среди пользователей разъяснительную работу по вопросам компьютерной безопасности;

е) доводить до сведения пользователей правила работы на конкретном компьютерном оборудовании;

ж) не разглашать информацию (в том числе содержащую персональные данные субъектов персональных данных), полученную в ходе выполнения должностных обязанностей и не имеющую прямого отношения к выполняемым обязанностям.

6.2 Права:

а) делать замечания и предупреждения пользователям, нарушившим установленные правила работы;

б) требовать от пользователя подробного отчета о работе, если во время этой работы произошел отказ или сбой оборудования или программного обеспечения;

в) требовать обоснования необходимости выделения пользователю ограниченных ресурсов или расходных материалов сверх среднего запланированного уровня;

г) проверять исправность компьютеров подключенных к ЛВС, правильность настройки сетевых программ и соблюдение правил работы, с использованием, при необходимости, административного доступа к АРМ на время проверки;

д) оперативно отключать от сети, блокировать работу или выводить из эксплуатации оборудование в случае нарушения компьютерной безопасности, по причине неисправности или грубого нарушения правил работы;

е) в экстренной ситуации, для обеспечения бесперебойной работы ЛВС и компьютеров, осуществлять отключение оборудования в отсутствии пользователя и без предварительного уведомления;

ж) без предупреждения удалять с дисков компьютеров, серверов файлы пользователей содержащие игровые программы и программы, предназначенные для нарушения компьютерной безопасности, файлы зараженные компьютерными вирусами, файлы содержащие мультимедийную информацию и другую информацию, не имеющую отношения к деятельности предприятия.

7. Парольная политика

7.1 Общие положения:

а) Минимальное требование: буквенно-цифровой пароль. Желательно использовать буквы в верхнем или нижнем регистрах, цифры или специальные символы (например: ~ ! @ # $ % ^ & * ( ) _ - + = | \ ? / . , : ; ’] [{ } < > . и т.п.);

б) Минимальная длина пароля: не менее 8 (восьми) символов;

в) Максимальный срок действия пароля: 30 суток;

г) Запрет использования трех ранее использовавшихся паролей;

д) Пароль пользователя не должен включать в себя легко вычисляемые сочетания символов, общепринятые сокращения, имена, фамилии, должности, год рождения, номер паспорта, табельный номер, иную информацию о пользователе, доступную другим лицам;

е) Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

ж) Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например: 1234567, qwerty и т.п.);

7.2 Правила использования паролей:

а) хранить в тайне свой пароль, не сообщать его другим лицам;

б) не давать доступ в ИС другим лицам под своей учетной записью и паролем;
в) изменять свой пароль при первом требовании политики паролей операционной системы или ИС;
г) во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.);
д) немедленно сообщить Администратору (Оператору) ИС об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей;
е) запрещается записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе АРМ, на обратной стороне клавиатуры и т.д;
ж) запрещается хранить пароли в записанном виде на отдельных листах бумаги.

7.3 Смена, удаление личного пароля любого пользователя производится в следующих случаях:
а) в случае подозрения на компрометацию пароля;
б) по окончании срока действия;
в) в случае прекращения полномочий (увольнение, переход на другую работу внутри Администрации) пользователя после окончания последнего сеанса работы в информационных системах;
г) по указанию Администратора (Оператора) ИС или ответственного за организацию обработки персональных данных.

7.4 Для создания значений паролей могут применяться специальные программные средства (генераторы паролей).

8. Антивирусная защита

8.1 В своей работе пользователь Администрации обязан выполнять требования Положения об антивирусной защите.

8.2 В случае отсутствия штатных функций антивирусной программы, предусматривающих автоматическую проверку файлов, пользователь обязан осуществлять проверку файлов получаемых:
а) по электронной почте;
б) через сеть Интернет;
в) на магнитном, оптическом диске, флеш–накопителе;
г) ином съемном носителе информации;
д) полученные иным способом.

8.3 Пользователю запрещается:
а) осуществлять действия, направленные на выключение антивирусной программы;
б) самостоятельно устанавливать на АРМ программное обеспечение;
в) запускать файлы, полученные по сетям связи (электронной почте, Интернет), со съемных носителей, даже если они получены проверенного адресата, без предварительной их проверки антивирусной программой;

8.4 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно или вместе с

ответственным за антивирусную защиту должен провести внеочередной антивирусный контроль своего рабочего места.

8.5 В случае обнаружения при проведении антивирусной проверки вирусного заражения пользователи обязаны:

а) приостановить работу;

б) немедленно поставить в известность о факте обнаружения вирусного заражения ответственного за антивирусную защиту (или Администратора ЛВС);

в) совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

г) провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь ответственного за антивирусную защиту).

9. Порядок работы в сети Интернет

9.1 Использование пользователями Администрации сети Интернет должно осуществляться исключительно для выполнения должностных обязанностей.

9.2 Информация, образованная (образующаяся) в процессе трудовой деятельности пользователя Администрации является собственностью Администрации и не подлежит использованию (в том числе использованию в сети Интернет или с помощью сети Интернет) в личных целях и (или) в корыстных интересах других лиц (организаций).

9.3 Вся информация о ресурсах, посещаемых сотрудниками Администрации, протоколируется и, при необходимости, может быть предоставлена главе администрации сельского поселения «Визинга» для детального изучения и принятия решения о мерах дисциплинарной ответственности.

9.4 При работе в сети Интернет пользователям запрещается:

а) умышленное распространение и получение материалов в/из сети Интернет, противоречащих законодательству Российской Федерации, в том числе материалов, пропагандирующих насилие или экстремизм; разжигающих расовую, национальную или религиозную вражду; разъясняющих порядок изготовления и/или применения наркотиков, взрывчатых веществ, оружия и т. п.; материалов порнографического характера; компьютерных вирусов и других вредоносных программ;

б) передавать в сеть Интернет информацию, к которой в соответствии с законодательством ограничен доступ (персональные данные, служебная информация) без соответствующего разрешения;

в) фальсифицировать IP-адрес, MAC-адрес, иные адреса, используемые в сетевых протоколах, а также прочую служебную информацию при передаче данных через сеть Интернет.

г) предоставлять доступ в сеть Интернет со своей рабочей станции кому-либо, в том числе программно-техническими способами через локальную вычислительную сеть Администрации (например: путем несанкционированной установки локального Интернет-шлюза на рабочую станцию);

д) получать доступ к сети Интернет любыми способами, не предусмотренными действующими локальными документами (Инструкциями, стандартами Учреждения, положениями, регламентами);

е) осуществлять несанкционированный доступ к ресурсам и сервисам сети Интернет.
ж) выполнять действия (взлом, DoS (отказ в обслуживании), ARP-spoofing атаки, сканирование локальной вычислительной сети) направленные на нарушение функционирования элементов сети Интернет (коммуникационного оборудования, серверов, рабочих станций, программного обеспечения).

10. Правила работы пользователей с электронной почтой

10.1 В своей работе пользователь Администрации обязан выполнять требования Положения о системе электронной почты.

10.2 Пользователи обязаны использовать электронную почту только для выполнения служебных обязанностей.

10.3 Запрещается отправлять файлы, содержащие персональные данные в открытом виде (не зашифрованные).

10.4 Запрещается массовая рассылка почтовых сообщений (более 100) внешним адресатам без согласования с руководством Администрации (спама).

10.5 Запрещается использовать не свой обратный адрес при отправке электронной почты.

10.6 Запрещается отправлять по электронной почте исполняемые файлы (обычно имеют расширения exe, com, bat, js, vbs и т.п.). В случае необходимости отправки таких файлов, помещать их в архив.

10.7 Присоединяемые файлы рекомендуется упаковывать в архив при помощи программ-архиваторов.

11. Порядок работы со съемными носителями информации

11.1 Под использованием носителей информации в ИС Администрации понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между информационными системами и носителями информации.

11.2 При использовании носителей информации необходимо использовать носители информации исключительно для выполнения своих служебных обязанностей, бережно относится к носителям персональных данных.

11.3 При использовании носителей, содержащих персональные данные, запрещено:
а) использовать носители в личных целях;
б) кратковременно передавать носители другим лицам;
в) хранить съемные носители на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
г) выносить съемные носители из служебных помещений для работы с ними на дому и т. д.

12. Порядок доступа пользователей в помещения, предназначенные для обработки персональных данных

12.1 Пользователи имеют доступ в помещения, предназначенные для работы с персональными данными, в рабочее время без ограничений согласно матрице доступа.

12.2 Присутствие других лиц (пользователи Администрации вне матрицы доступа, субъекты персональных данных и т.д.) в данных помещениях допускается в той мере, в какой этого требуют процессы обработки персональных данных, оказания государственных и муниципальных услуг и исполнения своих должностных обязанностей.

12.3 Уборка помещений выполняется обслуживающим персоналом под контролем пользователей Администрации согласно матрице доступа.

12.4 В нерабочее время помещения должны опечатываться одним из способов:

а) с помощью пломбиратора и проволоки;

б) с помощью пластилина и пломбира под пластилин;

в) с помощью опечатывающего устройства «под нить» и пломбира под пластилин;

г) с помощью штока и пломбира под пластилин.

12.5 Допускается пребывание в помещениях, предназначенных для обработки персональных данных, пользователей Администрации в нерабочее время согласно матрицы доступа и при обязательной регистрации в журнале выдачи ключей от помещений в выходные и нерабочие дни.

13. Ответственность

13.1 За неисполнение возложенных настоящей Инструкцией функций и требований пользователь Администрации несет персональную ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение № 3
к постановлению администрации
сельского поселения «Вотча»
от 12 января 2015 г. № 1/1

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных

1. Общие положения

1.1 Лицо, ответственное за организацию обработки персональных данных (далее – Ответственный), назначается и смещается распоряжением администрации (далее - Администрация), в соответствии со ст. 22.1 и 18.1 Федерального закона от 27.06.2006 ФЗ-№ 152 «О персональных данных».

1.2 Ответственный подчиняется главе сельского поселения «Вотча».

1.3 В своей деятельности Ответственный руководствуется:

1) действующим законодательством Российской Федерации;
2) Уставом администрации сельского поселения «Вотча»;
3) локальными документами Администрации, регламентирующих организацию обработки персональных данных;
4) настоящей Инструкцией.

2. Задачи

2.1 Разработка и осуществление мероприятий по обеспечению безопасности персональных данных при их обработке в Администрации.

3. Функции

3.1 Организация внедрения организационных и технических мероприятий по комплексной защите персональных данных.

3.2 Организация обеспечения соблюдения режима работ и сохранение конфиденциальности персональных данных.

3.3 Организация обеспечения конфиденциальности обсуждений, бесед, совещаний в которых присутствуют персональные данные.

3.4 Организация разработки проектов текущих планов по обеспечению защиты персональных данных.

3.5 Организация, координация и выполнение работ по защите информации в пределах компетенции.

3.6 Организация подготовки проектов договоров на работы по защите персональных данных с участием юридической службы Администрации.

3.7 Проверка готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации.

3.8 Организация установки и ввода в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией.

3.9 Организация обучения работников Администрации, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними.

3.10 Контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

3.11 Разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

3.12 Организация разработки и реализации мер по устранению выявленных недостатков по защите информации в пределах компетенции.

3.13 Контроль выявления нарушений требований по защите информации работниками Администрации.

3.14 Организация работ по информированию работников Администрации о положениях законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

3.15 Организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов.

3.16 Осуществление всех выше изложенных функций по организации организационной и технической защиты информации, может быть возложено на стороннюю организацию, имеющую лицензию ФСТЭК России на право осуществления деятельности по технической защите конфиденциальной информации (персональных данных).

4. Права

4.1 Осуществлять контроль за деятельностью Администрации по выполнению ими требований по защите информации.

4.2 По согласованию с главой Администрации привлекать других работников Администрации для помощи в организации обработки персональных данных в Администрации.

4.3 Давать работникам Администрации обязательные для исполнения указания по вопросам, входящим в компетенцию Ответственного.

4.4 Запрашивать и получать сведения, справочные материалы, необходимые для осуществления деятельности Ответственного.

4.5 Подготавливать материалы для переписки с государственными и муниципальными органами по правовым вопросам.

4.6 Принимать необходимые меры при обнаружении несанкционированного доступа к информации, как внутри Администрации, так и извне, и докладывать о принятых мерах главе Администрации с предоставлением информации о субъектах, нарушивших режим доступа.

4.7 По согласованию с главой Администрации привлекать специалистов в сфере информационной безопасности для консультаций, подготовки заключений, рекомендаций и предложений.

5. Ответственность

5.1 За неисполнение возложенных настоящей Инструкцией функций и требований лицо, ответственное за организацию обработки персональных данных несет персональную ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение № 4
к постановлению администрации
сельского поселения «Вотча»
от 12 января 2015 г. № 1/1

ИНСТРУКЦИЯ
пользователя по обращению со средствами криптографической защиты информации (СКЗИ)

1.Общие положения

1.1 Настоящая Инструкция определяет:

а) порядок обращения со средствами криптографической защиты информации (далее – СКЗИ) и криптографическими ключами;

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

в) действия при компрометации ключей и восстановлении конфиденциальной связи;

г) специальные требования по обработке информации с использованием СКЗИ;

1.2 Пользователь должен выполнять все требования настоящей Инструкции, правила, изложенные в эксплуатационной документации на СКЗИ, а также другие документы, регламентирующие порядок работы с СКЗИ.

1.3 Деятельность Пользователя по вопросам обращения со СКЗИ контролируется непосредственным работником Администрации (далее – Администратор СКЗИ).

1.4 Администратор СКЗИ назначается и смещается распоряжением Администрации. Обязанности, права и ответственность Администратора СКЗИ устанавливаются отдельным нормативным актом Администрации.

1.5 СКЗИ и средства ЭЦП могут использоваться для защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.

2. Основные обязанности Пользователя

2.1. Пользователь обязан:

а) соблюдать требования по обеспечению безопасности функционирования СКЗИ;

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

в) сдать Администратору СКЗИ носители ключевой информации (далее – НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

г) сдать Администратору СКЗИ НКИ по окончании срока действия сертификата ключа, а также в случае компрометации ключа;

д) немедленно уведомлять главу сельского поселения «Вотча» и Администратора СКЗИ о случаях компрометации криптографических ключей;

е) немедленно уведомлять главу сельского поселения «Вотча» и Администратора СКЗИ о фактах утраты или недостачи СКЗИ, НКИ;

ж) в пределах своей компетенции предоставлять информацию комиссии, проводящей служебные расследования по фактам компрометации, а также выявлению причин нарушения требований безопасности функционирования СКЗИ.

3. Права Пользователя

3.1. Пользователь имеет право:

а) вносить предложения по совершенствованию СКЗИ;

б) повышать уровень квалификации по использованию СКЗИ.

4. Порядок обращения со СКЗИ

4.1 Монтаж и установка СКЗИ осуществляются уполномоченным лицом – Администратором СКЗИ или представителем оператора безопасности Республики Коми - ГБУ Республики Коми «Центр безопасности информации».

4.2 Служебные помещения (кабинеты), в которых размещаются СКЗИ, должны отвечать всем требованиям по оборудованию и охране, предъявляемым к помещениям, выделенным для работы с конфиденциальной информацией. Для хранения носителей ключевой информации помещения обеспечиваются запираемыми шкафами, сейфами (металлическими шкафами), по убытию работников закрываются и опломбируются.

4.3 К эксплуатации СКЗИ допускаются работники, прошедшие соответствующую подготовку и изучившие правила пользования СКЗИ и НКИ, изложенные в настоящей Инструкции.

4.4 Все программное обеспечение АРМ, предназначенное для установки СКЗИ, должно иметь соответствующие лицензии. Установка средств разработки и отладки программ на АРМ, использующее СКЗИ, не допускается.

5. Использование ЭЦП

5.1 Электронная цифровая подпись (далее - ЭЦП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

5.2 Сертификат ключа подписи – документ на бумажном носителе или электронный документ с ЭЦП Удостоверяющего центра, которые включают в себя открытый ключ ЭЦП и которые выдаются Удостоверяющим центром участнику информационной системы для подтверждения подлинности ЭЦП и идентификации Владельца сертификата ключа подписи. Сертификат ключа подписи хранится у Владельца с соблюдением требований безопасности.

5.3 Владелец сертификата ключа подписи – физическое лицо, на имя которого Удостоверяющим центром выдан сертификат ключа подписи и

которое владеет соответствующим закрытым ключом ЭЦП, позволяющим с помощью средств ЭЦП создавать свою ЭЦП в электронных документах (подписывать электронные документы).

5.4 Подтверждение подлинности ЭЦП в электронном документе – положительный результат проверки соответствующим сертифицированным средством ЭЦП с использованием сертификата ключа подписи принадлежности ЭЦП в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

5.5 ЭЦП в электронном документе равнозначна собственноручной подписи владельца ключа в документе на бумажном носителе при одновременном соблюдении следующих условий:

а) сертификат ключа подписи, относящийся к этой ЭЦП, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

б) подтверждена подлинность электронной цифровой подписи в электронном документе;

в) электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

6. Порядок обращения с ключами ЭЦП

6.1 Криптографический ключ Владельца ключа применяется для подписания (проверки ЭЦП) электронных документов до окончания срока его действия или наступления события, трактуемого как компрометация криптоключей.

6.2 Владелец ЭЦП – Пользователь СКЗИ, получивший установленным порядком право использовать персональный ключ ЭЦП для удостоверения содержания электронных документов и своего авторства.

6.3 Доверенное лицо Владельца ЭЦП – пользователь СКЗИ, получивший установленным порядком право использовать ключ Владельца ЭЦП для удостоверения содержания электронных документов и авторства Владельца.

6.4 Назначение владельцев ЭЦП и доверенных лиц осуществляется на основании распоряжения Администрации о назначении пользователей СКЗИ.

6.5 Подготовку документации (подача заявки) для изготовления ключей ЭЦП осуществляется работником отдела общего обеспечения – Администратором СКЗИ. Получение ключа ЭЦП в Удостоверяющем центре выполняет лично Владелец ЭЦП или доверенное лицо Владельца ЭЦП.

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

6.7 НКИ являются объектами особой важности, т.к. они содержат информацию, предназначенную для гарантированной идентификации Владельца ключа, защиты электронного документа от подделки, компрометации.

6.8 Владельцы ключей (доверенные лица Владельца) несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту НКИ от несанкционированного использования.

6.9 Для хранения носителей ключевой информации Пользователь должен быть обеспечен запираемым шкафом, сейфом (металлическими шкафами).

6.10 Пользователю категорически запрещается:

а) осуществлять несанкционированное и безучётное копирование ключевых данных;

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

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

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

д) хранить на НКИ какую-либо информацию, кроме ключевой;

е) использование криптоключей, выведенных из действия;

ж) разглашать содержимое НКИ;

з) вносить какие-либо изменения в программное обеспечение СКЗИ и средств ЭЦП;

и) вставлять НКИ в интерфейс АРМ при проведении работ, не являющихся штатными процедурами использования ключей(шифрование/расшифровывание информации, проверка ЭЦП и т.д.), а также в интерфейсы других АРМ.

6.11 Запрещается использовать НКИ на АРМ с не установленными программными средствами антивирусной защиты.

7. Действия при компрометации действующих ключей и восстановлении конфиденциальной связи

7.1 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:

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

б) увольнение (переназначение) сотрудников, имевших доступ к ключевой информации;

в) передача секретных ключей по линии связи в открытом виде;

г) нарушение правил хранения криптоключей;

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

е) отрицательный результат при проверке наложенной ЭЦП;

ж) несанкционированное или безучётное копирование ключевой информации;

з) 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).

7.2 События 7.1.(а-д) должны трактоваться как безусловная компрометация действующих ключей. Остальные события требуют специального расследования в каждом конкретном случае.

7.3 При наступлении любого из перечисленных в п. 7.1 событий Владелец ключа должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации главе сельского поселения «Вотча» или Администратору СКЗИ.

7.4 При подтверждении факта компрометации действующих ключей Пользователь обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей.

7.5 Для восстановления конфиденциальной связи, после компрометации действующих ключей, на Пользователя оформляются новые ключи ЭЦП.

8. Ответственность Пользователя

8.1. Владелец ключа несет персональную ответственность за обеспечение конфиденциальности личных ключевых носителей.

8.2 В случае неисполнения или ненадлежащего выполнения требований настоящей Инструкции Пользователь ключа может быть привлечен к дисциплинарной и/или административной ответственности в соответствии с действующим законодательством Российской Федерации.

Приложение
к инструкции пользователя по обращению
со средствами криптографической
защиты информации (СКЗИ)

п/п	Нештатная ситуация	Действие работника
1.	Эвакуация, угроза взрыва или нападения, стихийные бедствия и т.д.	- Остановить ПЭВМ. - Сдать все имеющиеся ключевые носители администрации или администратору СКЗИ. - Администратор СКЗИ упаковывает все ключевые носители, регистрационные карточки открытых ключей в опечатываемый контейнер, который выносит в безопасное помещение/здание. - Администратор СКЗИ оповещает всех пользователей о приостановки работы. - В случае наступления события, повлекшего за собой долговременный выход из строя аппаратный средств, администратор СКЗИ уничтожает все ключевые носители, находящиеся в опечатываемом контейнере.
2.	Компрометация одного из личных ключевых носителей.	Смотри п.7 настоящей инструкции.
3.	Утеря личного носителя ключевой информации.	Смотри п.7 настоящей инструкции.
4.	Выход из строя личного основного ключевого носителя (дискета).	- Сообщить администратору СКЗИ о выходе из строя ключевого носителя. - Обеспечить доставку основного ключевого носителя администратору СКЗИ для выяснения причин выхода его из строя. - Для работы использовать резервный ключевой носитель.
5.	Выход из строя личного резервного ключевого носителя (дискета).	- Сообщить администратору СКЗИ о выходе из строя резервного ключевого носителя. - Обеспечить доставку резервного ключевого носителя администратору СКЗИ для выяснения причин выхода его из строя. - Получение от администратора СКЗИ дубликата резервной копии ключевого носителя.
6.	Отказы и сбои в работе аппаратной части АРМ со встроенным СКЗИ.	Необходимо остановить работу, по возможности локализовать неисправность и выполнить ремонт. При необходимости переустановить СКЗИ.
7.	Отказы и сбои в	Необходимо остановить работу, по возможности

	работе программных средств.	локализовать неисправность. Устранить причину отказа ПО. При необходимости переустановить СКЗИ.
8.	Отказы в работе программных средств вследствие случайного или умышленного их повреждения.	Администратор СКЗИ инициирует проведение служебного расследования по факту умышленного или случайного повреждения ПО с целью установления причин отказа. Выполнение работ по восстановлению работоспособности ПО.

Приложение № 5
к постановлению администрации
сельского поселения «Вотча»
от 12 января 2015 г. № 1/1

ИНСТРУКЦИЯ

администратора средств криптографической защити информации (СКЗИ)

1. Термины и определения

1.1 В настоящей Инструкции по эксплуатации средств криптографической защиты информации в Администрации применяются следующие термины и определения:

а) безопасность эксплуатации СКЗИ - совокупность мер управления и контроля, защищающая СКЗИ и криптографические ключи от несанкционированного (умышленного или случайного) их раскрытия, модификации, разрушения или использования;

б) Администратор (ответственный за эксплуатацию) СКЗИ – работник, осуществляющий организацию и обеспечение работ по техническому обслуживанию СКЗИ и управление криптографическими ключами (далее – Администратор СКЗИ).

в) Пользователь СКЗИ – работник Администрации, который использует СКЗИ;

г) средства криптографической защиты информации (СКЗИ) - совокупность программно-технических средств, обеспечивающих применение шифрования при осуществлении электронного документооборота, в том числе программное обеспечение с реализацией криптографических функций.

2. Общие положения

2.1 Настоящая Инструкция определяет:

а) порядок учета, хранения и использования СКЗИ и криптографических ключей, а также порядок их изготовления, смены, уничтожения в целях обеспечения безопасности эксплуатации СКЗИ;

б) обязанности, права и ответственность Администратора СКЗИ.

2.2 Все действия с СКЗИ осуществляются в соответствии с эксплуатационной и технической документацией на СКЗИ.

2.3 Методическая и техническая поддержка осуществляется оператором безопасности Республики Коми – ГБУ РК «Центр безопасности информации» (далее - Оператор).

2.4 Администратор СКЗИ назначается и смещается распоряжением администрации.

3. Основные обязанности Администратора СКЗИ

3.1 Администратор СКЗИ обязан:

а) вести поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним;

б) вести учет Пользователей СКЗИ;

в) осуществлять контроль за соблюдением условий использования СКЗИ в соответствии с эксплуатационной и технической документацией на СКЗИ и настоящей Инструкцией;

г) вести расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации;

г) осуществлять разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

д) не разглашать конфиденциальную информацию, к которой допущен, рубежи ее защиты, в том числе сведения о криптографических ключах;

е) соблюдать требования к обеспечению безопасности конфиденциальной информации при использовании СКЗИ;

4. Допуск к эксплуатации СКЗИ

4.1 Обучение Пользователей СКЗИ правилам работы с СКЗИ осуществляет Администратор СКЗИ.

4.2 Администратор СКЗИ должен иметь соответствующий документ о квалификации в области эксплуатации СКЗИ.

4.3 Непосредственно к работе с СКЗИ пользователи СКЗИ допускаются после обучения и выдачи соответствующего заключения. Заключение о прохождении тестирования оформляется в 2-х экземплярах. Для получения заключения необходимо зарегистрироваться на сайте Оператора и пройти тестирование на знание правил работы со СКЗИ.

4.4 Администратор СКЗИ должен быть ознакомлен с настоящей Инструкцией под роспись.

5. Учет и хранение СКЗИ и криптографических ключей

5.1 СКЗИ, эксплуатационная и техническая документация к ним, криптографические ключи подлежат поэкземплярному учету.

5.2 Поэкземплярный учет СКЗИ ведет Администратор СКЗИ в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним (далее – Журнал).

5.3 Все полученные экземпляры СКЗИ, криптографических ключей должны быть выданы под роспись в Журнале Пользователям СКЗИ, несущим персональную ответственность за их сохранность. При необходимости Пользователю СКЗИ выдается документация по эксплуатации СКЗИ с последующим возвратом Администратору СКЗИ.

5.4 Дистрибутивы СКЗИ на носителях, эксплуатационная и техническая документация к СКЗИ, инструкции хранятся у Администратора СКЗИ. Криптографические ключи хранятся у Пользователей СКЗИ. Хранение осуществляется в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

5.5 Резервные криптографические ключи находится на хранении у Администратора СКЗИ.

5.6 Ключевые носители подлежат обязательной маркировке (если это возможно) с изготовлением наклейки, содержащей реквизиты регистрации из

Журнала и/или сертификата.

5.7 Неработоспособные ключевые носители подлежат уничтожению. Уничтожение оформляется актом (приложение № 1 к настоящей Инструкции).

5.8 Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

5.9 Ключевые носители совместно с Журналом должны храниться в запираемом шкафу, сейфе (металлическом шкафу), как правило, в отдельной ячейке. В исключительных случаях допускается хранить ключевые носители и Журнал совместно с другими документами, при этом ключевые носители и Журнал должны быть помещены в отдельную папку.

5.10 На время отсутствия Администратора СКЗИ распоряжением администрации должен быть назначен работник его замещающий.

6. Использование СКЗИ и криптографических ключей

6.1 Факт готовности эксплуатации СКЗИ оформляется актом о готовности эксплуатации СКЗИ (приложение № 3, к настоящей Инструкции).

7. Изготовление и плановая смена криптографических ключей

7.1 Изготовление криптографических ключей производиться Администратором СКЗИ в присутствии Пользователя СКЗИ.

7.2 Криптографические ключи изготавливаются на отчуждаемый ключевой носитель (дискету, ruToken, EToken и др.) в соответствии с эксплуатационно-технической документацией на СКЗИ и требованиями безопасности, установленными настоящей Инструкцией.

7.3 В целях обеспечения непрерывности проведения работы плановую смену криптографических ключей следует производить заблаговременно.

7.4 Переход на новые криптографические ключи Пользователь СКЗИ выполняет самостоятельно в соответствии с эксплуатационной документацией на СКЗИ. Переход на новые криптографические ключи осуществляется в сроки, указанные в сертификате ключа подписи.

7.5 При замене криптографических ключей используют программное обеспечение в соответствии с документами по эксплуатации. Пользователь СКЗИ обязан самостоятельно обновить сертификат ключ подписи. Обновление справочников сертификатов ключей производится путем добавления новых сертификатов ключей подписи из файлов, содержащих сертификаты ключей подписи, предоставляемых Администратором СКЗИ. Обновление справочников сертификатов ключей подписи осуществляется в соответствии с эксплуатационной документацией на СКЗИ.

8. Действия при компрометации криптографических ключей

8.1 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:

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

б) увольнение (переназначение) работников, имевших доступ к ключевой информации;

в) передача секретных ключей по линии связи в открытом виде;

г) нарушение правил хранения криптоключей;

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

е) отрицательный результат при проверке наложенной ЭЦП;

ж) несанкционированное или безучётное копирование ключевой информации;

з) 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).

8.2 События 8.1(а-д) должны трактоваться как безусловная компрометация действующих ключей. Остальные события требуют специального расследования в каждом конкретном случае.

8.3 При наступлении любого из перечисленных в п. 8.1 событий Владелец ключа должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации главе сельского поселения «Вотча» или Администратору СКЗИ.

8.4 При подтверждении факта компрометации действующих ключей Пользователь СКЗИ обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей.

8.5 Для восстановления конфиденциальной связи, после компрометации действующих ключей, на Пользователя СКЗИ оформляются новые ключи ЭЦП.

9. Уничтожение криптографических ключей

9.1 Неиспользованные или выведенные из действия криптографические ключи подлежат уничтожению.

9.2 Уничтожение криптографических ключей на ключевых носителях производится уполномоченной на то комиссий с участием Администратора СКЗИ с оформлением акта актом (приложение № 1 к настоящей Инструкции).

9.3 Криптографические ключи, находящиеся на ключевых носителях, уничтожаются путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на СКЗИ. При уничтожении криптографических ключей, находящихся на ключевых носителях, необходимо:

а) установить наличие оригинала и количество копий криптографических ключей;

б) проверить внешним осмотром целостность каждого ключевого носителя;

в) установить наличие на оригинале и всех копиях ключевых носителей реквизитов путем сверки с записями в Журнале поэкземплярного учета;

г) убедиться, что криптографические ключи, находящиеся на ключевых носителях, действительно подлежат уничтожению;

д) произвести уничтожение ключевой информации на оригинале и на всех копиях носителей.

9.4 В Журнале поэкземплярного учета Администратором СКЗИ производится отметка об уничтожении криптографических ключей.

10. Права Администратора СКЗИ

10.1. Администратор СКЗИ имеет право:

а) вносить предложения по совершенствованию СКЗИ;

б) повышать уровень квалификации по использованию СКЗИ.

11. Ответственность Администратора СКЗИ

11.1. Администратора СКЗИ несет персональную ответственность за обеспечение конфиденциальности ключевых носителей.

11.2 В случае неисполнения или ненадлежащего выполнения требований настоящей Инструкции Администратора СКЗИ может быть привлечен к дисциплинарной и/или административной ответственности в соответствии с действующим законодательством Российской Федерации

Приложение № 1
к инструкции администратора средств
криптографической защити информации (СКЗИ)

УТВЕРЖДАЮ:
Глава сельского поселения «Вотча»

_____ /_____/

« ____ » _____ 20____ г.

м.п.

А К Т № ____
об уничтожении ключевого носителя СКЗИ

Комиссия в составе:
_____
_____выполнила уничтожение ключевых носителей СКЗИ, методом последовательного уничтожения информации: (форматирование дискеты 1.4 средствами операционной системы Windows, физическое уничтожение дискеты 1.4); другое: _____

Инвентарный номер системного блока (персональный компьютер)	**Фамилия, имя, отчество Пользователя СКЗИ**	**Дата изъятия (уничтожения)**	**Серийный номер СКЗИ**

Всего уничтожено _____ ключевых носителей СКЗИ.

Члены комиссии:

Дата уничтожения:
« ___ » _____ 20___ г.

_____ /_____/
_____ /_____/
_____ /_____/
_____ /_____/

Приложение № 2
к инструкции администратора средств
криптографической защити информации (СКЗИ)

УТВЕРЖДАЮ:
Глава сельского поселения «Вотча»
_____ /_____/

« ____ » _____ 20____ г.

м.п.

А К Т № ____
об изъятии СКЗИ из аппаратных средств

Комиссия в составе:
_____
_____
_____ выполнила изъятие СКЗИ (КриптоПро CSP, ViPNet Client, SecretNet и др.), методом деинсталляции программы средствами операционной системы Windows:

Инвентарный номер системного блока (персональный компьютер)	**Фамилия, имя, отчество Пользователя СКЗИ**	**Дата изъятия (уничтожения)**	**Серийный номер жесткого диска**

Всего уничтожено _____ средств СКЗИ.

Члены комиссии:

Дата уничтожения:
« ___ » _____ 20___ г.

_____ /_____/
_____ /_____/
_____ /_____/
_____ /_____/

Приложение № 3
к инструкции администратора средств
криптографической защити информации (СКЗИ)

УТВЕРЖДАЮ
Глава сельского поселения «Вотча»
_____/_____/
(подпись и Фамилия И.О. руководителя)
«___»_____20___г.
м.п.

УТВЕРЖДАЮ
Директор ГБУ РК «Центр безопасности информации»
_____ /_____/

«___»_____20__г.

АКТ №_____
о готовности эксплуатации СКЗИ

Комиссия сотрудников _____ в составе:
(название организации)
_____

в соответствии с Договором № _____ от «___»_____20___г. и «Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации (СКЗИ) с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной Приказом ФАПСИ №152 от 13.06.2001г., следующими данными о _____:
(название организации)
Расположение тех. средств с СКЗИ (насел. пункт, ул., дом, каб.) _____
_____.
Инвентарный или заводской № ПЭВМ (где используется СКЗИ), № СКЗИ (указан на полученном CD-диске): _____.
Печать (которой опечатана ПЭВМ): _____.
Наименование и код СКЗИ: _____.
Используемое программное обеспечение (версия и код операционной системы, ПО):_____
_____.
проведенными работами по проверке функционирования СКЗИ, а также на основании соответствующей подготовки лиц, использующих СКЗИ, делает вывод о _____ вышеуказанной организации
(соответствии/не соответствии)
требованиям «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 ФАПСИ №152 от 13.06.2001г. и она _____(готова/не готова)_____к самостоятельному использованию СКЗИ.

Члены комиссии:
_____/_____
_____/_____
_____/_____