АДМИНИСТРАЦИЯ ВЕРХНЕХАВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА ВОРОНЕЖСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

от 28.04 2020 г. № 95-р
с. Верхняя Хава

Об утверждении документов, регламентирующих обработку и обеспечение безопасности персональных данных

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановлением правительства Воронежской области от 30.12.2019 № 1344, руководящими документами ФСТЭК Российской Федерации и другими нормативными правовыми документами по вопросам использования и защиты информационных ресурсов, содержащих персональные данные,

1. Утвердить прилагаемые:

1.1. Правила работы с обезличенными данными в администрации Верхнехавского муниципального района Воронежской области (Приложение № 1).

1.2. Перечень информационных систем персональных данных (Приложение № 2).

1.3. Инструкцию ответственного за обеспечение безопасности персональных данных в информационной системе (администратора безопасности) (Приложение № 3).

1.4. Инструкцию пользователя информационных систем персональных данных (Приложение № 4).

1.15. Схему контролируемой зоны (Приложение № 5).

1.16. Инструкцию ответственного пользователя средств криптографической защиты информации (Приложение № 6).

1.17. Инструкцию 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 (Приложение № 7).

1.18. Регламент по учету, хранению и уничтожению носителей персональных данных администрации Верхнехавского муниципального района (Приложение № 8).

2. Назначить:

2.1. Ответственного пользователя средств криптографической защиты информации – Саблина В.В. – начальника отдела по информационным технологиям, организационной работе и муниципальной службе администрации.

2.2. Пользователей средств криптографической защиты информации согласно приложению.

3. Ознакомить с настоящим распоряжением работников администрации Верхнехавского муниципального района Воронежской области в части их касающейся.

4. Контроль за исполнением настоящего распоряжения возложить на руководителя аппарата Боброва В.Ф.

Глава Верхнехавского
муниципального района С.А. Василенко

Приложение 1
Утверждено
распоряжением
администрации Верхнехавского
муниципального района
от 28.04.2020 г № 95-р

Правила
работы с обезличенными данными в администрации Верхнехавского муниципального района Воронежской области

1. Общие положения

1.1. Настоящие Правила работы с обезличенными персональными данными администрации Верхнехавского муниципального района Воронежской области (далее - администрация) разработаны с учетом Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" и Постановления Правительства РФ от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами".

1.2. Для целей настоящих Правил используются понятия, определенные Федеральным законом "О персональных данных".

2. Условия и способы обезличивания персональных данных

2.1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных администрации и по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- обобщение - понижение точности некоторых сведений;
- понижение точности некоторых сведений (например, "Место жительства" может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);

- деление сведений на части и обработка в разных информационных системах;

- другие способы.

2.3. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

2.4. Решение о необходимости обезличивания персональных данных принимается руководителем аппарата.

2.5. Начальники отделов, непосредственно осуществляющих обработку персональных данных, готовят предложения по обезличиванию персональных данных, способу обезличивания, а также обоснование такой необходимости.

2.6. Сотрудники подразделений, обслуживающих базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных осуществляют непосредственное обезличивание выбранным способом.

3. Порядок работы с обезличенными персональными данными

3.1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

3.2. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

3.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;

- антивирусной политики;

- правил работы со съемными носителями (если они используются);

- правил резервного копирования;

- правил доступа в помещения, где расположены элементы информационных систем.

3.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение правил хранения бумажных носителей, а также правил доступа к ним и в помещения, где они хранятся.

Приложение № 2
Утверждено
распоряжением
администрации Верхнехавского
муниципального района
от 28.04.2020 г № 95-р

Перечень
информационных систем персональных данных
администрации Верхнехавского муниципального района Воронежской области

№ п/п	Наименование информационной системы персональных данных	Назначение информационной системы персональных данных	Наименование структурного подразделения
1.	«Автоматизация бухгалтерского учета»	Ведение бухгалтерского учёта, ведение бухгалтерской отчётности, начисление заработной платы, предоставление сведений ФНС, ПФР	Отдел по информационным технологиям, организационной работе и муниципальной службе администрации
2.	«Автоматизация кадрового учета»	Обеспечение кадровой работы	Отдел по информационным технологиям, организационной работе и муниципальной службе администрации
3.	«Автоматизация деятельности административной комиссии»	Реализация возложенных на администрацию Верхнехавского муниципального района Воронежской области	Отдел по информационным технологиям, организационной работе и муниципальной службе администрации
4.	«Автоматизация деятельности по программе «Обеспечение жильем молодых семей»	Реализация возложенных на администрацию Верхнехавского муниципального района Воронежской области	Отдел по экономике и управлению муниципальным имуществом администрации

5.	«Автоматизация деятельности по программе «Земельный контроль»	Реализация возложенных на администрацию Верхнехавского муниципального района Воронежской области	Отдел по правовой работе и муниципальному контролю
6.	«Автоматизация обработки услуг в сфере строительства»	Реализация возложенных на администрацию Верхнехавского муниципального района Воронежской области	Отдел по строительству, архитектуре и ЖКХ администрации

Приложение № 3
Утверждено
распоряжением
администрации Верхнехавского
муниципального района
от 28.04.2020 г № 95-р

Инструкция
ответственного за обеспечение безопасности
персональных данных в информационной системе (администратора безопасности)
администрации Верхнехавского муниципального района
Воронежской области

1. Общие положения

1.1. Ответственный за обеспечение безопасности персональных данных в информационной системе - лицо, выполняющее функции по настройке и сопровождению всех программных и технических средств защиты информации информационной системы персональных данных, предназначенных для обработки информации, содержащей персональные данные (далее ИСПДн).

1.2. Ответственный за обеспечение безопасности персональных данных в информационной системе в пределах своих функциональных обязанностей обеспечивает безопасность информации, обрабатываемой, передаваемой и хранимой в ИСПДн.

1.3. Ответственный за обеспечение безопасности персональных данных назначается установленным порядком.

1.4. Ответственный за обеспечение безопасности персональных данных в своей работе руководствуется положениями нормативно - правовых актов РФ, руководящими документами по безопасности информации, положениями, приказами и нормативными актами министерств и ведомств Российской Федерации и положениями настоящей Инструкции.

2. Обязанности

Основными обязанностями ответственного за обеспечение безопасности персональных данных являются:

− управление средствами и системами защиты информации (СЗИ) ИСПДн и поддержание их функционирования;

− восстановление функций программных и технических СЗИ от НСД к информации;

− генерация ключей, личных идентификаторов, а так же паролей для пользователей АС;

− формирование и управление списком необходимых реквизитов и значением атрибутов объектов и субъектов доступа;

– назначение прав доступа, полномочий и привилегий пользователей к объектам доступа (программам, файлам, каталогам, портам и устройствам ввода-вывода (УВВ);

– обеспечение правильной эксплуатации технических и программных СЗИ в ИСПДн;

– контроль целостности эксплуатируемого в ИСПДн программного обеспечения, в том числе самих СЗИ, с целью недопущения и выявления несанкционированных модификаций;

– текущий, после сбоев и периодический (не реже 1 раза в год) контроль работоспособности средств и систем защиты информации от НСД;

– контроль соблюдения пользователями ИСПДн требований инструкций и порядка работы при обработке информации в ИСПДн, по вопросам защиты информации от НСД;

– контроль выполнения утвержденной технологии обработки информации в ИСПДн;

– выявление подозрительных действий пользователей и попыток НСД к информации, обрабатываемой в ИСПДн, путем анализа системных журналов информационной безопасности при работе в ИСПДн. В случае обнаружения или выявления таких попыток, немедленно докладывать ответственному за соблюдение режима конфиденциальности и руководителю организации;

– выполнение резервного копирования машинных документов содержащих персональные данные;

– обучение и консультации персонала и пользователей ИСПДн правилам работы с СЗИ от НСД;

– организация антивирусной защиты информации и программных средств в ИСПДн;

– корректировка содержания с целью соответствия реальным условиям следующих документов:

- инструкция системному администратору;
- инструкция пользователю.
- разрешительная система доступа к информационным ресурсам, программным и техническим средствам.

– взаимодействие с системным администратором, ответственным за организацию обработки персональных данных, по вопросам обеспечения защиты информации и предоставления пользователям прав доступа к ней.

3. Права

Ответственный за обеспечение безопасности персональных данных имеет право:

– Требовать от пользователей ИСПДн выполнения установленной технологии обработки информации, инструкций по обеспечению информационной безопасности ИСПДн.

– Останавливать обработку информации в ИСПДн в случаях подтвержденных нарушений установленной технологии обработки данных, приводящих к нарушению функционирования СЗИ.

4. Ответственность

4.1. На ответственного за обеспечение безопасности персональных данных возлагается персональная ответственность за качество и полноту проводимых им работ по обеспечению защиты информации в соответствии с его функциональными обязанностями.

4.2. Ответственный за обеспечение безопасности персональных данных несет ответственность по законодательству РФ за нарушение требований нормативно - методических документов по защите информации и настоящей инструкции.

ОЗНАКОМЛЕНЫ

_____ _____

Приложение № 4
Утверждено
распоряжением
администрации Верхнехавского
муниципального района
от 28.04.2020 г № 95-р

Инструкция
пользователя информационных систем персональных данных
администрации Верхнехавского муниципального района

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция определяет основные обязанности, права и ответственность пользователя информационных систем персональных данных (далее - пользователь) администрации Верхнехавского муниципального района (далее - администрация).

1.2. Пользователем является каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты информации (далее - СЗИ) информационных систем персональных данных (далее - ИСПДн).

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией и Положением по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных администрации Верхнехавского муниципального района.

1.5. Ознакомление сотрудников с требованиями настоящей Инструкции проводит ответственный за обеспечение безопасности персональных данных (далее - ПДн) под роспись.

1.6. Методическое руководство работой пользователя осуществляется ответственным за обеспечение безопасности ПДн.

2. ФУНКЦИИ И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

2.1. Каждый пользователь обязан:

2.1.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по обеспечению безопасности ПДн.

2.1.2. Выполнять свои функциональные обязанности строго в рамках прав доступа к внутренним и внешним информационным ресурсам,

техническим средствам, полученным согласно Разрешительной системы доступа к информационным ресурсам, программным и техническим средствам ИСПДн.

2.1.3. Знать и соблюдать установленные требования по режиму обработки ПДн, организации парольной защиты, по проведению антивирусного контроля, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн.

2.1.4. Знать и строго выполнять правила работы с СЗИ.

2.1.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена.

2.1.6. Во время работы с защищаемой информацией экран монитора в помещении располагать так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами, шторы (жалюзи) на оконных проемах должны быть завешаны.

2.1.7. Обо всех выявленных нарушениях, связанных с обработкой ПДн, сообщать ответственному за обеспечение безопасности ПДн.

2.1.8. Заблокировать доступ при отсутствии визуального контроля за рабочей станцией. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

2.2. Пользователю запрещается:

2.2.1. Разглашать защищаемую информацию по Перечню ПДн, подлежащих защите, третьим лицам.

2.2.2. Копировать защищаемую информацию на неучтенные носители информации.

2.2.3. Использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях.

2.2.4. Самостоятельно устанавливать, тиражировать, или модифицировать программное и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств ИСПДн.

2.2.5. Подключать личные внешние носители и мобильные устройства к техническим средствам ИСПДн.

2.2.6. Отключать (блокировать) СЗИ ИСПДн.

2.2.7. Обрабатывать информацию и выполнять работы, не предусмотренные Разрешительной системой доступа к информационным ресурсам, программным и техническим средствам ИСПДн.

2.2.8. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

2.2.9. Привлекать посторонних лиц для производства ремонта или настройки средств ИСПДн.

3. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

3.1. Личные пароли доступа к средствам ИСПДн выдаются пользователям администратором безопасности, ответственным за обеспечение безопасности ПДн или другим уполномоченным лицом.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила ввода пароля:

- ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;
- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами.

3.4. Правила хранение пароля:

- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
- запрещается сообщать другим пользователям личный пароль.

3.5. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования организации парольной защиты;
- своевременно сообщать администратору безопасности или ответственному за обеспечение безопасности ПДн об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ

4.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, другими организационно-распорядительными документами, в соответствии с действующим трудовым законодательством Российской Федерации.

4.2. За правонарушения, совершенные в процессе своей деятельности в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

4.3. За разглашение сведений конфиденциального характера и другой защищаемой информации в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

Приложение № 5
Утверждено
распоряжением
администрации Верхнехавского
муниципального района
от 28.04.2020 г № 95-р

Схема
контролируемой зоны помещений (здание администрации Верхнехавского муниципального района Воронежской области 1,2,3 этажи)

Условные обозначения:
– – - Контролируема зона

Приложение № 6
Утверждено
распоряжением
администрации Верхнехавского
муниципального района
от 28.04.2020 г № 95-р

Инструкция
ответственного пользователя средств криптографической защиты информации

1. Общая часть

1.1. Настоящая инструкция разработана в соответствии приказом ФАПСИ от 13.06.2001 №152 «Об утверждении 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» и приказом ФСБ России от 10.07.2014 N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности".

1.2. Ответственный пользователь средств криптозащиты информации (далее – СКЗИ) назначается из числа сотрудников администрации Верхнехавского муниципального района Воронежской области (далее – администрация) и освобождается от этих обязанностей распоряжением главы администрации.

2. Квалификационные требования

Профессиональные знания и навыки:

2.1. Ответственный пользователь СКЗИ в своей работе руководствуется следующими нормативными документами Российской Федерации и организационно-распорядительной документацией администрации:

– «Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ от 13.06.2001 №152;

– «Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для

обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные ФСБ России от 21.02.2008 № 149/6/6-622;

- приказом ФСБ России от 10.07.2014 N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности";

– распоряжениями, инструкциями и иными организационно-распорядительные документами администрации.

3. Функциональные обязанности

В обязанности ответственного пользователя СКЗИ входит:

3.1. Своевременное и качественное исполнение поручений руководства администрации, данные в пределах их полномочий, установленных законодательством Российской Федерации.

3.2. Оказание консультационной помощи по вопросам соблюдения защиты информации при обращении со средствами криптографической защиты информации.

3.3. Постоянное повышение профессиональных навыков и умений, необходимых для надлежащего исполнения функциональных обязанностей.

3.4. Знание порядка эксплуатации используемых администрацией СКЗИ.

3.5. Ведение установленного нормативными документами учета СКЗИ, ключевых документов, сертификатов электронных цифровых подписей.

3.6. Соблюдение режима конфиденциальности при обращении со сведениями, полученными при исполнении функциональных обязанностей, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документах к ним.

3.7. Надежное хранение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

3.8. Выявление попыток посторонних лиц получить сведения о защищаемой конфиденциальной информации, об используемых СКЗИ или ключевых документах к ним и своевременное оповещение об этом руководителя органа криптографической защиты информации.

3.9. Немедленное принятие мер по предупреждению разглашения защищаемых сведений конфиденциального характера, а также возможной утечки таких сведений при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

Ответственный пользователь СКЗИ осуществляет следующие функции:

3.10. Осуществляет профилактическую деятельность по соблюдению требований руководящих документов, технической, эксплуатационной документации с сотрудниками администрации, назначенными пользователями СКЗИ.

3.11. Участвует в проведении служебных расследований по фактам нарушения требований по обращению с СКЗИ.

3.12. Принимает меры к предотвращению разглашения и утечки информации ограниченного доступа при эксплуатации и хранении специальных технических средств, предназначенных для передачи, приема и обработки конфиденциальной информации, а также при использовании незащищенных каналов связи.

3.13. Участвует в разработке методических и нормативных материалов и оказании необходимой методической помощи в проведении работ по защите информации при обращении с СКЗИ.

4. Права

Ответственный пользователь СКЗИ:

4.1. Осуществлять плановые и внеплановые проверки функционирования СКЗИ, наличия ключевых документов и технической документации с СКЗИ.

4.2. Осуществлять, в рамках своей компетенции, взаимодействие с организациями-производителями СКЗИ.

4.3. При изменении состава СКЗИ получить профессиональную переподготовку, повышение квалификации и стажировку в порядке, установленном законодательством Российской Федерации.

4.4. Ходатайствовать о проведении служебной проверки.

5. Ответственность

Ответственный пользователь СКЗИ несет персональную ответственность в соответствии с законодательством Российской Федерации за:

5.1. Выполнение возложенных на него обязанностей и правильное использование предоставленных ему прав в соответствии с данными функциональными обязанностями.

5.2. Несвоевременное или некачественное выполнение приказов главы администрации.

5.3. Разглашение сведений, отнесенных к сведениям ограниченного доступа, ставших известными в ходе выполнения функциональных обязанностей или иным путем, утрату их носителей, передачу третьим лицам, публикацию без разрешения руководства, а также использование для занятия любой деятельностью, которая может нанести ущерб администрации.

С инструкцией ознакомлен:

Приложение № 7
Утверждено
распоряжением
администрации Верхнехавского
муниципального района
от 28.04.2020 г № 95-р

Инструкция
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
(инструкция пользователя СКЗИ)

1. Средства криптографической защиты информации (далее – СКЗИ) предназначены для обеспечения безопасности хранения, обработки и передачи по каналам связи информации с ограниченным доступом, не содержащих сведений, составляющих государственную тайну.
2. Обладатели конфиденциальной информации обязаны выполнять указания ответственного пользователя СКЗИ по всем вопросам организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.
   Для работы с СКЗИ допускаются только уполномоченные должностные лица, имеющие необходимый уровень знаний работы с СКЗИ и назначенные распоряжением главы администрации Верхнехавского муниципального района Воронежской области.
3. Пользователи СКЗИ ОБЯЗАНЫ**:**
   - не разглашать конфиденциальную информацию, к которой они допущены, рубежи её защиты, в том числе сведения о криптоключах;
   - соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
   - сообщать ответственному пользователю СКЗИ о ставших им известных попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документов к ним;
   - при отстранении увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы;
   - немедленной уведомлять ответственного пользователя СКЗИ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений

конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

4. Пользователям ЗАПРЕЩАЕТСЯ**:**
   - осуществлять несанкционированное копирование ключевых документов;
   - осуществлять несанкционированный вынос ключевых носителей за пределы контролируемой зоны;
   - хранить ключевые документы и ключевые носители вне специально выделенных хранилищ и помещений;
   - вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом использования ключевого носителя;
   - вносить какие-либо изменения в программное обеспечение СКЗИ;
   - изменять настройки, установленные программой установки СКЗИ или администратором информационной безопасности;
   - осуществлять несанкционированное вскрытие системных блоков ПЭВМ, подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные в комплектации.
5. Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения и ознакомления с настоящей инструкцией. Обучение пользователей правилам работы с СКЗИ осуществляет ответственный пользователь СКЗИ.
6. Изготовление ключевых документов осуществляется ответственным пользователем СКЗИ с применением штатных СКЗИ (если такая возможность предусмотрена эксплуатационной и технической документацией СКЗИ).
7. Ключевые документы, СКЗИ с введёнными криптографическими ключами относятся к материальным носителям, содержащие конфиденциальную информацию. При этом должны выполняться требования настоящей Инструкции и иных документов, регламентирующих порядок обращения с конфиденциальной информацией в организации.
8. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учёту в «Журнале поэкземплярного учета криптографических средств, эксплуатационной и технической документации к ним, ключевых документов».
9. Все экземпляры СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы должны быть выданы под расписку в соответствующем журнале учета пользователей СКЗИ, несущих персональную ответственность за их сохранность.
10. Передача экземпляров СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ под расписку в соответствующем журнале.

11. Пользователи СКЗИ хранят установочные пакеты СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в шкафах (ящиках, сейфах) индивидуального пользования, в условиях, исключающих бесконтрольный доступ к ним, а также и непреднамеренное уничтожение.
12. Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется создать их резервные копии. Копии должны быть соответствующим образом маркированы и могут использоваться и храниться так же, как и оригиналы.
13. Криптографические ключи, в отношении которых возникло подозрение в компрометации, необходимо немедленно изъять и при доказательстве компрометации надлежащим образом уничтожить.
14. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним, должны обеспечивать сохранность конфиденциальной информации, СКЗИ, ключевых документов и ключевых носителей.
15. Средства вычислительной техники, на которых осуществляется штатное функционирование 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.

Лист ознакомления с Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну

№ п/п	Должность	Фамилия, инициалы	Подпись, дата
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			

Приложение № 8
Утверждено
распоряжением
администрации Верхнехавского
муниципального района
от 28.04.2020 г № 95-р

Регламент по
учету, хранению и уничтожению
носителей персональных данных
администрации Верхнехавского муниципального района

1. Настоящий документ устанавливает организацию учета, хранения, выдачи и уничтожению машинных носителей персональных данных информационных систем персональных данных (ИСПДн) администрации Верхнехавского муниципального района.

2. Учет, хранение и выдачу машинных носителей персональных данных осуществляют сотрудники структурных подразделений, на которых возложены функции учета, хранения и выдачи носителей персональных данных, данные сотрудники несут персональную ответственность за сохранность персональных данных. При увольнении сотрудника, ответственного за учет, хранение и выдачу машинных носителей персональных данных, составляется акт приема-сдачи этих документов.

3. Организация учета машинных носителей персональных данных.

Все находящиеся на хранении и в обращении машинные носители персональных данных (далее - носители) подлежат учёту. Учет всех видов и типов носителей производится в Журнале учета носителей персональных данных (приложение №1).

Каждый носитель должен иметь этикетку, на которой указывается его уникальный учетный номер. На несъемную часть носителя ПДн наносятся:

- учетный номер;
- отметка «Персональные данные»;
- дата регистрации (день, месяц, год);

4. Организация выдачи машинных носителей персональных данных.

Пользователи ИСПДн получают учтенный съемный носитель от уполномоченного сотрудника, для выполнения работ на конкретный срок. При получении делаются соответствующие записи в Журнале учета выдачи машинных носителей персональных данных (приложение №2). По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в Журнале учета выдачи машинных носителей персональных данных.

5. Организация хранения машинных носителей персональных данных.

Хранение носителей осуществляется в условиях, исключающих несанкционированное копирование, изменение или уничтожение конфиденциальной информации, а также хищение носителей. Носители должны храниться в служебных помещениях, в сейфе – установленным порядком. Запрещается хранить машинные носители персональных данных вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

6. Действия при утрате или уничтожении съемных носителей персональных данных – в случае утраты носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность ответственный за обеспечение безопасности персональных данных. Соответствующие отметки вносятся в Журналы учета машинных носителей персональных данных.

7. Носители, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение носителей осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется Акт уничтожения машинных носителей персональных данных.

8. При передаче средств вычислительной техники администрации Верхнехавского муниципального района сторонним организациям для проведения ремонтно-восстановительных или иных работ, несъемные машинные носители изымаются из состава средства вычислительной техники.

9. Ответственность за выполнение правил эксплуатации машинных носителей персональных данных при выполнении непосредственных работ с носителями несет пользователь ИСПДн.

10. Контроль выполнения пользователями установленных правил эксплуатации машинных носителей персональных данных, осуществляет ответственный за эксплуатацию объекта информатизации, ответственный за обеспечение безопасности персональных данных и администратор безопасности информации в рамках своих должностных обязанностей.

ОЗНАКОМЛЕНЫ

_____	_____
_____	_____
_____	_____

Приложение №1
к регламенту по
учету, хранению и уничтожению
носителей персональных данных
администрации Верхнехавского
муниципального района

Журнал учета носителей персональных данных

Журнал начат «____» _____ 201__ г. Должность_____ _____ / ФИО должностного лица /	Журнал завершен «____» _____ 201__ г. Должность_____ _____ / ФИО должностного лица /

На _____ листах

№ п/п	Регистрационный номер	Дата учета	Тип / емкость носителя	Серийный номер	Отметка о постановке на учет (ФИО, подпись, дата)	Отметка о снятии с учета (ФИО, подпись, дата)	Местоположение носителя	Сведения об уничтожении носителя / стирании информации
1	2	3	4	5	6	7	8	9

Приложение №2
к регламенту по
учету, хранению и уничтожению
носителей персональных данных
администрации Верхнехавского
муниципального района

Журнал учета выдачи носителей персональных данных

Журнал начат «____» _____ 201__ г.

Должность_____
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 201__ г.

Должность_____
_____ / ФИО должностного лица /

На _____ листах

Учетный номер	Дата выдачи НПДн	Кому выдан (фамилия)	Расписка в получении, дата	Расписка в обратном приеме, дата

Приложение № 9
Утверждено
распоряжением
администрации Верхнехавского
муниципального района
от 28.04.2020 г № 95-р

Список пользователей
средств криптографической защиты информации

№ п/п	Должность	ФИО
1.	Глава администрации	Василенко С.А.
2.	Руководитель аппарата	Бобров В.Ф.
3.	Начальник отдела по информационным технологиям, организационной работе и муниципальной службе администрации	Саблин В.В.
4.	Главный бухгалтер отдела по информационным технологиям, организационной работе и муниципальной службе администрации	Небогина В.Н.
5.	Старший инспектор – делопроизводитель отдела по информационным технологиям, организационной работе и муниципальной службе администрации	Шабунина В.И.
6.	Ведущий специалист отдела по информационным технологиям, организационной работе и муниципальной службе администрации	Ситникова О. Е.
7.	Ведущий консультант по муниципальному заказу	Власова Е. В.
8.	Начальник отдела по правовой работе и муниципальном у контролю	Канаева Т.Л.
9.	Заместитель начальника отдела по правовой работе и муниципальном у контролю	Вострикова М.Н.
10.	Ведущий специалист отдела по правовой работе и муниципальному контролю	Попова В.О.
11.	Начальник отдела по строительству, архитектуре и ЖКХ администрации	Иванов Н.В.
12.	Специалист по архитектуре и градостроительству	Хатунцева О.А.
13.	Руководитель отдела по экономике и управлению муниципальным имуществом	Федюкина Т.В.
14.	Консультант отдела по экономике и управлению муниципальным имуществом	Кондаурова Н.В.
15.	Бухгалтер отдела по экономике и управлению муниципальным имуществом	Пономарева Е.В.
16.	Консультант отдела по экономике и управлению муниципальным имуществом	Савельева Л.А.

17.	Ведущий консультант отдела по экономике и управлению муниципальным имуществом	Штанько Л.Б.
18.	Начальник сектора по имущественным и земельным отношениям	Гаськова Н.П.
19.	Начальник отдела по правовой работе и муниципальному контролю	Канаева Т.Л.
20.	Заместитель начальника отдела по правовой работе и муниципальному контролю	Вострикова М.Н.
21.	Начальник сектора по земельному контролю	Истомина Е.А.
22.	Специалист	Попова Н.А.
23.	Руководитель финансового отдела	Никитина Т.Ф.
24.	Ведущий консультант финансового отдела	Попов С.А.
25.	Начальник отдела образования, физической культуры и спорта	Хатунцев С.И.
26.	Начальник отдела культуры и архивного дела	Маракаев А.Ф.
27.	Начальник отдела – ответственный секретарь комиссии по делам несовершеннолетних и защите их прав	Писаренко Е.А.