Официальное издание муниципального образования «Казачье»

**Муниципальный Вестник**

26 февраля 2021 г. № 2

**25.02.2021г. №111**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ КАЗАЧЬЕ**

**ДУМА**

**РЕШЕНИЕ**

**О ВНЕСЕНИИ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ В РЕШЕНИЕ ДУМЫ МО «КАЗАЧЬЕ» ОТ 24.09.2020 №82** **«ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ О ПОРЯДКЕ СООБЩЕНИЯ ЛИЦАМИ, ЗАМЕЩАЮЩИМИ МУНИЦИПАЛЬНЫЕ ДОЛЖНОСТИ В МУНИЦИПАЛЬНОМ ОБРАЗОВАНИИ «КАЗАЧЬЕ» О ВОЗНИКНОВЕНИИ ЛИЧНОЙ ЗАИНТЕРЕСОВАННОСТИ ПРИ ИСПОЛНЕНИИ ДОЛЖНОСТНЫХ ОБЯЗАННОСТЕЙ, КОТОРАЯ ПРИВОДИТ ИЛИ МОЖЕТ ПРИВЕСТИ К КОНФЛИКТУ ИНТЕРЕСОВ»**

В соответствии с Федеральным законом от 25 декабря 2008 года № 273-ФЗ «О противодействии коррупции», Указом Президента Российской Федерации от 22 декабря 2015 года № 650 «О порядке сообщения лицами, замещающими отдельные государственные должности Российской Федерации, должности федеральной государственной службы, и иными лицами о возникновении личной заинтересованности при исполнении должностных обязанностей, которая приводит или может привести к конфликту интересов, и о внесении изменений в некоторые акты Президента Российской Федерации», руководствуясь Уставом муниципального образования «Казачье», дума

**РЕШИЛА:**

1.Внести изменения и дополнения в Решение Думы от 24.09.2020г. № 82 «Об утверждении положения о порядке сообщения лицами, замещающими муниципальные должности в муниципальном образовании «казачье» о возникновении личной заинтересованности при исполнении должностных обязанностей, которая приводит или может привести к конфликту интересов»

1.1 в пункте 5 Положения слова «заместителем председателя Думы муниципального образования «Казачье» заменить словами «председателем Думы муниципального образования «Казачье»

2. Администрации МО «Казачье» опубликовать настоящее решение с приложением в муниципальном Вестнике и на официальном сайте МО «Казачье» в сети Интернет.

Председатель Думы,

Глава муниципального образования «Казачье»

Т.С. Пушкарева

**25.02.2021г. №112**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ КАЗАЧЬЕ**

**ДУМА**

**РЕШЕНИЕ**

**О ВНЕСЕНИИ ИЗМЕНЕНИЙ В ПОЛОЖЕНИЕ О ЗЕМЕЛЬНОМ НАЛОГЕ НА ТЕРРИТОРИИ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ «КАЗАЧЬЕ», УТВЕРЖДЕННОЕ РЕШЕНИЕМ ДУМЫ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ «КАЗАЧЬЕ» ОТ 12 НОЯБРЯ 2020 ГОДА № 100 «ОБ УСТАНОВЛЕНИИ И ВВЕДЕНИИ В ДЕЙСТВИЕ ЗЕМЕЛЬНОГО НАЛОГА НА ТЕРРИТОРИИ МО «КАЗАЧЬЕ»**

Руководствуясь Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», главой 31 Налогового кодекса, Федеральным законом от 3 августа 2018 г. N 334-ФЗ «О внесении изменений в статью 52 части первой и часть вторую Налогового кодекса Российской Федерации», Уставом муниципального образования «Казачье», дума

**РЕШИЛА:**

1. В абзаце втором пункта 3.1. раздела 3 Положения о земельном налоге на территории муниципального образования «Казачье», утвержденного Решением Думы муниципального образования «Казачье» от 12 ноября 2020 года № 100 «Об установлении и введении в действие земельного налога на территории МО «Казачье» слова «по состоянию на 1 января года, являющегося налоговым периодом» исключить.

2. Настоящее решение вступает в силу не ранее, чем по истечении одного месяца со дня его официального опубликования.

3. Администрации МО «Казачье» опубликовать настоящее решение с приложением в муниципальном Вестнике и на официальном сайте МО «Казачье» в сети интернет.

4. В течение 5 дней с момента принятия направить настоящее решение в МИ ФНС № 16 по Иркутской области.

Председатель Думы,

Глава муниципального образования «Казачье»

Т.С. Пушкарева

**25.02.2021г. №113**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ КАЗАЧЬЕ**

**ДУМА**

**РЕШЕНИЕ**

**О ВНЕСЕНИИ ИЗМЕНЕНИЙ В БЮДЖЕТ МО «КАЗАЧЬЕ» НА 2021 ГОД**

Руководствуясь Федеральным законом от 06.10.2003 г. № 131-ФЗ «Об общих принципах организации органов местного самоуправления Российской Федерации», Бюджетным кодексом Российской Федерации, в соответствии с Уставом муниципального образования «Казачье», дума

**РЕШИЛА:**

1.Внести изменения в решение Думы №102 от 25.12.2020г. "О бюджете МО "Казачье" на 2021 год и плановый период 2022 и 2023 годов

1.1 Пункт 1 статьи 1 изложить в следующей редакции:

«Утвердить основные характеристики бюджета муниципального образования «Казачье» на 2021 год:

прогнозируемый общий объем доходов бюджета в сумме 12039500 рублей, из них объем безвозмездных поступлений, получаемых из других бюджетов бюджетной системы Российской Федерации, в сумме 10242700 рублей

общий объем расходов бюджета в 2021 году составит 12355624,90 рубля;

размер дефицита местного бюджета в сумме 316124,90 руб.

Установить, что превышение дефицита над ограничениями, установленными статьей 92.1 Бюджетного кодекса РФ, осуществлено в пределах сумм снижения остатка средств на счетах по учету средств местного бюджета в объеме 226324,90 руб.;

дефицит местного бюджета составляет 5 % утвержденного общего годового объема доходов бюджета МО «Казачье» с учетом остатков средств на счетах по учету средств бюджета и утвержденного объема безвозмездных поступлений»

2. Приложение 1,2,3,4 изложить в новой редакции.

Председатель Думы,

Глава муниципального образования «Казачье»

Т.С. Пушкарева

**01.02.2021 г. №10**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КАЗАЧЬЕ**

**ПОСТАНОВЛЕНИЕ**

**О ПРОВЕДЕНИИ ДЕКАДНИКА ПО ВОПРОСАМ ПРОФИЛАКТИКИ И ОБЕСПЕЧЕНИЯ ПОЖАРНОЙ БЕЗОПАСНОСТИ НА ТЕРРИТОРИИ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ «КАЗАЧЬЕ»**

С целью снижения количества пожаров, тяжести последствий от них, недопущения гибели людей при пожарах, активизации работы по обучению населения мерам пожарной безопасности, в соответствие с Федеральным законом №69-ФЗ от 21 декабря 1994 года «О пожарной безопасности», Федерального закона от 06 октября 2003 года № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», законом Иркутской области от 07 октября 2008 года № 78-ОЗ «О пожарной безопасности в Иркутской области», решения КЧС и ПБ МО «Боханский район» протокол №5 от 27.01.2021 года, в целях стабилизации обстановки с пожарами, в соответствии с Уставом муниципального образования «Казачье», администрация муниципального образования «Казачье»

**постановляЕТ:**

1.Провести в период с 01 по 10 февраля 2021 года декадник по вопросам профилактики и обеспечения пожарной безопасности на территории муниципального образования «Казачье»

2.Утвердить План мероприятий по проведению декадника по вопросам профилактики и обеспечения пожарной безопасности на территории муниципального образования «Казачье» (Приложение 1).

3. Утвердить состав группы профилактики на территории муниципального образования «Казачье» (Приложение 2)

4.Настоящее постановление подлежит официальному опубликованию на официальном сайте администрации муниципального образования «Казачье» и в муниципальном Вестнике

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к постановлению

МО Казачье

от 01.02.2021 № 10

**План мероприятий по проведению декадника по вопросам профилактики и обеспечения пожарной безопасности на территории МО «Казачье» в период с 01 по 10 февраля 2021 года**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Мероприятие | Сроки исполнения | Ответственные |
| 1 | Проверка искусственных и естественных водоемов, искусственного наружного противопожарного водоснабжения (Состояние подъездов, освещение, указатели, наличие патрубков для заправки пожарных автомашин) | в течение декадника | Герасимова Т.Г. |
| 2 | Подворный обход в жилом секторе с организацией обучения населения правилам безопасной эксплуатации печного отопления и электробытовых приборов по месту жительства | в течение декадника | Члены группы профилактики |
| 3 | Противопожарные инструктажи по месту жительства с лицами, относящихся к группе риска | в течение декадника | Члены группы профилактики |
| 4 | Распространение листовок, памяток о соблюдении мер пожарной безопасности при эксплуатации электронагревательных приборов, печного отопления | в течение декадника | Члены группы профилактики |
| 5 | Провести комплекс мер по выявлению юридических лиц, индивидуальных предпринимателей, граждан, оказывающих социальные услуги для престарелых граждан и инвалидов в стационарной форме, не состоящих в соответствующих реестрах и не отвечающих требованиям пожарной безопасности, принять меры к приостановлению функционирования указанных объектов до легализации их деятельности и полного устранения имеющихся нарушений и недостатков. | в течение декадника | Герасимов Т.Г. |
| 6 | Размещение в средствах массовой информации, в том числе через Интернет-ресурсы, блогосферу, социальные сети, СМС-оповещения и ролики социальной рекламы, материалов, направленных на доведение информации о возможных последствиях пожаров, связанных с несоблюдением требований пожарной безопасности | в течение декадника | Бормотова Т.С. |

Приложение 2

к постановлению

МО Казачье

от 01.02.2021 № 10

**Состав группы профилактики при муниципальном образовании «Казачье»**

1.Герасимова Т.Г. – руководитель группы.

2.Верхозин А.С.- член ДПД, член группы.

3.Кузнецова Н.В. – специалист по социальной работе, член группы.

4.Пузикова С.С. – староста д. Тымырей, член группы.

5.Юганова М.В. – староста д. Логанова, член группы.

6.Ершова С.П. – староста д. Крюкова, член группы.

7.Романова Н.В. – староста д. Ершова, член группы.

8.Михайлова Г.В. – староста д. Черниговская, член группы.

9.Михеев А.А. – ПСЧ 44, член группы.

10.Дорошенко Е.А. –ПСЧ 44, член группы.

**04.02.2021 г. №11**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КАЗАЧЬЕ**

**ПОСТАНОВЛЕНИЕ**

**ОБ УТВЕРЖДЕНИИ ИНСТРУКЦИИ О ПОРЯДКЕ ОБРАЩЕНИЯ С НОСИТЕЛЯМИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ**

В соответствии со Специальными требования и рекомендации по технической защите конфиденциальной информации» (СТР-К) (Гостехкомиссия России, от 30.08.2002 № 282), в соответствии с Уставом муниципального образования «Казачье», администрация муниципального образования «Казачье»

**постановляЕТ:**

1.Утвердитьинструкцию о порядке обращения с носителями конфиденциальной информации (Приложение 1)

2.Настоящее постановление подлежит официальному опубликованию на официальном сайте администрации муниципального образования «Казачье» и в муниципальном Вестнике

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к постановлению

МО Казачье

от 04.02.2021 № 11

**Инструкция о порядке обращения с носителями конфиденциальной информации**

1.Общие положения

Цель настоящей Инструкции заключается в доведении до всех работников правил использования защищаемых носителей информации и достижения эффективного использования защищаемых носителей информации.

Все защищаемые носители конфиденциальной информации делятся на съемные машинные носители информации (далее – СМНИ) и накопители на жёстких магнитных дисках (НЖМД).

СМНИ являются средством передачи и хранения различной информации в электронном виде. Нарушения правил использования СМНИ приводят к утечке информации ограниченного доступа, нарушению функционирования телекоммуникационных систем, утрате и искажению информации, что может нанести ущерб администрации МО "Казачье". Наиболее часто встречаются СМНИ в виде USB-флеш накопителей, CD (DVD)-R или CD-RW дисков, различных типов карт флеш памяти, мультимедийных устройств, сотовых телефонов (смартфонов коммуникаторов), внешних жестких дисков, цифровых фотоаппаратов и видеокамер. Требования настоящей Инструкции обязательны для всех работников администрации МО "Казачье".

Настоящая Инструкция распространяется на любые устройства независимо от интерфейсов подключения, способные подключаться к телекоммуникационному оборудованию, компьютерам, иным служебным техническим средствам и использоваться в качестве СМНИ.

Настоящая Инструкция не распространяется на СМНИ, предназначенные для записи и хранения сведений, составляющих государственную тайну. Все СМНИ, используемые в администрации МО "Казачье" делятся на служебные и личные. СМНИ регистрируются в Журнале учёта машинных носителей информации, предназначенных для хранения конфиденциальной информации в структурном подразделении, использующем этот СМНИ.

2.Порядок подключения СМНИ

Использование СМНИ осуществляется только при наличии служебной необходимости в порядке, определенном настоящей Инструкцией или иными документами администрации МО "Казачье".

Для работы со СМНИ, содержащими конфиденциальную информацию и персональные данные, должны использоваться автоматизированные рабочие места (АРМ), в том числе и портативные компьютеры, оборудованные программным обеспечением, предназначенным для контроля внешних носителей.

Все АРМ, на которых используются СМНИ, должны быть предварительно оснащены лицензионным антивирусным программным обеспечением с организацией обязательного оперативного обновления антивирусных баз.

3.Порядок подключения СМНИ

СМНИ используются работниками администрации МО "Казачье" для обеспечения производственной деятельности. Доступ к СМНИ должен производится только с АРМ, к которому СМНИ подключен в данный момент.

Информация, сохраненная на СМНИ с рабочих мест администрации МО "Казачье", не является частной собственностью работника, а составляет часть внутреннего документооборота администрации МО "Казачье". СМНИ не гарантируют 100% сохранность информации, соответственно, запрещается хранение информации только на СМНИ без мер резервирования. Информация ограниченного доступа должна храниться только на служебных СМНИ.

При использовании СМНИ категорически запрещается:

1.умышленно заносить в ИСПДн администрации МО "Казачье" вирусы или любые вредоносные программы, а также умышленно распространять их за пределы ИСПДн администрации МО "Казачье";

2.подключать служебные СМНИ к домашним компьютерам, если данные СМНИ содержат информацию ограниченного доступа;

3.использовать не зарегистрированные СМНИ;

4.хранить на личных СМНИ документы и сведения, относящиеся к информации ограниченного доступа согласно действующему законодательству;

5.несанкционированное использование любых средств и способов, позволяющих скрывать содержание информации, хранимой на СМНИ.

При работе со СМНИ работники администрации МО "Казачье" обязаны:

6.не допускать повреждений СМНИ при хранении и эксплуатации;

7.не запускать программное обеспечение, хранящееся на СМНИ;

8.создавать копии информации, хранимой на служебных СМНИ;

Запрещается обрабатывать с помощью СМНИ любые изображения, текст, программный код и иные материалы, которые:

9.могут быть признаны нелегальными или неэтичными;

10.могут призывать к действиям, выполнение которых нанесет или может нанести ущерб администрации МО "Казачье";

11.могут отрицательно влиять на производительность ИСПДн администрации МО "Казачье", включая локальную сеть и другие средства связи и обработки информации;

12.могут привести к возникновению каких-либо судебных споров или конфликтов с участием администрации МО "Казачье";

13.являются предметом авторского права, защищенного законодательством, а разрешение на их использование у отправителя в том или ином виде отсутствует.

При использовании СМНИ работникам администрации МО "Казачье" рекомендуется:

14.не хранить СМНИ вблизи промышленных и/или бытовых приборов, генерирующих сильное электромагнитное излучение или имеющих магнитный контур в своей конструкции;

15.не работать с информацией непосредственно со СМНИ;

16.во избежание потери информации отключать СМНИ средствами операционной системы (безопасное отключение СМНИ);

1. не выносить за пределы администрации МО "Казачье" СМНИ, содержащие документы и сведения, относящиеся к информации ограниченного доступа.

4.Порядок подключения СМНИ

При передаче СМНИ другим организациям или иным получателям ответственный пользователь должен пройти процедуру вывода из эксплуатации СМНИ. т.е. вывести из эксплуатации (снять с учета).

Передача СМНИ в пределах администрации МО "Казачье" третьим лицам осуществляется в соответствии с требованиями конфиденциального документооборота администрации МО "Казачье", при этом при передаче СМНИ, содержащих персональные данными, третьим лицам обязательно должен быть составлен акта приема-передачи документов (иных материальных носителей), содержащих персональные данные субъектов.

5.Ответственность

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

Контроль выполнения пользователями установленных правил эксплуатации съемных носителей персональных данных, осуществляет ответственное лицо за организацию обработки персональных данных.

Специалисты администрации МО "Казачье", нарушившие требования настоящего порядка, несут ответственность в соответствии с действующим законодательством.

**04.02.2021 г. №12**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КАЗАЧЬЕ**

**ПОСТАНОВЛЕНИЕ**

**ОБ УТВЕРЖДЕНИИ ИНСТРУКЦИИ ПО АНТИВИРУСНОЙ ЗАЩИТЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В соответствии 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 актам», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», .в соответствии с Уставом муниципального образования «Казачье», администрация муниципального образования «Казачье»

**постановляЕТ:**

1.Утвердитьинструкцию по антивирусной защите в информационных системах персональных данных (Приложение 1)

2. Настоящее постановление подлежит официальному опубликованию на официальном сайте администрации муниципального образования «Казачье» и в муниципальном Вестнике

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к постановлению

МО Казачье

от 04.02.2021 № 12

**Инструкция по антивирусной защите в информационных системах персональных данных**

Настоящая инструкция разработана с целью защиты персональных данных от несанкционированного, в том числе случайного, доступа, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

Пользователи ИСПДн при работе со съемными носителями обязаны перед началом работы осуществить их проверку на предмет наличия компьютерных вирусов.

Ответственный за обеспечение безопасности персональных данных настраивает антивирусное средство на автоматическое обновление и ведет за ним контроль.

Ответственный за обеспечение безопасности персональных данных проводит периодическое тестирование всех элементов ИСПДн и установленного программного обеспечения на предмет наличия компьютерных вирусов.

Использование для обработки и хранения персональных данных неучтенных носителей запрещается.

При обнаружении компьютерного вируса пользователи ИСПДн обязаны немедленно поставить в известность ответственного за обеспечение безопасности персональных данных и прекратить какие-либо действия в соответствующей ИСПДн.

Ответственный за обеспечение безопасности персональных данных при обнаружении компьютерного вируса принимает меры для «лечения» зараженного файла и удаления вируса и после этого вновь проводит антивирусный контроль.

В случае обнаружения на учтенном в Журнале учёта съёмных носителей персональных данных носителе вируса, не поддающегося лечению, ответственный за обеспечение безопасности персональных данных обязан:

запретить использование носителя;

поставить в известность ответственного за организацию обработки персональных данных;

запретить работу в ИСПДн;

в возможно короткие сроки обновить пакет антивирусных программ;

провести антивирусное сканирование ИСПДн.

Ответственность за поддержание установленного в настоящей инструкции порядка проведения антивирусного контроля возлагается на ответственного за обеспечение безопасности персональных данных.

**04.02.2021 г. №13**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КАЗАЧЬЕ**

**ПОСТАНОВЛЕНИЕ**

**ОБ УТВЕРЖДЕНИИ ИНСТРУКЦИИ ПО ПРОВЕДЕНИЮ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В соответствии 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 актам», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», .в соответствии с Уставом муниципального образования «Казачье», администрация муниципального образования «Казачье»

**постановляЕТ:**

1.Утвердитьинструкцию по антивирусной защите в информационных системах персональных данных (Приложение 1)

2.Настоящее постановление подлежит официальному опубликованию на официальном сайте администрации муниципального образования «Казачье» и в муниципальном Вестнике

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к постановлению

МО Казачье

от 04.02.2021 № 13

**Инструкция по антивирусной защите в информационных системах персональных данных**

1.Общие положения

Настоящая «Инструкция по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных» (далее — Инструкция) определяет порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации МО "Казачье" (далее — Оператор) в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства от 21 марта 2012 г. № 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», иными нормативными правовыми актами РФ в области защиты персональных данных.

Инструкцию обязаны выполнять все работники Оператора, допущенные к обработке персональных данных «Приказом о допуске к обработке персональных данных».

2.Порядок проведения внутреннего контроля

В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям Оператор организует проведение периодических проверок условий обработки персональных данных.

Внутренний контроль проводит ответственный за организацию обработки персональных данных (далее — Ответственный) либо комиссия по персональным данным, назначенная Оператором.

Внутренний контроль осуществляется не реже 1 раза в год. При необходимости контроль может проводиться чаще в соответствии с поручением Оператора.

Ответственный либо комиссия проводит внутренний контроль непосредственно на месте обработки персональных данных, опрашивает работников, осуществляющих обработку персональных данных, осматривает рабочие места. Все работники обязаны по запросу контролирующих предъявить все материалы и документы, числящиеся за ними, дать устные или письменные объяснения по существу заданных вопросов.

При выявлении нарушений в ходе проверки Ответственным либо Председателем комиссии:

1 создается запись в Акте контроля соответствия обработки персональных данных о мероприятиях по устранению нарушений и сроках их исполнения;

2 информация о нарушениях и о мерах для их устранения доводится до сведения руководителя организации.

В ходе внутренней проверки контролирующие проводят:

1 контроль соответствия обработки персональных данных требованиям законодательства, нормативных актов по вопросам обработки персональных данных;

2 контроль выполнения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;

3 проверку параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;

4 анализ изменения угроз безопасности персональных данных в информационной системе Оператора, возникающих в ходе её эксплуатации;

5 контроль наличия или отсутствия фактов несанкционированного доступа к персональным данным;

6 контроль соблюдения работниками, допущенными к обработке персональных данных, «Положения об обработке персональных данных», «Инструкции по порядку уничтожения и обезличивания персональных данных», «Инструкции по учёту и хранению съёмных носителей персональных данных», «Положения о порядке доступа в помещения» и других локальных актов, регламентирующих обработку персональных данных Оператора;

7 проверку «Журнала учёта съёмных носителей персональных данных»

3.Ответственность

За организацию проведения внутреннего контроля соответствия обработки персональных данных требованиям законодательства отвечает Ответственный за организацию обработки персональных данных, специалист по информационно техническому обеспечению.

Ответственность за соблюдение Инструкции возлагается на всех работников Оператора, на которых распространяется Инструкция.

**04.02.2021 г. №14**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КАЗАЧЬЕ**

**ПОСТАНОВЛЕНИЕ**

**ОБ УТВЕРЖДЕНИИ ИНСТРУКЦИИ ПО ПРОВЕДЕНИЮ ИНСТРУКТАЖА К РАБОТЕ С ИНФОРМАЦИОННОЙ СИСТЕМОЙ ЛИЦ, ДОПУЩЕННЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В соответствии Приказом ФСТЭК России от 18.02.2013 №21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", в соответствии с Уставом муниципального образования «Казачье», администрация муниципального образования «Казачье»

**постановляЕТ:**

1.Утвердитьинструкцию по проведению инструктажа лиц, допущенных к работе с информационной системой персональных данных (Приложение 1)

2.Настоящее постановление подлежит официальному опубликованию на официальном сайте администрации муниципального образования «Казачье» и в муниципальном Вестнике

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к постановлению

МО Казачье

от 04.02.2021 № 14

**Инструкция по проведению инструктажа лиц, допущенных к работе с информационной системой персональных данных**

Настоящая инструкция разработана с целью обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных администрации МО "Казачье" (далее - ИСПДн).

При поступлении на работу сотрудника, которому для выполнения своих трудовых обязанностей необходим доступ к ИСПДн (далее - новый сотрудник), ответственный за организацию обработки персональных данных:

в соответствии с п.6 ч.1 ст.18.1 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» проводит ознакомление нового сотрудника с положениями законодательства Российской Федерации о персональных данных и локальными актами организации в отношении обработки персональных данных, перечисленными в Приложении № 1 к данной инструкции;

знакомит нового сотрудника с ответственностью за неисполнение требований по обеспечению безопасности персональных данных в ИСПДн, предусмотренной действующим законодательством Российской Федерации;

отмечает в Журнале учета прохождения первичного инструктажа данные о проведении инструктажа.

Новый сотрудник может приступить к исполнению своих непосредственных трудовых обязанностей, связанных с обработкой персональных данных, только после успешного прохождения первичного инструктажа.

Приложение1

к Инструкции по проведению инструктажа лиц

допущенных к работе с информационными

системами персональных данных

Перечень законодательных актов Российской Федерации о персональных данных, документов, определяющих требования к защите персональных данных, внутренних локальных актов, определяющих политику организации в отношении обработки персональных данных, с которыми необходимо ознакомить нового сотрудника при проведении первичного инструктажа

Законодательные акты Российской Федерации о персональных данных:

1 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 21.07.2014).

2. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3. Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (для сотрудников, обрабатывающих персональные данные в том числе без использования средств автоматизации).

Внутренние локальные акты АДМИНИСТРАЦИЯ М.О. "КАЗАЧЬЕ":

1.Приказ о допуске к обработке персональных данных.

2.Политика в отношении обработки персональных данных.

3.Положение об обработке персональных данных.

4.Положение о порядке доступа в помещения, в которых ведётся обработка персональных данных.

5.Положение об обработке персональных данных без использования средств автоматизации.

6.Инструкция по учёту и хранению съёмных носителей персональных данных.

7.Инструкция по организации резервного копирования и восстановления в ИСПДн.

8.Инструкция по учёту лиц, допущенных к обработке.

9.Инструкция по антивирусной защите.

10.Инструкция по проведению инструктажа лиц, допущенных к работе с ПДн.

11.Инструкция по проведению внутреннего контроля.

12Инструкция по порядку уничтожения и обезличивания персональных данных.

13.Инструкция пользователя ИСПДн.

14.Инструкция пользователя при возникновении нештатной ситуации.

15.План проведения внутреннего контроля.

Приказ об утверждении перечня помещений, в которых ведется обработка персональных данных.

Приложение 2

К Инструкции по проведению инструктажа лиц,

допущенных к работе с информационными

системами персональных данных

**Журнал учёта** **прохождения первичного инструктажа работниками, допущенными к работе с пдн в испдн**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №п/п | ФИО работника | Датапрохожденияинструктажа | Подписьработника | ФИО должностного лица, проводившего инструктаж | Подписьдолжностноголица |
| 1 | 2 | 3 | 4 | 5 | 6 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**04.02.2021 г. №15**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КАЗАЧЬЕ**

**ПОСТАНОВЛЕНИЕ**

**ОБ УТВЕРЖДЕНИИ ИНСТРУКЦИИ ПО ОРГАНИЗАЦИИ РЕЗЕРВИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, БАЗ ПЕРСОНАЛЬНЫХ ДАННЫХ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В соответствии Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», в соответствии с Уставом муниципального образования «Казачье», администрация муниципального образования «Казачье»

**постановляЕТ:**

1.Утвердить инструкцию по организации резервирования и восстановления программного обеспечения, баз персональных данных информационной системы персональных данных (Приложение 1)

2.Настоящее постановление подлежит официальному опубликованию на официальном сайте администрации муниципального образования «Казачье» и в муниципальном Вестнике

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к постановлению

МО Казачье

от 04.02.2021 № 15

**Инструкция по организации резервирования и восстановления программного обеспечения, баз персональных данных информационной системы персональных данных**

Настоящая инструкция разработана с целью обеспечения возможности незамедлительного восстановления персональных данных в информационной системе персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационной системы персональных данных администрации МО "Казачье".

Резервированию подлежат базы данных и файлы, содержащие персональные данные.

Резервирование выполняется штатным средством архивирования системы и данных и производится на локальный дисковый массив. Процедура резервного копирования производится каждый день.

Ответственным за процедуру резервирования и восстановления назначается ответственный за организацию обработки персональных данных.

Восстановление файлов производится путем разархивирования файлов базы данных в исходный каталог.

**04.02.2021 г. №16**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КАЗАЧЬЕ**

**ПОСТАНОВЛЕНИЕ**

**ОБ УТВЕРЖДЕНИИ ИНСТРУКЦИИ ПО УЧЕТУ ЛИЦ, ДОПУЩЕННЫХ К РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В соответствии Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», в соответствии с Уставом муниципального образования «Казачье», администрация муниципального образования «Казачье»

**постановляЕТ:**

1.Утвердить инструкцию по учету лиц, допущенных к работе с персональными данными в информационных системах персональных данных (Приложение 1)

2.Настоящее постановление подлежит официальному опубликованию на официальном сайте администрации муниципального образования «Казачье» и в муниципальном Вестнике

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к постановлению

МО Казачье

от 04.02.2021 № 16

**Инструкция по учету лиц, допущенных к работе с персональными данными в информационных системах персональных данных**

Настоящая инструкция определяет порядок учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных АДМИНИСТРАЦИЯ М.О. "КАЗАЧЬЕ" (далее - ИСПДн).

Порядок допуска работника к работе с персональными данными:

1.утверждение приказом о допуске к обработке персональных данных перечня должностей работников, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей (далее - Перечень);

2.прохождение первичного инструктажа, включающего ознакомление со всеми нормативными документами, регламентирующими работу с персональными данными, согласно Инструкции по проведению инструктажа лиц, допущенных к работе с персональными данными с внесением соответствующей информации в Журнал учёта прохождения первичного инструктажа сотрудниками, допущенными к работе с персональными данными в ИСПДН;

3.внесение записи в Журнал учёта прав доступа к ИСПДн.

Допуск работника к персональным данным прекращается:

4.в случае обнаружения нарушений порядка обработки персональных данных до выяснения и устранения причин нарушений;

5.в случае увольнения сотрудника с момента подписания приказа об увольнении;

6.при изменении его служебных обязанностей с момента утверждения нового Перечня.

**04.02.2021 г. №17**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КАЗАЧЬЕ**

**ПОСТАНОВЛЕНИЕ**

**ОБ УТВЕРЖДЕНИИ ИНСТРУКЦИИ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ**

В соответствии с 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 актам», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», в соответствии с Уставом муниципального образования «Казачье», администрация муниципального образования «Казачье»

**постановляЕТ:**

1.Утвердить инструкцию пользователя информационной системы (Приложение 1)

2.Настоящее постановление подлежит официальному опубликованию на официальном сайте администрации муниципального образования «Казачье» и в муниципальном Вестнике

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к постановлению МО Казачье

от 04.02.2021 № 17

**Инструкция пользователя информационной системы**

Пользователем информационной системы персональных данных администрации МО "Казачье" (далее - Пользователь) является любой работник администрации МО "Казачье", осуществляющий обработку персональных данных в информационной системе персональных данных администрации МО "Казачье" (далее - ИСПДн).

Согласно ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» обработка ПДн - 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 (далее - ПДн).

Пользователь в своей работе руководствуется настоящей Инструкцией, Положением об обеспечении безопасности ПДн, руководящими и нормативными документами ФСТЭК и ФСБ России и внутренними нормативными актами администрации МО "Казачье", с которыми он был ознакомлен при прохождении первичного инструктажа. Пользователь несет персональную ответственность за свои действия.

Пользователь обязан:

* знать и выполнять требования Положения об обработке данных, Политики в отношении обработки данных, других локальных актов оператора в отношении персональных данных;
* знать и выполнять установленные требования по режиму обработки ПДн, учету, хранению и использованию носителей ПДн, обеспечению безопасности ПДн;
* соблюдать требования парольной политики;
* блокировать АРМ в случае отсутствия на рабочем месте;
* оповещать ответственного за обеспечение безопасности ПДн о фактах нарушения информационной безопасности и возникновения нештатных ситуаций;
* при возникновении нештатных и аварийных ситуаций действовать согласно Инструкции пользователя при возникновении нештатных ситуаций с целью ликвидации их последствий и возможного ущерба.

Пользователю запрещается:

* разглашать обрабатываемые ПДн;
* производить несанкционированное копирование ПДн на учтенные носители;
* производить копирование ПДн на неучтенные носители;
* оставлять незаблокированным АРМ при отсутствии на рабочем месте;
* сообщать и передавать третьим лицам личные пароли и атрибуты доступа к ресурсам ИСПДн.

За нарушение информационной безопасности Пользователь несет ответственность согласно действующему законодательству Российской Федерации.

**04.02.2021 г. №18**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КАЗАЧЬЕ**

**ПОСТАНОВЛЕНИЕ**

**ОБ УТВЕРЖДЕНИИ ИНСТРУКЦИИ ПОЛЬЗОВАТЕЛЯ ПРИ НЕШТАТНОЙ СИТУАЦИИ**

В соответствии с Приказом ФСТЭК России от 18.02.2013 №21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", в соответствии с Уставом муниципального образования «Казачье», администрация муниципального образования «Казачье»

**постановляЕТ:**

1.Утвердить инструкцию пользователя при нештатной ситуации (Приложение 1)

2.Настоящее постановление подлежит официальному опубликованию на официальном сайте администрации муниципального образования «Казачье» и в муниципальном Вестнике

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к постановлению

МО Казачье

от 04.02.2021 № 18

**Инструкция пользователя при нештатной ситуации**

Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием информационных систем персональных данных администрации МО "Казачье" (далее - ИСПДн), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания работоспособности в случае реализации рассматриваемых угроз.

Задачами данной Инструкции являются:

1.определение мер защиты от прерывания работоспособности;

2.определение действий по восстановлению в случае прерывания работоспособности.

3.Действие настоящей Инструкции распространяется на всех пользователей ИСПДн, имеющих доступ к ресурсам ИСПДн, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

4.системы жизнеобеспечения;

5.системы обеспечения отказоустойчивости;

6.системы резервного копирования и хранения данных;

7.системы контроля физического доступа.

Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении № 1.

При реагировании на инцидент важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

Уровень 1. Незначительный инцидент - локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты;

Уровень 2. Авария - любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты;

Уровень 3. Катастрофа - любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, к уничтожению, блокированию, неправомерной модификации или компрометации защищаемых персональных данных, а также к угрозе жизни пользователей ИСПДн.

При возникновении нештатной ситуации любого уровня пользователь обязан оповестить ответственного за организацию обработки персональных данных, сообщив характер аварийной ситуации, масштаб ситуации по предварительной субъективной оценке.

Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за организацию обработки персональных данных в Журнале регистрации фактов нарушения и восстановления работоспособности оборудования или ИСПДн. В кратчайшие сроки, не превышающие одного рабочего дня, должны быть предприняты меры по восстановлению работоспособности ИСПДн.

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные (программно-аппаратные) и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

системы жизнеобеспечения;

системы обеспечения отказоустойчивости;

системы резервного копирования и хранения данных;

системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

пожарные сигнализации и системы пожаротушения;

системы вентиляции и кондиционирования;

системы резервного питания.

Все критичные помещения, в которых размещаются элементы ИСПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Ответственный за организацию обработки персональных данных:

ознакомляет всех сотрудников, находящихся в его зоне ответственности, с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу;

обучает пользователей, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций.

Пользователи ИСПДн должны получить базовые знания в следующих областях:

оказание первой медицинской помощи;

пожаротушение;

эвакуация людей;

защита материальных и информационных ресурсов;

методы оперативной связи со службами спасения и руководителями структурных подразделений;

выключение оборудования, электричества, водоснабжения, газоснабжения;

Навыки и знания пользователей ИСПДн по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение пользователей ИСПДн порядку действий при возникновении аварийной ситуации. Ответственность за организацию обучения пользователей ИСПДн несет ответственный за организацию обработки персональных данных. Глава администрации администрации МО "Казачье" согласует сроки и порядок их обучения.

Приложение1

К Инструкции пользователя

при нештатной ситуации

**Источники угроз безопасности персональных данных**

Технологические угрозы:

Пожар в здании;

Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения);

Взрыв (бытового газа, взрывчатых веществ или приборов, работающих под давлением);

Химический выброс в атмосферу.

Внешние угрозы:

Массовые беспорядки;

Сбои общественного транспорта;

Эпидемия;

Массовое отравление персонала;

Теракт.

Стихийные бедствия:

Удар молнии;

Сильный снегопад;

Сильные морозы;

Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания;

Затопление водой в период паводка;

Наводнение, вызванное проливным дождем;

Торнадо;

Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод).

ИТ-угрозы:

Сбой системы кондиционирования в серверном помещении;

Выход из строя файлового сервера;

Частичная потеря информации на сервере без потери его работоспособности;

Выход из строя локальной сети;

Выход из строя рабочей станции;

Частичная потеря информации на рабочей станции без потери её работоспособности. Угроза, связанная с человеческим фактором:

Ошибка персонала, имеющего доступ к элементам ИСПДн;

Нарушение конфиденциальности, целостности и доступности конфиденциальной информации, а также несанкционированные действия, заблокированные средствами защиты и зафиксированные средствами регистрации.

Угрозы, связанные с внешними поставщиками:

Отключение электроэнергии;

Сбой в работе интернет-провайдера;

Физический разрыв внешних каналов связи.

**04.02.2021 г. №19**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КАЗАЧЬЕ**

**ПОСТАНОВЛЕНИЕ**

**ОБ УТВЕРЖДЕНИИ МАТРИЦИ ДОСТУПА**

**К ИНФОРМАЦИОННЫМ СИСТЕМАМ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В соответствии с 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 актам», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», в соответствии с Уставом муниципального образования «Казачье», администрация муниципального образования «Казачье»

**постановляЕТ:**

1.Утвердить Матрицу доступа к информационным системам персональных данных (Приложение 1)

2.Настоящее постановление подлежит официальному опубликованию на официальном сайте администрации муниципального образования «Казачье» и в муниципальном Вестнике

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к постановлению

МО Казачье

от 04.02.2021 № 19

**Матрица доступа к информационным системам персональных данных**

Таблица 1. Описание ролей пользователей информационной системы

|  |  |  |
| --- | --- | --- |
| Группа | Уровень доступа к ПДн | Разрешенные действия |
| Администраторы ИСПДн | Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн.Обладает полной информацией о технических средствах и конфигурации ИСПДн.Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн.Обладает правами конфигурирования и административной настройки технических средств ИСПДн. | сборсистематизациянакоплениехранениеуточнениеиспользованиеуничтожение |
| Администратор безопасности | Обладает правами Администратора ИСПДн.Обладает полной информацией об ИСПДн.Имеет доступ к средствам защиты информации ипротоколирования и к части ключевых элементов ИСПДн.Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных). | сборсистематизациянакоплениехранениеуточнениеиспользованиеуничтожение |
| Операторы ИСПДн | Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн. | сборсистематизациянакоплениехранениеуточнениеиспользованиеуничтожениеиспользование |

Таблица 2. Матрица доступак информационным системам персональных данных

|  |  |  |  |
| --- | --- | --- | --- |
| №п/п | Должности пользователей | Роль | Перечень информационных, технический и программных ресурсов |
| Средства конфигурированиясредств защиты информации | Файловая система жесткого диска | Открытая сеть | Закрытая сеть | Привод оптический дисков | Системное и прикладное ПО |
| 1 | Глава администрации; Исполняющий обязанности ответственного за организацию обработки персональных данных | Администраторы ИСПДн | Полный доступ | Полный доступ | Нет доступа | Полный доступ | Полный доступ | Полный доступ |
| 2 | Исполняющий обязанности ответственного за обеспечение безопасности персональных данных | Администратор безопасности | Нет доступа | Чтение, запись | Нет доступа | Полный доступ | Полный доступ | Запуск на выполнение |
| 3 | Прочие должности, согласно приказу“Об утверждении перечня лиц, допущенных к обработкезащищаемой информации в информационной системе персональных данных” | Оператор | Нет | Чтение, запись | Нет | Полный доступ | Полный доступ | Запуск на выполнение |

**04.02.2021 г. №20**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КАЗАЧЬЕ**

**ПОСТАНОВЛЕНИЕ**

**ОБ УТВЕРЖДЕНИИ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В соответствии с п.1) п.2 ст.19 Федерального закона №152 "О персональных данных", "Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (ФСТЭК), "Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (ФСТЭК), Постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 г. "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Приказом ФСТЭК №21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", Приказом ФСБ России от 10 июля 2014 г. №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", Приказом ФСТЭК России от 11.02.2013 №17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, в соответствии с Уставом муниципального образования «Казачье», администрация муниципального образования «Казачье»

**постановляЕТ:**

1.Утвердить Модель угроз безопасности персональных данных (Приложение 1)

2.Настоящее постановление подлежит официальному опубликованию на официальном сайте администрации муниципального образования «Казачье» и в муниципальном Вестнике

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к постановлению

МО Казачье

от 04.02.2021 № 20

**Модель угроз безопасности персональных данных**

Определения

В настоящем документе используются следующие термины и их определения.

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

Аутентификация отправителя данных – подтверждение того, что от­правитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персо­нальных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, це­лостность и доступность персональных данных при их обработке в информа­ционных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами не­санкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но со­храняют способность к дальнейшему распространению и самовоспроизведе­нию.

Вредоносная программа – программа, предназначенная для осуществ­ления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические сред­ства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средст­вами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персо­нальных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных про­грамм.

Доступ к информации – возможность получения информации и ее ис­пользования.

Закладочное устройство – элемент средства съема информации, скрыт­но внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, пред­меты интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом соб­ственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информа­ции.

Идентификация – присвоение субъектам и объектам доступа иденти­фикатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, элек­тромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабаты­ваемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хра­нения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, мате­риальный объект или физическое явление, являющиеся причиной возникно­вения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторон­них лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблю­дения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функциональ­но-распределенное программное (программно-аппаратное) средство (ком­плекс), реализующее контроль за информацией, поступающей в информаци­онную систему персональных данных и (или) выходящей из информацион­ной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных дан­ных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой ин­формации.

Несанкционированный доступ (несанкционированные действия) – дос­туп к информации или действия с информацией, нарушающие правила раз­граничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, коли­чественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональ­ными данными, включая сбор, систематизацию, накопление, хранение, уточ­нение (обновление, изменение), использование, распространение (в том чис­ле передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридиче­ское или физическое лицо, организующее и (или) осуществляющее обработ­ку персональных данных, а также определяющие цели и содержание обра­ботки персональных данных.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, пе­реговорные и телевизионные устройства, средства изготовления, тиражиро­вания документов и другие технические средства обработки речевой, графи­ческой, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) – неправомерное получение информации с ис­пользованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определен­ному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущест­венное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возни­кающие как побочное явление и вызванные электрическими сигналами, дей­ствующими в их электрических и магнитных цепях, а также электромагнит­ные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламенти­рующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппа­ратные средства.

Программное (программно-математическое) воздействие – несанкцио­нированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и тех­нических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого рег­ламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя ин­формации (средства обработки), физической среды распространения инфор­мативного сигнала и средств, которыми добывается защищаемая информа­ция.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случай­ного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение пер­сональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информаци­онной системе персональных данных или в результате которых уничтожают­ся материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – некон­тролируемое распространение информации от носителя защищаемой инфор­мации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – слабость в средствах защиты, которую можно использо­вать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной тех­ники или автоматизированной системы обеспечивать неизменность инфор­мации в условиях случайного и/или преднамеренного искажения (разрушения).

Обозначения и сокращения

АВС – антивирусные средства

АРМ – автоматизированное рабочее место

ВТСС – вспомогательные технические средства и системы

ИСПДн – информационная система персональных данных

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

САЗ – система анализа защищенности

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

СОВ – система обнаружения вторжений

ТКУ И – технические каналы утечки информации

УБПДн – угрозы безопасности персональных данных

Введение

Модель угроз безопасности персональных данных (далее – Модель) при их обработке в ИСПДнАДМИНИСТРАЦИЯ М.О. "КАЗАЧЬЕ" строится на основании следующих документов:

- Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации";

- Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных";

- Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119;

- Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";

В модели угроз представлено описание структуры ИСПДн, состава и режима обработки ПДн, классификацию потенциальных нарушителей, оценку исходного уровня защищенности, анализ угроз безопасности персональных данных.

Модель угроз является методическим документом и предназначена для должностных и ответственных лиц оператора персональных данных, администраторов ИСПДн, разработчиков ИСПДн и их подсистем.

* Анализ УБПДн включает:
* Описание угроз.
* Оценку вероятности возникновения угроз.
* Оценку реализуемости угроз.
* Оценку опасности угроз.
* Определение актуальности угроз.

В заключении даны рекомендации по мерам защиты для уменьшения опасности актуальных угроз.

1.Описание ИСПДн

ИСПДн позволяет осуществлять сбор, хранение, использование и уничтожение персональных данных, содержащих информацию, позволяющую получить дополнительную информацию о субъекте персональных данных.

Состав ПО ИСПДн

Для данной ИСПДн в целом необходимо обеспечить следующие характеристики безопасности информации – конфиденциальность, целостность.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного воздействия.

2. Пользователи

В АДМИНИСТРАЦИЯ М.О. "КАЗАЧЬЕ" обработка персональных данных осуществляется в многопользовательском режиме с разграничением прав доступа.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в виде матрицы доступа в таблице 2.

Таблица 1– Матрица доступа

|  |  |  |
| --- | --- | --- |
| Группа | Уровень доступа к ПДн | Разрешенные действия |
| Администратор ИСПДн | Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн.Обладает полной информацией о технических средствах и конфигурации ИСПДн.Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн.Обладает правами конфигурирования и административной настройки технических средств ИСПДн. | - сбор- систематизация- накопление- хранение- уточнение- использование- уничтожение |
| Администратор безопасности | Обладает правами Администратора ИСПДн.Обладает полной информацией об ИСПДн.Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных). | - сбор- систематизация- накопление- хранение- уточнение- использование- уничтожение |
| Оператор ИСПДн | Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн. | - сбор- систематизация- накопление- хранение- уточнение- использование- уничтожение |

Предоставление или прекращение доступа к ИСПДн осуществляется в соответствии с приказом о назначении на должность или приказом об увольнении.

3. Тип ИСПДн

Таблица 3 – Параметры ИСПДн

|  |  |
| --- | --- |
| Заданные характеристики безопасности персональных данных | Типовая информационная система |
| Структура информационной системы | Локальная информационная система |
| Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена | Имеется |
| Режим обработки персональных данных | Многопользовательская система |
| Режим разграничения прав доступа пользователей | С разграничением доступа |
| Местонахождение технических средств информационной системы | Все технические средства находятся в пределах Российской Федерации |
| Дополнительная информация | К персональным данным предъявляется требование целостности и (или) доступности |

ЛИС II типа – локальная информационная система, имеющая подключение к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы, с разграничением прав доступа.

**4.** **Исходный уровень защищенности ИСПДн**

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

В таблице представлены характеристики уровня исходной защищенности для ИСПДн АДМИНИСТРАЦИЯ М.О. "КАЗАЧЬЕ" .

Таблица 2 – Исходный уровень защищенности

|  |  |  |
| --- | --- | --- |
| Позиция | Технические и эксплуатационные характеристики | Уровеньзащищенности |
| 1 | По территориальному размещению | Высокий |
| 2 | По наличию соединения с сетями общего пользования | Средний |
| 3 | По встроенным (легальным) операциям с записями баз персональных данных | Низкий |
| 4 | По разграничению доступа к персональным данным | Средний |
| 5 | По наличию соединений с другими базами ПДн иных ИСПДн | Высокий |
| 6 | По уровню (обезличивания) ПДн | Низкий |
| 7 | По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки | Высокий |

Определение исходной степени защищенности:

1. ИСПДн имеет высокий уровень исходной защищенности, если не менее 70 % характеристик соответствуют уровню «высокий»;

2. ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70 % характеристик ИСПДн соответствуют уровню не ниже «средний»;

3. ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

Таблица 4

| № п/п | Значение характеристики (уровень защищенности) | Количество значений | Процент значений не ниже данного уровня |
| --- | --- | --- | --- |
| 1 | Высокий | 3 | 42% |
| 2 | Средний | 2 | 29% |
| 3 | Низкий | 2 | 29% |

В соответствии с полученными данными устанавливается средний показатель исходной защищенности, значение коэффициента Y1=5.

5. Вероятность реализации угроз безопасности

5.1 Классификация угроз безопасности

Перечень угроз, уязвимостей и технических каналов утечки информации сформирован в соответствии с требованиями руководящих документов ФСТЭК России.

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн обрабатываемым в ИСПДн.

ИСПДн Учреждения представляет собой совокупность информационных и программно-аппаратных элементов и их особенностей как объектов обеспечения безопасности. Основными элементами ИСПДн являются:

* персональные данные, обрабатываемые в ИСПДн;
* информационные технологии, как совокупность приемов, способов и методов применения средств вычислительной техники при обработке ПДн;
* технические средства ИСПДн, осуществляющие обработку ПДн (средства вычислительной техники (СВТ), информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн;
* программные средства (операционные системы, системы управления базами данных и т.п.);
* средства защиты информации (СЗИ), включая СКЗИ;
* вспомогательные технические средства и системы (технические средства и системы, их коммуникации, не предназначенные для обработки ПДн, но размещенные в помещениях, в которых расположены ИСПДн, такие как средства вычислительной техники, средства и системы охранной и пожарной сигнализации, средства и системы кондиционирования, средства электронной оргтехники и т.п.) (далее - ВТСС);
* документация на СКЗИ и на технические и программные компоненты ИСПДн;
* ключевая, аутентифицирующая и парольная информация;
* помещения, в которых находятся защищаемые ресурсы.

Возможности источников УБПДн обусловлены совокупностью методов и способов несанкционированного и (или) случайного доступа к ПДн, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн.

Угроза безопасности ПДн реализуется в результате образования канала реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает необходимые условия для нарушения безопасности ПДн (несанкционированный или случайный доступ).

Основными элементами канала реализации УБПДн являются:

* источник УБПДн – субъект, материальный объект или физическое явление, создающиеУБПДн;
* среда (путь) распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) ПДн;
* носитель ПДн – физическое лицо или материальный объект, в том числе физическое поле, в котором ПДн находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Источниками угроз НСД в ИСПДн могут быть:

* нарушитель;
* носитель вредоносной программы.

5.2 Классификация нарушителей

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных утечку информации по техническим каналам утечки.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи.

Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа.

Система разграничения доступа ИСПДн обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

администраторы ИСПДн (категория I);

администраторы конкретных подсистем или баз данных ИСПДн (категория II);

пользователи ИСПДн (категория III);

пользователи, являющиеся внешними по отношению к конкретной АС (категория IV);

лица, обладающие возможностью доступа к системе передачи данных (категория V);

сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ИСПДн, но не имеющие права доступа к ним (категория VI);

обслуживающий персонал ЛПУ (охрана, работники инженерно–технических служб и т.д.) (категория VII);

уполномоченный персонал разработчиков ИСПДн, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн (категория VIII).

На лиц категорий I и II возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПДн для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПДн. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн, включая средства защиты, используемые в конкретных АС, в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

К лицам категорий I и II ввиду их исключительной роли в ИСПДн должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-VIII относятся к вероятным нарушителям.

Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

Предположения об имеющейся у нарушителя информации об объектах реализации угроз

В качестве основных уровней знаний нарушителей об АС можно выделить следующие:

*общая информация* – информации о назначения и общих характеристиках ИСПДн;

*эксплуатационная информация –* информация, полученная из эксплуатационной документации;

*чувствительная информация* – информация, дополняющая эксплуатационную информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может иметь:

данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;

сведения об информационных ресурсах ИСПДн: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;

данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПДн;

данные о реализованных в ПСЗИ принципах и алгоритмах;

исходные тексты программного обеспечения ИСПДн;

сведения о возможных каналах реализации угроз;

информацию о способах реализации угроз.

Предполагается, что лица категории III и категории IV владеют только эксплуатационной информацией, что обеспечивается организационными мерами. При этом лица категории IV не владеют парольной, аутентифицирующей и ключевой информацией, используемой в АИС, к которым они не имеют санкционированного доступа.

Предполагается, что лица категории V владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией об АИС, использующих эту систему передачи информации, что обеспечивается организационными мерами. При этом лица категории V не владеют парольной и аутентифицирующей информацией, используемой в АИС.

Предполагается, что лица категории VI и лица категории VII по уровню знаний не превосходят лица категории V.

Предполагается, что лица категории VIII обладают чувствительной информацией об ИСПДн и функционально ориентированных АИС, включая информацию об уязвимостях технических и программных средств ИСПДн. Организационными мерами предполагается исключить доступ лиц категории VIII к техническим и программным средствам ИСПДн в момент обработки с использованием этих средств защищаемой информации.

Таким образом, наиболее информированными об АИС являются лица категории III и лица категории VIII.

Степень информированности нарушителя зависит от многих факторов, включая реализованные в ЛПУ конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания определенного запаса прочности предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет:

- аппаратные компоненты СЗПДн и СФ СЗПДн;

- доступные в свободной продаже технические средства и программное обеспечение;

- специально разработанные технические средства и программное обеспечение.

Внутренний нарушитель может использовать штатные средства*.*

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные на объектах ЛПУ конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для создания устойчивой СЗПДн предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

- средств перехвата в технических каналах утечки;

- средств воздействия через сигнальные цепи;

- средств воздействия на источники и через цепи питания;

- средств воздействия через цепи заземления;

- средств активного воздействия на технические средства (средств облучения).

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории III и лица категории VIII.

5.3 Классификация уязвимостей ИСПДн

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности персональных данным.

Причинами возникновения уязвимостей являются:

* ошибки при проектировании и разработке программного (программно-аппаратного) обеспечения;
* преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения;
* неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;
* несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
* внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;
* несанкационированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;
* сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

Различают следующие группы основных уязвимостей:

* уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);
* уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

5.4 Перечень возможныхУБПДн

Для ИСПДн Учреждения можно выделить следующие угрозы:

1. Угрозы от утечки по техническим каналам.

1.1. Угрозы утечки акустической информации.

1.2. Угрозы утечки видовой информации.

1.3. Угрозы утечки информации по каналам ПЭМИН.

2. Угрозы несанкционированного доступа к информации.

2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн.

2.1.1. Кража ПЭВМ;

2.1.2. Кража носителей информации;

2.1.3. Кража ключей и атрибутов доступа;

2.1.4. Кражи, модификации, уничтожения информации;

2.1.5. Вывод из строя узлов ПЭВМ, каналов связи;

2.1.6. Несанкционированное отключение средств защиты.

2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).

2.2.1. Действия вредоносных программ (вирусов);

2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных;

2.2.3. Установка ПО не связанного с исполнением служебных обязанностей.

2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

2.3.1. Утрата ключей и атрибутов доступа;

2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками;

2.3.3. Непреднамеренное отключение средств защиты;

2.3.4. Выход из строя аппаратно-программных средств;

2.3.5. Сбой системы электроснабжения;

2.3.6. Стихийное бедствие.

2.4. Угрозы преднамеренных действий внутренних нарушителей.

2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке;

2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке.

2.5. Угрозы несанкционированного доступа по каналам связи.

2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:

2.5.1.1. Перехват за переделами с контролируемой зоны;

2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;

2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.

2.5.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.

2.5.3. Угрозы выявления паролей по сети.

2.5.4. Угрозы навязывание ложного маршрута сети.

2.5.5. Угрозы подмены доверенного объекта в сети.

2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.

2.5.7. Угрозы типа «Отказ в обслуживании».

2.5.8. Угрозы удаленного запуска приложений.

2.5.9. Угрозы внедрения по сети вредоносных программ.

5. 5 Вероятность реализации УБПДн

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);

низкая вероятность- объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);

средняя вероятность *-* объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2 = 5);

высокая вероятность *-* объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2 = 10).

5.5.1 Угрозы утечки информации по техническим каналам

5.5.1.1 Угрозы утечки акустической (речевой) информации.

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

В ИСПДн функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют.

Вероятность реализации угрозы – маловероятна.

5.5.1.2 Угрозы утечки видовой информации.

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео и буквенно-цифровой информации, входящих в состав ИСПДн.

На окнах используются жалюзи и занавески. Доступ посторонних лиц в помещения, в которых производится обработка ПДН, ограничен.

Вероятность реализации угрозы – маловероятна.

5.5.1.3 Угрозы утечки информации по каналам ПЭМИН.

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия паразитных электромагнитных излучений у элементов ИСПДн.

Угроза утечки информации, содержащей ПДн, по каналу ПЭМИН возможна, за счет перехвата техническими средствами разведки за пределами контролируемой зоны ПЭМИН, возникающих при обработке ПДн средствами вычислительной техники ИСПДн. Наиболее опасным режимом работы средств вычислительной техники является вывод информации на экран монитора автоматизированного рабочего места оператора (пользователя) ИСПДн.

Элементы ИСПДн находятся в самом центре здания и экранируются несколькими несущими стенами, и паразитный сигнал маскируется с множеством других паразитных сигналов элементов не входящих в ИСПДн.

Вероятность реализации угрозы – маловероятна.

5.5.2. Угрозы несанкционированного доступа к информации

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

-нарушению конфиденциальности (копирование, неправомерное распространение);

-нарушению целостности (уничтожение, изменение);

-нарушению доступности (блокирование).

5.5.2.1 Угрозы уничтожения, хищения аппаратных средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн

*Кража ПЭВМ.*

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещениях, где расположены элементы ИСПДн.

В Учреждении введен контроль доступа. Ключи от серверного помещения учреждения хранятся у системного администратора. Кабинеты пользователей запираются на ключи.

Вероятность реализации угрозы – маловероятна.

*Кража носителей информации*

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации. В результате возможно несанкционированное копирование разделов системы хранения данных штатными средствами на съемные устройства хранения.

В Учреждении введен контроль доступа. Ключи от серверного помещения учреждения хранятся у системного администратора. Кабинеты пользователей запираются на ключи.Хранение носителей осуществляется в сейфе.

Доступ к техническим средствам ИСПДн при обслуживании возможен только под контролем со стороны системного администратора. Переносные компьютеры для обработки ПДН в ИСПДН не используются.

Вероятность реализации угрозы – маловероятна.

*Кража ключей и атрибутов доступа.*

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещениях, где происходит работа пользователей.

В Учреждении введен контроль доступа. Ключи от серверного помещения учреждения хранятся у системного администратора. Кабинеты пользователей запираются на ключи.

Вероятность реализации угрозы – маловероятна.

*Кражи, модификации, уничтожения информации*

Угроза осуществляется путём НСД внешними и внутренними нарушителями в помещениях, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

В Учреждении введен контроль доступа. Ключи от серверного помещения учреждения хранятся у системного администратора. Кабинеты пользователей запираются на ключи.

Вероятность реализации угрозы – маловероятна.

*Вывод из строя узлов ПЭВМ и каналов связи*

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и проходят каналы связи.

В Учреждении введен контроль доступа. Ключи от серверного помещения учреждения хранятся у системного администратора. Кабинеты пользователей запираются на ключи.

Вероятность реализации угрозы – маловероятна.

*Несанкционированное отключение средств защиты.*

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещениях, где расположены средства защиты ИСПДн.

В Учреждении введен контроль доступа. Ключи от серверного помещения учреждения хранятся у системного администратора. Кабинеты пользователей запираются на ключи.

Возможность отключения или изменения настроек СЗИ пользователем запрещена. Настройка средств разграничения доступа к ресурсам ИСПДн производится системным администратором.

Вероятность реализации угрозы – маловероятна.

5.5.2.2 Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).

*Действия вредоносных программ (вирусов).*

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

- скрывать признаки своего присутствия в программной среде компьютера;

- обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

- разрушать (искажать произвольным образом) код программ в оперативной памяти;

- выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);

- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

- искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

В Учреждении на всех элементах ИСПДн установлена антивирусная защита, пользователи проинструктированы о мерах предотвращения вирусного заражения.

Вероятность реализации угрозы – *является низкой*.

*Недекларированные возможности системного ПО и ПО для обработки персональных данных.*

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Вероятность реализации угрозы повышается:

* при увеличении элементов, в том числе программного обеспечения, ИСПДн;
* при увеличении числа функциональных связей между элементами;
* наличии подключения к сетям общего доступа и (или) международного обмена.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 5.

Таблица 5

|  |  |  |
| --- | --- | --- |
| Тип ИСПДн | Вероятность реализации угрозы | Коэфф. вероятности реализации угрозы нарушителем |
| Автономная ИС I типа | маловероятная | 0 |
| Автономная ИС II типа | маловероятная | 0 |
| Автономная ИС III типа | маловероятная | 0 |
| Автономная ИС IV типа | маловероятная | 0 |
| Автономная ИС V типа | маловероятная | 0 |
| Автономная ИС VI типа | маловероятная | 0 |
| ЛИС I типа | маловероятная | 0 |
| ЛИС II типа | низкая | 2 |
| Распределенная ИС I типа | низкая | 2 |
| Распределенная ИС II типа | низкая | 2 |

В случае если в обработке персональных данных участвует ПО собственной разработки или стандартное ПО, доработанное под нужды учреждения, то следует повысить значение вероятности реализации угрозы:

* для всех типов ИСПДн, кроме Автономная ИС I типа, на порядок;
* для Распределенной ИС II типа на два порядка.

В данном случае рассматривается Локальная ИС II типа.

Вероятность реализации угрозы – является низкой.

*Установка ПО не связанного с исполнением служебных обязанностей*

Угроза осуществляется путем несанкционированной установки ПОвнутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.

В Учреждении введено разграничение правами пользователей на установку ПО и осуществляется контроль, пользователи проинструктированы о политике установки ПО.

Вероятность реализации угрозы –маловероятна.

5.5.2.3 Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

*Утрата ключей и атрибутов доступа.*

Угроза может осуществляться за счет человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политики в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

В Учреждении введена парольная политика, предусматривающая сложность пароля и периодическую его смену, введена политика «чистого стола». Пользователи проинструктированы о парольной политике и о действиях в случае утраты или компрометации паролей.

Вероятность реализации угрозы – является низкой.

*Непреднамеренная модификация (уничтожение) информации сотрудником.*

Угроза может осуществляться за счет человеческого фактора пользователей ИСПДн, которые нарушают правила работы с конфиденциальной информацией.

Перед началом работы каждый пользователь изучает Инструкцию пользователя. В Учреждении осуществляется резервное копирование обрабатываемыхПДн, пользователи проинструктированы о работе с ИСПДн.

Вероятность реализации угрозы – маловероятна.

*Непреднамеренное отключение средств защиты*

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и средствами защиты или не осведомлены о них.

В Учреждении введен контроль доступа в контролируемую зону, двери закрываются на замок, осуществляется разграничение доступа к настройкам режимов средств защиты, пользователи проинструктированы о работе с ИСПДн,

Вероятность реализации угрозы - маловероятна.

*Выход из строя аппаратно-программных средств*

Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации.

В Учрежденииосуществляется резервное копирование информации.

Вероятность реализации угрозы – маловероятна.

*Сбой системы электроснабжения*

Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации.

В Учреждении ко всем ключевым элементам ИСПДн подключены источники бесперебойного питания и осуществляется резервное копирование информации.

Вероятность реализации угрозы – маловероятна.

*Стихийное бедствие*

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

В Учреждении установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций.

Вероятность реализации угрозы – маловероятна.

5.5.2.4 Угрозы преднамеренных действий внутренних нарушителей

*Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке*

Угроза осуществляется путем НСД внешних нарушителей в помещения, где расположены элементы ИСПДн и средства защиты, а так же происходит работа пользователей.

В Учреждении введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – маловероятна.

*Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке*

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.

В Учреждении пользователи осведомлены о порядке работы с персональными данными, а так же подписали Соглашение о неразглашении.

Вероятность реализации угрозы – является низкой.

5.5.2.5 Угрозы несанкционированного доступа по каналам связи

В соответствии с «Типовой моделью угроз безопасности персональных данных, обрабатываемых в распределенных ИСПДн, имеющих подключение к сетям общего пользования и (или) международного информационного обмена» (п. 6.6.Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 г.), для ИСПДн можно рассматривать следующие угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:

* угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;
* угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;
* угрозы выявления паролей по сети;
* угрозы навязывание ложного маршрута сети;
* угрозы подмены доверенного объекта в сети;
* угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;
* угрозы типа «Отказ в обслуживании»;
* угрозы удаленного запуска приложений;
* угрозы внедрения по сети вредоносных программ.

*Угроза «Анализ сетевого трафика»*

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль. В ходе реализации угрозы нарушитель:

* изучает логику работы ИСПДн - то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней;
* перехватывает поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающих шифрование), ее подмены, модификации и т.п.

*Перехват за переделами контролируемой зоны.*

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – является маловероятной.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 6.

Таблица 6

|  |  |  |
| --- | --- | --- |
| Тип ИСПДн | Вероятность реализации угрозы | Коэфф. вероятности реализации угрозы нарушителем |
| Автономная ИС I типа | маловероятная | 0 |
| Автономная ИС II типа | низкая | 2 |
| Автономная ИС III типа | маловероятная | 0 |
| Автономная ИС IV типа | низкая | 2 |
| Автономная ИС V типа | маловероятная | 0 |
| Автономная ИС VI типа | низкая | 2 |
| ЛИС I типа | маловероятная | 0 |
| ЛИС II типа | низкая | 2 |
| Распределенная ИС I типа | маловероятная | 0 |
| Распределенная ИС II типа | низкая | 2 |

В нашем случае, предполагается Локальная ИС II типа.

Вероятность реализации угрозы – является низкой.

Перехват в пределах контролируемой зоны внешними нарушителями

В Учреждении введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – маловероятна.

Перехват в пределах контролируемой зоны внутренними нарушителями.

В Учреждении введен контроль доступа в контролируемую зону, двери закрываются на замок

Вероятность реализации угрозы – маловероятна.

Угроза «Сканирование сети» в локальной сети.

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель - выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей. Реализация данной угрозы в локальной сети наиболее вероятна со стороны внутреннего нарушителя.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – является маловероятной.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 7.

Таблица 7

|  |  |  |
| --- | --- | --- |
| Тип ИСПДн | Вероятность реализации угрозы | Коэфф. вероятности реализации угрозы нарушителем |
| Автономная ИС I типа | маловероятная | 0 |
| Автономная ИС II типа | маловероятная | 0 |
| Автономная ИС III типа | маловероятная | 0 |
| Автономная ИС IV типа | маловероятная | 0 |
| Автономная ИС V типа | маловероятная | 0 |
| Автономная ИС VI типа | маловероятная | 0 |
| ЛИС I типа | маловероятная | 0 |
| ЛИС II типа | маловероятная | 0 |
| Распределенная ИС I типа | маловероятная | 0 |
| Распределенная ИС II типа | низкая | 2 |

Сетевое оборудование, применяемое в ИСПДн, размещается в служебных помещениях в пределах контролируемой зоны. Доступ в серверные помещения и помещения узлов связи разрешен только ограниченному кругу лиц.

В нашем случае имеем: Локальная ИС II типа.

Вероятность реализации угрозы – маловероятна.

*Угроза выявления паролей.*

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – является маловероятной.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 8.

Таблица 8

|  |  |  |
| --- | --- | --- |
| Тип ИСПДн | Вероятность реализации угрозы | Коэфф. вероятности реализации угрозы нарушителем |
| Автономная ИС I типа | маловероятная | 0 |
| Автономная ИС II типа | низкая | 2 |
| Автономная ИС III типа | маловероятная | 0 |
| Автономная ИС IV типа | низкая | 2 |
| Автономная ИС V типа | маловероятная | 0 |
| Автономная ИС VI типа | низкая | 2 |
| ЛИС I типа | маловероятная | 0 |
| ЛИС II типа | низкая | 2 |
| Распределенная ИС I типа | маловероятная | 0 |
| Распределенная ИС II типа | средняя | 5 |

Сетевое оборудование, применяемое в ИСПДн, размещается в служебных помещениях в пределах контролируемой зоны. Доступ в серверные помещения и помещения узлов связи разрешен только ограниченному кругу лиц.

В нашем случае Локальная ИС II типа.

Вероятность реализации угрозы – низкая вероятность.

*Угрозы навязывание ложного маршрута сети*

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализации угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – является маловероятной.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 9.

Таблица 9

|  |  |  |
| --- | --- | --- |
| Тип ИСПДн | Вероятность реализации угрозы | Коэфф. вероятности реализации угрозы нарушителем |
| Автономная ИС I типа | маловероятная | 0 |
| Автономная ИС II типа | маловероятная | 0 |
| Автономная ИС III типа | маловероятная | 0 |
| Автономная ИС IV типа | маловероятная | 0 |
| Автономная ИС V типа | маловероятная | 0 |
| Автономная ИС VI типа | маловероятная | 0 |
| ЛИС I типа | маловероятная | 0 |
| ЛИС II типа | маловероятная | 0 |
| Распределенная ИС I типа | маловероятная | 0 |
| Распределенная ИС II типа | низкая | 2 |

В нашем случае Локальная ИС II типа.

Вероятность реализации угрозы – маловероятна.

*Угрозы подмены доверенного объекта*

Такая угроза эффективно реализуется в системах, в которых применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа к техническому средству ИСПДн - цели угроз.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – является маловероятной.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 10.

Таблица 10

|  |  |  |
| --- | --- | --- |
| Тип ИСПДн | Вероятность реализации угрозы | Коэфф. вероятности реализации угрозы нарушителем |
| Автономная ИС I типа | маловероятная | 0 |
| Автономная ИС II типа | маловероятная | 0 |
| Автономная ИС III типа | маловероятная | 0 |
| Автономная ИС IV типа | маловероятная | 0 |
| Автономная ИС V типа | маловероятная | 0 |
| Автономная ИС VI типа | маловероятная | 0 |
| ЛИС I типа | маловероятная | 0 |
| ЛИС II типа | маловероятная | 0 |
| Распределенная ИС I типа | маловероятная | 0 |
| Распределенная ИС II типа | низкая | 2 |

В нашем случае Локальная ИС II типа.

Вероятность реализации угрозы – маловероятна.

*Внедрение ложного объекта сети*

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях NovellNetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – является маловероятной.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 11.

Таблица 11

|  |  |  |
| --- | --- | --- |
| Тип ИСПДн | Вероятность реализации угрозы | Коэфф. вероятности реализации угрозы нарушителем |
| Автономная ИС I типа | маловероятная | 0 |
| Автономная ИС II типа | маловероятная | 0 |
| Автономная ИС III типа | маловероятная | 0 |
| Автономная ИС IV типа | маловероятная | 0 |
| Автономная ИС V типа | маловероятная | 0 |
| Автономная ИС VI типа | маловероятная | 0 |
| ЛИС I типа | маловероятная | 0 |
| ЛИС II типа | маловероятная | 0 |
| Распределенная ИС I типа | маловероятная | 0 |
| Распределенная ИС II типа | низкая | 2 |

В нашем случае Локальная ИС II типа.

Вероятность реализации угрозы – маловероятна..

*Угрозы типа «Отказ в обслуживании».*

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

- скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Pingflooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;

- явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);

- явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP RedirectHost, DNS-flooding) или идентификационной и аутентификационной информации;

- явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «PingDeath»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, которое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, то вероятность реализации угрозы – является маловероятной.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 12.

Таблица 12

|  |  |  |
| --- | --- | --- |
| Тип ИСПДн | Вероятность реализации угрозы | Коэфф. вероятности реализации угрозы нарушителем |
| Автономная ИС I типа | маловероятная | 0 |
| Автономная ИС II типа | маловероятная | 0 |
| Автономная ИС III типа | маловероятная | 0 |
| Автономная ИС IV типа | маловероятная | 0 |
| Автономная ИС V типа | маловероятная | 0 |
| Автономная ИС VI типа | маловероятная | 0 |
| ЛИС I типа | маловероятная | 0 |
| ЛИС II типа | низкая | 2 |
| Распределенная ИС I типа | низкая | 2 |
| Распределенная ИС II типа | низкая | 2 |

Серверы ИСПДн, а также сегмент ИСПДн в учреждении защищены межсетевым экраном. В нашем случае Локальная ИС II типа.

Вероятность реализации угрозы – низкая вероятность.

*Угрозы удаленного запуска приложений*

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиден­циальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск приклад­ных программ пользователей для несанкционированного получения необхо­димых нарушителю данных, для запуска управляемых прикладной програм­мой процессов и др.

Выделяют три подкласса данных угроз:

распространение файлов, содержащих несанкционированный испол­няемый код;

удаленный запуск приложения путем переполнения буфера приложе­ний-серверов;

удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программны­ми и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения фай­лов могут использоваться службы электронной почты, передачи файлов, се­тевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за пере­полнением буфера). Настройкой системных регистров иногда удается пере­ключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морри­са».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back.Orifice, NetBus), либо штатными средствами управления и администрирования компьютерных се­тей (LandeskManagementSuite, Managewise, BackOrifice и т. п.). В результа­те их использования удается добиться удаленного контроля над станцией в сети.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, установлена антивирусная защита, то вероятность реализации угрозы – является маловероятной.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 13.

Таблица 13

|  |  |  |
| --- | --- | --- |
| Тип ИСПДн | Вероятность реализации угрозы | Коэфф. вероятности реализации угрозы нарушителем |
| Автономная ИС I типа | маловероятная | 0 |
| Автономная ИС II типа | низкая | 2 |
| Автономная ИС III типа | маловероятная | 0 |
| Автономная ИС IV типа | низкая | 2 |
| Автономная ИС V типа | маловероятная | 0 |
| Автономная ИС VI типа | низкая | 2 |
| ЛИС I типа | маловероятная | 0 |
| ЛИС II типа | низкая | 2 |
| Распределенная ИС I типа | маловероятная | 0 |
| Распределенная ИС II типа | средняя | 5 |

В нашем случае Локальная ИС II типа.

Вероятность реализации угрозы – низкая вероятность.

*Угрозы внедрения по сети вредоносных программ*

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения ак­тивно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность само­стоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью за­пустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

программы подбора и вскрытия паролей;

программы, реализующие угрозы;

программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;

программы-генераторы компьютерных вирусов;

программы, демонстрирующие уязвимости средств защиты информа­ции и др.

Если в Учреждении обрабатываемые ПДн не пересылаются по сетям общего пользования и международного обмена, установлена антивирусная защита, то вероятность реализации угрозы – является маловероятной.

Во всех других случаях должна быть оценена вероятность реализации угрозы.

Обобщенный список вероятности реализации угроз для разных типов ИСПДн представлен в таблице 14.

Таблица 14

|  |  |  |
| --- | --- | --- |
| Тип ИСПДн | Вероятность реализации угрозы | Коэфф. вероятности реализации угрозы нарушителем |
| Автономная ИС I типа | маловероятная | 0 |
| Автономная ИС II типа | низкая | 2 |
| Автономная ИС III типа | маловероятная | 0 |
| Автономная ИС IV типа | низкая | 2 |
| Автономная ИС V типа | маловероятная | 0 |
| Автономная ИС VI типа | низкая | 2 |
| ЛИС I типа | маловероятная | 0 |
| ЛИС II типа | низкая | 2 |
| Распределенная ИС I типа | маловероятная | 0 |
| Распределенная ИС II типа | средняя | 5 |

В нашем случае Локальная ИС II типа.

Вероятность реализации угрозы – низкая вероятность.

6. Реализуемость угроз

По итогам оценки уровня защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением Y = (Y1+ Y2)/20

Оценка реализуемости УБПДн представлена в таблице.

Таблица 15 – Реализуемость УБПДн

|  |  |  |
| --- | --- | --- |
| Тип угроз безопасности ПДн | Коэффициент реализуемости угрозы (Y) | Возможность реализации |
| 1. Угрозы от утечки по техническим каналам. |
| 1.1. Угрозы утечки акустической информации | 0,25 | низкая |
| 1.2. Угрозы утечки видовой информации | 0,25 | низкая |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | 0,25 | низкая |
| 2. Угрозы несанкционированного доступа к информации. |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн |
| 2.1.1. Кража ПЭВМ | 0,25 | низкая |
| 2.1.2. Кража носителей информации | 0,25 | низкая |
| 2.1.3. Кража ключей и атрибутов доступа | 0,25 | низкая |
| 2.1.4. Кражи, модификации, уничтожения информации | 0,25 | низкая |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | 0,25 | низкая |
| 2.1.6. Несанкционированное отключение средств защиты | 0,25 | низкая |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). |
| 2.2.1. Действия вредоносных программ (вирусов) | 0,35 | средняя |
| 2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных | 0,35 | средняя |
| 2.2.3. Установка ПО не связанного с исполнением служебных обязанностей | 0,25 | низкая |
| 2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера. |
| 2.3.1. Утрата ключей и атрибутов доступа | 0,35 | средняя |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками | 0,25 | низкая |
| 2.3.3. Непреднамеренное отключение средств защиты | 0,25 | низкая |
| 2.3.4. Выход из строя аппаратно-программных средств | 0,25 | низкая |
| 2.3.5. Сбой системы электроснабжения | 0,25 | низкая |
| 2.3.6. Стихийное бедствие | 0,25 | низкая |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей |
| 2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке | 0,25 | низкая |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке | 0,35 | средняя |
| 2.5.Угрозы несанкционированного доступа по каналам связи. |
| 2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации: |
| 2.5.1.1. Перехват за пределами с контролируемой зоны | 0,35 | средняя |
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями | 0,25 | низкая |
| 2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями. | 0,25 | низкая |
| 2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др. | 0,25 | низкая |
| 2.5.3.Угрозы выявления паролей по сети | 0,25 | низкая |
| 2.5.4.Угрозы навязывание ложного маршрута сети | 0,25 | низкая |
| 2.5.5.Угрозы подмены доверенного объекта в сети | 0,25 | низкая |
| 2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | 0,25 | низкая |
| 2.5.7.Угрозы типа «Отказ в обслуживании» | 0,35 | средняя |
| 2.5.8.Угрозы удаленного запуска приложений | 0,35 | средняя |
| 2.5.9.Угрозы внедрения по сети вредоносных программ | 0,35 | средняя |

7. Оценка опасности угроз

Оценка опасности УБПДн производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Оценка опасности УБПДн представлена таблице.

Таблица 16 – Опасность УБПДн

|  |  |
| --- | --- |
| Тип угроз безопасности ПДн | Опасностьугрозы |
| 1. Угрозы от утечки по техническим каналам. |
| 1.1. Угрозы утечки акустической информации | низкая |
| 1.2. Угрозы утечки видовой информации | низкая |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | низкая |
| 2. Угрозы несанкционированного доступа к информации. |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн |
| 2.1.1. Кража ПЭВМ | низкая |
| 2.1.2. Кража носителей информации | низкая |
| 2.1.3. Кража ключей и атрибутов доступа | низкая |
| 2.1.4. Кражи, модификации, уничтожения информации | низкая |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | низкая |
| 2.1.6. Несанкционированное отключение средств защиты | низкая |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). |
| 2.2.1. Действия вредоносных программ (вирусов) | средняя |
| 2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных | низкая |
| 2.2.3. Установка ПО не связанного с исполнением служебных обязанностей | низкая |
| 2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера. |
| 2.3.1. Утрата ключей и атрибутов доступа | средняя |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками | низкая |
| 2.3.3. Непреднамеренное отключение средств защиты | низкая |
| 2.3.4. Выход из строя аппаратно-программных средств | низкая |
| 2.3.5. Сбой системы электроснабжения | низкая |
| 2.3.6. Стихийное бедствие | низкая |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей |
| 2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке | низкая |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке | низкая |
| 2.5.Угрозы несанкционированного доступа по каналам связи. |
| 2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации: |
| 2.5.1.1. Перехват за пределами с контролируемой зоны | низкая |
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями | низкая |
| 2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями. | низкая |
| 2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др. | низкая |
| 2.5.3.Угрозы выявления паролей по сети | средняя |
| 2.5.4.Угрозы навязывание ложного маршрута сети | низкая |
| 2.5.5.Угрозы подмены доверенного объекта в сети | низкая |
| 2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | низкая |
| 2.5.7.Угрозы типа «Отказ в обслуживании» | низкая |
| 2.5.8.Угрозы удаленного запуска приложений | низкая |
| 2.5.9.Угрозы внедрения по сети вредоносных программ | средняя |

8. Определение актуальности угроз в ИСПДн

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы.

Таблица 17 – Правила определения актуальности УБПДн

|  |  |
| --- | --- |
| Возможность реализацииугрозы | Показатель опасности угрозы |
| Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

Оценка актуальности угроз безопасности представлена в таблице.

Таблица 18 – Актуальность УБПДн

|  |  |
| --- | --- |
| Тип угроз безопасности ПДн | Опасностьугрозы |
| 1. Угрозы от утечки по техническим каналам. |
| 1.1. Угрозы утечки акустической информации | неактуальная |
| 1.2. Угрозы утечки видовой информации | неактуальная |
| 1.3. Угрозы утечки информации по каналам ПЭМИН | неактуальная |
| 2. Угрозы несанкционированного доступа к информации. |
| 2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн |
| 2.1.1. Кража ПЭВМ | неактуальная |
| 2.1.2. Кража носителей информации | неактуальная |
| 2.1.3. Кража ключей и атрибутов доступа | неактуальная |
| 2.1.4. Кражи, модификации, уничтожения информации | неактуальная |
| 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи | неактуальная |
| 2.1.6. Несанкционированное отключение средств защиты | неактуальная |
| 2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий). |
| 2.2.1. Действия вредоносных программ (вирусов) | актуальная |
| 2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных | неактуальная |
| 2.2.3. Установка ПО не связанного с исполнением служебных обязанностей | неактуальная |
| 2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера. |
| 2.3.1. Утрата ключей и атрибутов доступа | актуальная |
| 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками | неактуальная |
| 2.3.3. Непреднамеренное отключение средств защиты | неактуальная |
| 2.3.4. Выход из строя аппаратно-программных средств | неактуальная |
| 2.3.5. Сбой системы электроснабжения | неактуальная |
| 2.3.6. Стихийное бедствие | неактуальная |
| 2.4. Угрозы преднамеренных действий внутренних нарушителей |
| 2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке | неактуальная |
| 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке | неактуальная |
| 2.5.Угрозы несанкционированного доступа по каналам связи. |
| 2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации: |  |
| 2.5.1.1. Перехват за пределами с контролируемой зоны | неактуальная |
| 2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями | неактуальная |
| 2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями. | неактуальная |
| 2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др. | неактуальная |
| 2.5.3.Угрозы выявления паролей по сети | неактуальная |
| 2.5.4.Угрозы навязывание ложного маршрута сети | неактуальная |
| 2.5.5.Угрозы подмены доверенного объекта в сети | неактуальная |
| 2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | неактуальная |
| 2.5.7.Угрозы типа «Отказ в обслуживании» | неактуальная |
| 2.5.8.Угрозы удаленного запуска приложений | неактуальная |
| 2.5.9.Угрозы внедрения по сети вредоносных программ | актуальная |

Были выявлены следующие актуальные угрозы:

- действия вредоносных программ (вирусов)

- утрата ключей и атрибутов доступа

- угрозы внедрения по сети вредоносных программ

Для снижения опасности реализации актуальныхУБПДн рекомендуется:

- назначение ответственного за безопасность персональных данных из числа сотрудников учреждения;

- инструкции пользователей ИСПДн, в которых отражены порядок безопасной работы с ИСПДн, а так же с ключами и атрибутами доступа;

- организация разграничения прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПДн и средств защиты.

- постоянное обновление антивирусных баз.

**04.02.2021 г. №21**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КАЗАЧЬЕ**

**ПОСТАНОВЛЕНИЕ**

**ОБ УТВЕРЖДЕНИИ ПОЛИТИКИ В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В соответствии с ст. 1 пункт б ПП 2012 года № 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 и муниципальными органами». ст. 18.1 ч. 1 Федерального закона № 152-ФЗ «О персональных данных», в соответствии с Уставом муниципального образования «Казачье», администрация муниципального образования «Казачье»

**постановляЕТ:**

1.Утвердить Политику в отношении обработки персональных данных (Приложение 1)

2.Настоящее постановление подлежит официальному опубликованию на официальном сайте администрации муниципального образования «Казачье» и в муниципальном Вестнике

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к постановлению

МО Казачье

от 04.02.2021 № 21

**Политика в отношении обработки персональных данных**

1.Общие положения

Настоящая политика в отношении обработки персональных данных администрации МО "Казачье", ИНН 8503005810 (далее - Политика) определяет:

-основные права и обязанности оператора и субъекта ПДн;

-цели обработки ПДн;

-правовые основания обработки ПДн;

-объем и категории обрабатываемых ПДн;

-категории (виды) обрабатываемых субъектов ПДн;

-порядок и условия обработки ПДн;

-взаимодействие с третьими лицами при обработке ПДн;

-принятые меры, предусмотренные . 2 ст. 18.1, ч. 1 ст. 19 Федерального -закона «О персональных данных»;

-условия прекращения обработки персональных данных;

-сроки хранения персональных данных;

-регламент реагирования на запросы/обращения субъектов персональных данных и их представителей, уполномоченных органов по поводу неточности персональных данных, неправомерности их обработки, отзыва согласия и доступа субъекта персональных данных к своим данным, а также соответствующие формы запросов/обращений.

Политика разработана с учетом рекомендаций Федеральной службы в сфере связи, информационных технологий и массовых коммуникаций по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Оператор ведет свою деятельность по адресу: 669323, Иркутская обл, Боханский р-н, село Казачье, ул. Мира, д. 10

Специалист по информационно техническому обеспечению назначен ответственным за организацию обработки персональных данных. База данных информации, содержащей персональные данные граждан Российской Федерации, находится по адресу: 669323, Иркутская обл, Боханский р-н, село Казачье, ул. Мира, д. 10.

Документ принят с целью обеспечения защиты прав и свобод субъекта персональных данных при обработке его персональных данных.

Положения Политики служат основой для разработки локальных нормативных актов, регламентирующих в администрации МО "Казачье" вопросы обработки персональных данных работников администрации МО "Казачье" и других субъектов персональных данных.

Все работники Оператора, в обязательном порядке должны быть ознакомлены с настоящим Положением для последующего его исполнения в ходе выполнения должностных обязанностей.

Действующая редакция Политики, содержит сведения, подлежащие раскрытию в соответствии с ч. 1 ст. 14 ФЗ «О персональных данных» и является общедоступным документом, доступна любому Пользователю сети Интернет при переходе по ссылке: bohan.irkobl.ru

Таблица 1. - «Перечень сокращений»

|  |  |
| --- | --- |
| **Сокращение** | **Расшифровка сокращения** |
| ПДн | Персональные данные |
| Оператор | АДМИНИСТРАЦИЯ М.О. "КАЗАЧЬЕ" |
| Политика | Политика администрации МО "Казачье" в отношении обработки персональных данных |

Таблица 2. - «Термины и определения»

|  |  |
| --- | --- |
| Термин | Определение термина |
| Персональные данные | Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). |
| Субъект персональных данных |  |
| Оператор персональных данных | Оператор персональных данных (оператор) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. |
| Обработка персональных данных | Обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования.Обработка персональных данных включает в себя, в том числе:сбор;запись;систематизацию;накопление;хранение;уточнение(обновление, изменение);извлечение;использование;передачу (распространение, предоставление, доступ);обезличивание;блокирование;удаление;уничтожение. |
| Автоматизированная обработка персональных данных | Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники. |
| Распространение персональных данных | Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц. |
| Предоставление персональных данных | Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц. |
| Блокирование персональных данных | Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных). |
| Уничтожение персональных данных | Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных. |
| Обезличивание персональных данных | Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных |
| Информационная система персональных данных | Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств. |
| Трансграничная передача персональных данных | Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу. |

1.Правовые основания обработки персональных данных

Оператор обрабатывает персональные данные на законной и справедливой основе для выполнения возложенных законодательством функций, полномочий и обязанностей, осуществления прав и законных интересов Оператора, работников Оператора и других физических лиц, персональные данные которых обрабатываются в информационной системе АДМИНИСТРАЦИЯ М.О. "КАЗАЧЬЕ". При обработке персональных данных, оператор руководствуется следующими правовыми основаниями:

Федеральным законом от 06.04.2011 г. № 63-ФЗ "Об электронной подписи", Конституцией Российской Федерации (ст.ст.23, 24), Трудовым кодексом Российской Федерации (ст.ст.65, 66, 86-90, 166), Налоговым кодексом Российской Федерации (ст.ст.226, 230), Гражданским кодексом Российской Федерации (гл.гл.39, 40, 52),; Федеральным законом от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» (ст.ст.6, 9, 11), Федеральным законом от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации» (ст.11), Федеральным законом от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации» (ст.38), Федеральным законом от 29.12.2006 № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством» (ч.4 ст.13), Федеральным законом от 28.12.2013 № 426-ФЗ «О специальной оценке условий труда» (ч.2 ст.4, ст.ст.7, 8), Постановлением Госкомстата Российской Федерации от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты» (п.2), Положением, утвержденным постановлением Правительства РФ от 27 ноября 2006 г. № 719 (п. 7 ст. 8 Закона от 28 марта 1998 г. № 53-ФЗ) (п.32), Федеральным законом от 08.02.1998 № 14-ФЗ «Об обществах с ограниченной ответственностью» (ст. 31.1), Постановлением Минтруда Российской Федерации, Минобразования Российской Федерации от 13.01.2003 № 1/29 «Об утверждении Порядка обучения по охране труда и проверки знаний требований охраны труда работников организаций» (п.1.2), Уставом АДМИНИСТРАЦИЯ М.О. "КАЗАЧЬЕ", Согласиями субъектов персональных данных на обработку их персональных данных, а также договорами, выгодоприобретателем или поручителем в которых являются субъекты персональных данных.

Цели и принципы обработки персональных данных

Оператор обрабатывает персональные данные работников Оператора в рамках правоотношений, урегулированных Трудовым Кодексом Российской Федерации от 30 декабря 2001 г. № 197-ФЗ (далее — ТК РФ), в том числе главой 14 ТК РФ, касающейся защиты персональных данных работников.

Оператор не принимает решения, затрагивающие интересы работников, основываясь на их персональных данных, полученных электронным образом или исключительно в результате автоматизированной обработки.

Оператор защищает персональные данные работников за счет собственных средств в порядке, установленном ТК РФ, ФЗ «О персональных данных» и иными федеральными законами.

Оператор знакомит работников и их представителей под роспись с документами, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

Оператор разрешает доступ к персональным данным работников только допущенным лицам, которые имеют право получать только те данные, которые необходимы для выполнения их функций.

Оператор получает все персональные данные работников у них самих. Если данные работника возможно получить только у третьей стороны, Оператор заранее уведомляет об этом работника и получает его письменное согласие. Оператор сообщает работнику о целях, источниках, способах получения, а также о характере подлежащих получению данных и последствиях отказа работника дать письменное согласие на их получение.

Оператор обрабатывает персональные данные работников в течение срока действия трудового договора. Оператор обрабатывает персональные данные уволенных работников в течение срока, установленного п. 5 ч. 3 ст. 24 части первой Налогового Кодекса Российской Федерации от 31 июля 1998 г. № 146-ФЗ, ч. 1 ст. 29 Федерального закона «О бухгалтерском учёте» от 6 декабря 2011 г. № 402-ФЗ и иными нормативными правовыми актами.

Оператор может обрабатывать специальные категории персональных данных работников (сведений о состоянии здоровья, относящихся к вопросу о возможности выполнения ими трудовых функций) на основании п. 2.3 ч. 2 ст. 10 ФЗ «О персональных данных».

Оператор не сообщает третьей стороне персональные данные работника без его письменного согласия, кроме случаев, когда это необходимо для предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных ТК РФ, ФЗ «О персональных данных» или иными федеральными законами.

Оператор передаёт персональные данные работников их представителям в порядке, установленном ТК РФ, ФЗ «О персональных данных» и иными федеральными законами, и ограничивает эту информацию только теми данными, которые необходимы для выполнения представителями их функций.

Работник может получить свободный бесплатный доступ к информации о его персональных данных и об обработке этих данных. Работник может получить копию любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных федеральным законом.

Работник может требовать исключить или исправить свои неверные или неполные персональные данные, а также данные, обработанные с нарушением требований ТК РФ, ФЗ «О персональных данных» или иного федерального закона. При отказе Оператора исключить или исправить персональные данные работника он может заявить в письменной форме о своем несогласии и обосновать такое несогласие. Работник может дополнить персональные данные оценочного характера заявлением, выражающим его собственную точку зрения.

Работник может требовать известить всех лиц, которым ранее были сообщены его неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

Работник может обжаловать в суд любые неправомерные действия или бездействие Оператора при обработке и защите его персональных данных.

Цели обработки персональных данных администрации МО "Казачье", которые относятся к трудовому законодательству:

Соблюдение трудового законодательства и иных актов, содержащих нормы трудового права, включая учет труда и его оплаты, принятие управленческих и кадровых решений в отношении сотрудников и руководителя;

Ведение бухгалтерского учета, осуществление расчета и выплаты сотрудникам и руководителю причитающейся им заработной платы, компенсаций и премий, осуществление пенсионных и налоговых отчислений;

Осуществление расследования и учета несчастных случаев, происшедших с сотрудниками и иными лицами при исполнении ими своих трудовых функций, а также в иных случаях, предусмотренных трудовым законодательством и иные цели.

Вид деятельности АДМИНИСТРАЦИЯ М.О. "КАЗАЧЬЕ" предполагает обязательства по сбору, обработке, систематизации и хранении информации по физическим лицам с целями, которые не относятся к трудовому законодательству, включая осуществление хозяйственной деятельности, предусмотренной учредительными документами АДМИНИСТРАЦИЯ М.О. "КАЗАЧЬЕ", а именно:

поставка товаров, выполнение работ и оказание услуг, в пользу АДМИНИСТРАЦИЯ М.О. "КАЗАЧЬЕ" со стороны контрагентов (поставщиков), а также осуществление процедур закупок у указанных контрагентов и ведение деловых переговоров с указанными контрагентами;

осуществление взаимных расчетов с контрагентами (клиентами, агентами, партнерами, подрядчиками, поставщиками);

рассмотрение и учет обращений (запросов, предложений, комментариев, претензий, благодарностей), поступающих от контрагентов (клиентов) и иных лиц, а также осуществление информационного обслуживания указанных лиц;

предложение своих услуг действительным и потенциальным контрагентам (клиентам), а также участие в процедурах закупок указанных лиц и ведение деловых переговоров с указанными лицами; принятие мер должной осмотрительности при взаимодействии с действительными и потенциальными контрагентами (агентами, партнерами, подрядчиками, поставщиками), включающее в себя оценку соответствующих юридических, финансовых, репутационных и иных рисков;

оформление доверенностей в рамках наделения сотрудников и иных лиц специальными полномочиями для выполнения возложенных на них трудовых функций и (или) представления интересов администрации МО "Казачье"

участие в гражданском, арбитражном, уголовном, административном процессах, а также исполнение судебных актов; соблюдение трудового законодательства и иных актов, содержащих нормы трудового права, включая учет труда и его оплаты, принятие управленческих и кадровых решений в отношении сотрудников, контроль над трудовой дисциплиной;

организация обучения, инструктажа, проверки знаний сотрудников и иных лиц по охране труда и технике безопасности, а также проведение специальной оценки условий труда;

осуществление надлежащего учета, хранения и уничтожения по истечении сроков хранения отдельных категорий материальных носителей информации;

связь с субъектами ПДн по вопросам, относящимся к предметам деятельности, а также взаимодействие с должностными/физическими лицами, представляющими юридические лица и индивидуальных предпринимателей, по вопросам сотрудничества с администрации МО "Казачье"; организация и (или) осуществление обучения, повышения квалификации и проверки знаний для своих сотрудников; осуществление аттестации сотрудников посредством оценки их деловых и личностных качеств, а также результатов их труда; предоставление дополнительных социальных льгот сотрудникам, членам их семей и иным родственникам в виде предоставления бесплатного питания, организации доставки к месту работы и обратно, выплаты материальной помощи и иных компенсаций в случаях, определенных локальными актами администрации МО "Казачье"; выявление нарушений состояния здоровья и медицинских противопоказаний к работе у сотрудников (включая организацию проведения медицинских осмотров и организацию медицинского наркологического освидетельствования на состояние опьянения);содействие сотрудникам в надлежащем выполнении ими возложенных на них трудовых функций посредством выдачи визитных карточек, и обеспечения служебной униформой; предоставление служебных транспортных средств сотрудникам для обеспечения текущей деятельности, для учета и возмещения расходов на эксплуатацию предоставленных транспортных средств, для контроля надлежащего использования и сохранности предоставленных транспортных средств; организация оформления зарплатных карт для сотрудников; осуществление отчислений страховых взносов в НПФ; публикация данных сотрудников на сайте организации, внутренних справочниках; замещение вакантных должностей соискателями, наиболее полно соответствующими требованиям администрации МО "Казачье";ведение кадрового резерва;

Обработка персональных данных осуществляется на основе общих принципов:

законности заранее определенных конкретных целей и способов обработки персональных данных;

обеспечения надлежащей защиты персональных данных;

соответствия целей обработки персональных целям, заранее определенным и заявленным при сборе персональных данных;

соответствия объема, характера и способов обработки персональных данных целям обработки персональных данных;

достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

хранения персональных данных осуществляется в форме, позволяющей определить Субъекта персональных данных, не дольше, чем того требуют цели обработки;

уничтожения персональных данных по достижении целей обработки, если срок хранения персональных данных не установлен законодательством РФ:

обеспечения конфиденциальности и безопасности обрабатываемых персональных данных.

1.Перечень субъектов, персональные данные которых обрабатываются в администрации МО "Казачье"

В информационной системе администрации МО "Казачье" обрабатываются персональные данные следующих категорий физических лиц:

физические лица, состоящие в трудовых отношениях, и их родственники; физические лица, состоявшие в трудовых отношениях; соискатели на замещение вакантных должностей; Контрагенты (должностные лица) контрагентов-организаций, индивидуальных предпринимателей (клиенты, агенты, партнеры, подрядчики, поставщики) и их представители; потенциальные контрагенты (клиенты, агенты, партнеры, подрядчики, поставщики) и их представители; Физические лица – получатели услуг со стороны администрации МО "Казачье" и их законные представители.

2.Перечень персональных данных, обрабатываемых в администрации МО "Казачье"

3.Перечень персональных данных, обрабатываемых в администрации МО "Казачье" определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами администрации МО "Казачье" с учетом целей обработки персональных данных, указанных в разделе 3 Политики для каждой информационной системы ПДн. К ним относятся:

фамилия, имя, отчество, дата рождения, место рождения, адрес, семейное положение, образование, профессия, доходы, предыдущие фамилия, имя, отчество, если изменялись; наименование и реквизиты (серия и номер, дата выдачи, наименование и код выдавшего органа) документа, удостоверяющего личность лица на территории Российской Федерации; адрес регистрации; имущественное положение; гражданство; идентификационный номер налогоплательщика (ИНН); страховой номер индивидуального лицевого счета (СНИЛС); сведения о доходах за предыдущий период до текущего трудоустройства; сведения о размере оклада; сведения о начисленной и удержанной заработной плате; сведения о начисленных и уплаченных страховых взносах; сведения о премиях; сведения о периодических выплатах; сведения о сумме дополнительного вознаграждения; страховые взносы на ОПС; страховые взносы на ОМС; налоговые вычеты; сведения о воинском учете; номер контактного телефона; контактный адрес электронной почты; сведения об образовании, квалификации, специальности, переподготовке; наименование и реквизиты (серия и номер, дата выдачи, наименование выдавшего органа) документа об образовании, квалификации, специальности; сведения (дата, период, наименование организации, проводившей обучение) о прохождении обучения (повышения квалификации, переподготовке); наименование и реквизиты (серия и номер, дата выдачи, наименование проводившей обучение организации, наименование выдавшего органа) документа о прохождении обучения (повышения квалификации, переподготовке); наименование мест предыдущих трудоустройств, а также занимаемых должностей; сведения о периоде и продолжительности работы в местах предыдущих трудоустройств; сведения о дополнительных компетенциях, знаниях и навыках; сведения о знании и об уровне владения иностранными языками; сведения о знании и об уровне владения программным обеспечением; наименование должности; наименование структурного подразделения; наименование и адрес текущего места трудоустройства; реквизиты (сведения о дате заключения и номер) трудового договора; дата приема на работу; дата вступления в должность; сведения о факте и дате прекращения трудового договора; реквизиты (серия и номер, дата выдачи, наименование выдавшего органа) трудовой книжки; наименование профессии; сведения о трудовом стаже; табельный номер; сведения о месте и дате направления в командировку; сведения о факте, периоде и продолжительности нахождения в командировке; сведения о сумме произведенных командировочных расходов.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, а также биометрических персональных данных в администрации МО "Казачье" не осуществляется.

В целях индексации сайта bohan.irkobl.ru поисковыми системами yandex.ru и google.ru, а также учета частоты посещения страниц, Оператор использует службы сбора статистики посетителей технологии cookies. В момент посещения пользователем той или иной страницы Оператора, браузер пользователя, выполняя сервисные коды служб статистики, передает в них информацию о факте посещения страницы, о времени посещения и времени нахождения на странице, об адресе страницы, с которой произошел переход па текущую страницу. IP-адрес, данные об аппаратных событиях, файлы cookies, сведения о местоположении, уникальные номера приложений. Обработка персональных данных осуществляется в целях улучшения работы сайга Оператора, совершенствования программных продуктов Оператора, определения предпочтений пользователя, предоставления целевой информации по продуктам и услугам Оператора.

1.Трансграничная передача данных

Оператор не производит трансграничную передачу персональных данных.

2.Перечень действий, совершаемых оператором с персональными данными

Оператор осуществляет:

сбор:

систематизацию;

накопление;

хранение;

уточнение (обновление, изменение);

использование;

передачу (распространение, предоставление, доступ);

блокирование;

уничтожение персональных данных.

1.Способы обработки персональных данных

В зависимости от информационной системы, используемой Оператором, обработка персональных данных может осуществляться путем:

смешанной обработки с передачей по внутренней сети Оператора с передачей по сети интернет;

автоматизированной обработки без передачи по внутренней сети Оператора с передачей по сети интернет;

смешанной обработки без передачи по внутренней сети Оператора без передачи по сети интернет.

1.Сроки обработки персональных данных

Обработка персональных данных Оператором, в том числе их хранение, осуществляется в течение сроков, установленных действующим законодательством, а также локальными нормативными актами. Обработка избыточных категорий персональных данных и\или превышение допустимых сроков хранения – не допускается.

2.Порядок и условия обработки персональных данных

Обработка персональных данных Оператором осуществляется с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством Российской Федерации в области персональных данных.

Оператор без согласия субъекта персональных данных не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральным законом.

Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого с этим лицом договора. Договор должен содержать перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

В целях внутреннего информационного обеспечения Оператор может создавать внутренние справочные материалы, в которые с письменного согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, могут включаться его фамилия, имя, отчество, место работы, должность, год и место рождения, номер телефона (рабочего, сотового), адрес электронной почты, иные персональные данные, сообщаемые субъектом персональных данных.

Доступ к обрабатываемым Оператором персональным данным разрешается только работникам Оператора, занимающим должности, включенные в перечень должностей при замещении которых осуществляется обработка персональных данных.

Оператор осуществляет передачу персональных данных государственным органам в рамках и в соответствии с законодательством РФ.Оператор вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

Доступ к обрабатываемым персональным данным предоставляется только тем работникам Оператора, которым он необходим в связи с исполнением ими своих должностных обязанностей и с соблюдением принципов персональной ответственности.

Оператор обеспечивает раздельное хранение персональных данных и их материальных носителей, обработка которых осуществляется в разных целях и которые содержат разные категории персональных данных.

Хранение материальных носителей персональных данных осуществляется Оператором с соблюдением условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним.

При достижении целей обработки персональных данных, а также в случае отзыва Субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

иное не предусмотрено договором;

оператор не вправе осуществлять обработку без согласия Субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных» или иными федеральными законами;

иное не предусмотрено иным соглашением между оператором и Субъектом персональных данных.

1.Порядок и условия обработки персональных данных

Субъекты персональных данных имеют право па:

полную информацию об их персональных данных, обрабатываемых Оператором;

доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом, а также па доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной пели обработки;

отзыв согласия на обработку персональных данных;

принятие предусмотренных законом мер по защите своих прав;

обжалование действия или бездействия Оператором, осуществляемого с нарушением требований законодательства Российской Федерации в области персональных данных, в уполномоченный орган по защите прав субъектов персональных данных или в суд;

осуществление иных нрав, предусмотренных законодательством Российской Федерации.

В связи с тем, что безопасность определяется не только уровнем защиты портала, к которому подключается Субъект персональных данных, но и уровнем защиты рабочего места, с которого осуществляется доступ, для безопасной работы субъект персональных данных/пользователь должен следовать следующим рекомендациям:

использовать на рабочем месте исключительно лицензионное программное обеспечение;

устанавливать все необходимые обновления безопасности, рекомендуемые производителем программного обеспечения;

устанавливать и регулярно обновлять лицензионное антивирусное программное обеспечение, регулярно проводить проверку на отсутствие вирусов;

не загружать программ и данных из непроверенных источников, не посещать сан ты сомнительного содержания;

не заходить в личный кабинет со случайных компьютеров, интернет-кафе либо иных недоверенных рабочих мест;

не передавать кому-либо токены для авторизации на портале, либо информацию для входа в личный кабинет, следить за сохранностью средств доступа.

При использовании Субъектом ПДн функционала программного обеспечения Оператора может применяться технология cookies. Субъект ПДн вправе ограничить или запретить использование технологии cookies путем применения соответствующих настроек в браузере.

1.Обеспечение защиты персональных данных при их обработке Оператором

Оператор принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер. необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 года № 152 "О персональных данных", постановлением Правительства от 15 сентября 2008 года № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", постановлением Правительства от 01 ноября 2012 года № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", приказом ФСТЭК от 18 февраля 2013 года № 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", и другими нормативными правовыми актами, если иное не предусмотрено федеральными законами. К таким мерам относятся:

назначение Оператором ответственного за обработку ПДн и ответственного за безопасность при обработке ПДн;

издание Оператором документов, определяющих политику оператора в отношении обработки персональных данных, локальных нормативных актов по вопросам обработки персональных данных, а также локальных нормативных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

установление запрета на передачу персональных данных по открытым каналам связи, вычислительным сетям вне пределов контролируемой зоны и сетям Интернет без применения установленных Оператором мер по обеспечению безопасности персональных данных (за исключением общедоступных персональных данных)

хранение материальных носителей персональных данных с соблюдением условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним;

получение согласий субъектов персональных данных на обработку их персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации;

осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону "О персональных данных" и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Оператора в отношении обработки персональных данных, локальным нормативным актам Оператора;

определение оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных", соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных";

организация обучения и проведение методической работы с работниками обособленных подразделений Оператора, занимающими должности, включенные в перечень должностей Оператора, при замещении которых осуществляется обработка персональных данных;

ознакомление сотрудников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных сотрудников.

Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются в соответствии с локальными нормативными актами администрации МО "Казачье", регламентирующими вопросы обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных администрации МО "Казачье".

1.Актуализация, исправление, уничтожение персональных данных

В случае предоставления субъектом персональных данных фактов о неполных, устаревших, недостоверных или незаконно полученных персональных данных Оператор обязан принять меры:

в случае подтверждения факта неточности персональных данных персональные данные подлежат их актуализации оператором:

в случае неправомерности их обработки такая обработка должна быть прекращена.

При достижении целей обработки персональных данных, а также в случае истечения срока согласия на обработку персональных данных или отзыва субъектом персональных данных согласия па их обработку персональные данные подлежат уничтожению, если:

иное не предусмотрено договором, выгодоприобретателем или поручителем, по которому является субъект персональных данных;

оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или иными федеральными законами;

иное не предусмотрено иным соглашением между оператором и субъектом персональных данных.

1.Обработка запросов субъектов персональных данных

В случае поступления Запроса субъекта ПДн или его законного представителя по персональным данным необходимо выполнить следующие действия:

При получении запроса субъекта персональных данных или его представителя на наличие ПДн необходимо в течение 30 дней с даты получения запроса (согласно пункту 1 статьи 20 152-ФЗ) подтвердить обработку ПДн, в случае ее осуществления. Если обработка ПДн субъекта не ведется, то в течение 30 дней с даты получения запроса (согласно пункту 2 статьи 20 152-ФЗ) необходимо отправить уведомление об отказе подтверждения обработки ПД.

При получении запроса субъекта персональных данных или его представителя на ознакомление с ПДн необходимо в течение 30 дней с даты получения запроса (согласно пункту 1 статьи 20 152-ФЗ) предоставить для ознакомления ПДн, в случае осуществления обработки этих ПДн. Если обработка ПДн субъекта не ведется, то в течение 30 дней с даты получения запроса (согласно пункту 2 статьи 20 152-ФЗ) необходимо отправить уведомление об отказе предоставления информации по ПДн.

Субъект ПДн или его законный представитель имеет право получение информации, касающейся обработки его ПДн, в том числе содержащей:

Подтверждение обработки ПДн, а также правовые основания и цели такой обработки.

Способы обработки ПДн.

Сведения о лицах, которые имеют доступ к ПДн.

Перечень обрабатываемых ПДн и источник их получения.

Сроки обработки ПДн, в том числе сроки их хранения.

При получении запроса субъекта персональных данных или его представителя па уточнение ПДн необходимо внести в них необходимые изменения в срок, не превышающий 7 рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, неточными или неактуальными (согласно пункту 3 статьи 20 152-ФЗ) и отправить уведомление о внесенных изменениях.

Если обработка ПДн субъекта не ведется или не были предоставлены сведения, подтверждающие, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, неточными или неактуальными, то необходимо в течение 30 дней с даты получения запроса отправить уведомление об отказе осуществления изменения ПДн.

При получении запроса субъекта персональных данных или его представителя на уничтожение ПДн необходимо их уничтожить в срок, не превышающий 7 рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки (согласно пункту 3 статьи 20 152-ФЗ) и отправить уведомление об уничтожении.

Если обработка ПДн субъекта не ведется или не были предоставлены сведения, подтверждающие, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются незаконно полученными или не являются необходимыми для заявленной цели обработки, а также в силу необходимости обработки ПДн но требованиям иных законодательных актов, то необходимо в течение 30 дней с даты получения запроса отправить уведомление об отказе уничтожения ПДн.

При получении запроса на отзыв согласия па обработку ПДн необходимо прекратить их обработку и, в случае, если сохранение ПДн более не требуется для целей обработки персональных данных, уничтожить ПДн в срок, не превышающий 30 дней с даты поступления указанного отзыва (согласно пункту 5 статьи 21 152-ФЗ), если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами (согласно пункту 5 статьи 21 152-ФЗ).

При выявлении недостоверности ПДн при обращении или по запросу субъекта ПДн или его представителя необходимо их блокировать с момента такого обращения или получения такого запроса на период проверки (согласно пункту 1 статьи 21 152-ФЗ). Если факт недостоверности ПДн подтвержден на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов, необходимо уточнить персональные данные в течение 7 рабочих дней со дня представления таких сведений и спять блокирование персональных данных (согласно пункту 2 статьи 21 152-ФЗ).

Если факт недостоверности ПДн не подтвержден, то необходимо отправить уведомление об отказе изменения ПДн.

При выявлении неправомерных действий Оператора с ПДн при обращении или по запросу субъекта ПДн или его представителя необходимо в срок, не превышающий трех рабочих дней с даты этого выявления, прекратить неправомерную обработку персональных данных (согласно пункту 5 3 статьи 21 152-ФЗ).

В случае если обеспечить правомерность обработки персональных данных невозможно. Оператор в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных (согласно пункту 3 статьи 21 152-ФЗ), обязан уничтожить такие персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

При достижении целей обработки ПДн Оператор обязан незамедлительно прекратить обработку ПДн, уничтожить соответствующие 11Дн в срок, не превышающий 30 дней с даты достижения цели обработки ПДн (согласно пункту 4 статьи 21 152-ФЗ). если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем некоторому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных 152-ФЗ или другими федеральными законами.

Прием запросов от субъектов ПДн или его законных представителей.

В случае поступления запроса субъекта ПДн или его законного представителя сотрудник Оператора обязан зарегистрировать запрос в «Журнале учета обращений граждан (субъектов персональных данных) но вопросам обработки персональных данных». Запрос предоставляется субъектом ПДн в произвольной форме. После принятия запроса сотрудник Оператора сверяем сведения в запросе с предоставленными ему документами.

Необходимые сведения о субъекте ПДн, которые должны присутствовать в подаваемом запросе:

номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя,

сведения о дате выдачи указанного документа и выдавшем его органе,

сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором,

подпись субъекта персональных данных или его представителя.

Если запрос оформлен в соответствии с требованиями законодательства, он принимается к обработке.

1.Заключительные положения

Положения настоящей Политики вступают в силу с момента ее утверждения и действует до ее отмены или выпуска новой редакции.

Все изменения в положения Политики вносятся путем утверждения новой редакции Постановлением главы администрации МО "Казачье"

|  |  |  |
| --- | --- | --- |
| Ответственный заорганизацию обработкиперсональных данных | \_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись) |  |

**04.02.2021 г. №22**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КАЗАЧЬЕ**

**ПОСТАНОВЛЕНИЕ**

**ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ О ПОРЯДКЕ ДОСТУПА В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЕТСЯ ОБРАБОТКА ПДН**

В соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», в соответствии с Уставом муниципального образования «Казачье», администрация муниципального образования «Казачье»

**постановляЕТ:**

1.Утвердить Положение о порядке доступа в помещения, в которых ведется обработка ПДн (Приложение 1)

2.Настоящее постановление подлежит официальному опубликованию на официальном сайте администрации муниципального образования «Казачье» и в муниципальном Вестнике

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к постановлению

МО Казачье

от 04.02.2021 № 22

**Положение о порядке доступа в помещения, в которых ведется обработка ПДн**

Порядок доступа работников в помещения, в которых ведёт обработку персональных данных администрации МО "Казачье" (далее — Оператор), устанавливается в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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».

Порядок доступа в помещения распространяется на всех работников Оператора. В помещениях, в которых хранятся и обрабатываются персональные данные, должна быть исключена возможность бесконтрольного проникновения посторонних лиц и несанкционированного доступа к персональным данным.

В контролируемые помещения допускаются только работники, уполномоченные на обработку персональных данных в соответствии с «Приказом о допуске к обработке персональных данных». Иные лица допускаются только в присутствии допущенных работников Оператора.

Входные двери помещений оборудуются замками, гарантирующими надёжное закрытие в нерабочее время и при выходе из помещения в рабочее время. В случае утери ключей, замок заменяется. Уборка в помещениях, где хранятся и обрабатываются персональные данные, производится только в присутствии допущенного работника.

При обнаружении повреждений замков или других признаков, указывающих на возможное проникновение посторонних лиц в помещения, в которых ведется обработка персональных данных, составляется акт и о случившемся немедленно ставится в известность ответственный за обработку персональных данных.

Контроль за соблюдением порядка доступа в помещение, в котором ведется обработка персональных данных, проводится лицом, ответственным за организацию обработки персональных данных.

**04.02.2021 г. №23**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КАЗАЧЬЕ**

**ПОСТАНОВЛЕНИЕ**

**ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ О ПРАВИЛАХ РАБОТЫ С ОБРАБАТЫВАЕМЫМИ ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В соответствии с Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», ст.3., в соответствии с Уставом муниципального образования «Казачье», администрация муниципального образования «Казачье»

**постановляЕТ:**

1. Утвердить Положение о правилах работы с обрабатываемыми обезличенными персональными данными в информационной системе персональных данных (Приложение 1)

2.Настоящее постановление подлежит официальному опубликованию на официальном сайте администрации муниципального образования «Казачье» и в муниципальном Вестнике

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к постановлению МО Казачье

от 04.02.2021 № 23

**Положение о правилах работы с обрабатываемыми обезличенными персональными данными в информационной системе персональных данных**

1. Общие положения

Настоящие Правила работы с обрабатываемыми обезличенными персональными данными в информационной системе персональных данных (далее - Правила) разработаны на основании Федерального закона от 27.07.2006 № 152 - ФЗ «О персональных данных» (далее - Федеральный закон № 152 - ФЗ) и постановления Правительства РФ 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».

Настоящие Правила определяют порядок работы с обезличенными данными в информационной системе персональных данных (далее - ИСПДн) администрации МО "Казачье", утверждаются руководителем администрации МО "Казачье"и действуют постоянно.

1. Условия обезличивания

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

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, «Адрес» 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 и др.;

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

Для обезличивания персональных данных используются способы, не запрещенные действующим законодательством Российской Федерации.

Перечень должностей работников администрации МО "Казачье"ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, утверждается руководителем администрации МО "Казачье". Глава администрации МО "Казачье" принимает решение о необходимости обезличивания персональных данных.

1. Порядок работы с обезличенными персональными данными

Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

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

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.

При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

* правил хранения бумажных носителей;
* правил доступа к ним и в помещения, где они хранятся.

Ответственным за проведение мероприятий по обезличиванию обрабатываемых персональных данных в администрации МО "Казачье"является Специалист по информационно техническому обеспечению.

**04.02.2021 г. №24**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КАЗАЧЬЕ**

**ПОСТАНОВЛЕНИЕ**

**ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ ОБ ОБРАБОТКЕ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ**

В соответствии с Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», в соответствии с Уставом муниципального образования «Казачье», администрация муниципального образования «Казачье»

**постановляЕТ:**

1. Утвердить Положение об обработке данных без использования средств автоматизации (Приложение 1)

2.Настоящее постановление подлежит официальному опубликованию на официальном сайте администрации муниципального образования «Казачье» и в муниципальном Вестнике

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к постановлению

МО Казачье

от 04.02.2021 № 24

**Положение об обработке данных без использования средств автоматизации**

1.Общие положения

Настоящее Положение о порядке обработки персональных данных без использования средств автоматизации (далее – Положение) определяет порядок работы с документами, содержащими персональные данные, в администрации МО "Казачье". Положение разработано в соответствии с Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Ответственный за организацию обработки и обеспечение безопасности персональных данных администрации МО "Казачье" ответственен за подбор лиц, допускаемых к информации ограниченного доступа (персональным данным), и обязан обеспечить систематический контроль за тем, чтобы к этой информации получали доступ только работники, которым данная информация необходима для выполнения своих трудовых обязанностей.

Лица, допущенные к персональным данным, обязаны:

обеспечивать сохранность и конфиденциальность персональных данных;

информировать субъекта персональных данных об обращении посторонних лиц о предоставлении его персональных данных.

Запрещается выносить документы и дела, содержащие персональные данные, из помещений, а также передавать их по открытым каналам связи, за исключением случаев, предусмотренных законодательством Российской Федерации или по согласованию с субъектом персональных данных.

Во время пребывания в помещениях работник несет личную ответственность за защиту информации в данном помещении. Неконтролируемое пребывание в помещении посторонних лиц исключено.

Контроль за исполнением требований настоящего Положения возлагается на ответственного за организацию обработки и обеспечение защиты персональных данных администрации МО "Казачье"- Специалист по информационно техническому обеспечению.

Термины и определения

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

Администратор безопасности информации – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системой защиты информации в соответствии с установленной ролью.

Безопасность информации [данных] – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Доступность информации [ресурсов информационной системы] – состояние информации [ресурсов информационной системы], при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Защищаемая информация – информация, для которой обладателем информации определены характеристики ее безопасности.

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

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

Информация – сведения (сообщения, данные) независимо от формы их представления.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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.

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

Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц

Средство защиты информации – техническое, программное, программно-техническое средство, предназначенное или используемое для защиты информации.

Техническое средство – аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации в информационной системе.

2.Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес организации, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Организации способов обработки персональных данных;

типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, – при необходимости получения письменного согласия на обработку персональных данных;

типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимых для однократного пропуска субъекта персональных данных в помещение Организации или в иных аналогичных целях, должны соблюдаться следующие условия:

необходимость ведения такого журнала должна быть предусмотрена актом, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных;

копирование содержащейся в таких журналах информации не допускается;

персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более одного раза в каждом случае пропуска субъекта персональных данных.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

3.Меры по обеспечению безопасности персональных данных при их обработке и передаче, осуществляемой без использования средств автоматизации

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить список лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. В этих целях необходимо осуществлять хранение персональных данных в запираемых шкафах или ящиках, ключ от которых должен находиться у работника, имеющего право доступа к персональным данным, находящимся в этих шкафах (ящиках), дубликаты ключей должны храниться у заведующего хозяйством Организации.

Шкафы или ящики, в которых хранятся документы, содержащие персональные данные, по окончании рабочего дня запираются работниками, ответственными за учет и хранение документов.

Конфиденциальные документы должны пересылаться (доставляться) между организациями в соответствующим образом оформленных запечатанных пакетах.

Размножение и отправка документов, содержащих персональные данные, осуществляется только с согласия субъекта персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации.

Проверки наличия конфиденциальных документов проводятся не реже одного раза в год комиссией, назначаемой руководителем Организации.

Проверками должны быть охвачены дела, документы, и иные носители информации.

При обнаружении утраты документов, разглашения информации и признаков несанкционированного ознакомления с конфиденциальными документами, работник обязан доложить ответственному за организацию обработки и обеспечение безопасности персональных данных Организации, далее по распоряжению руководителя Организации проводится служебное расследование.

Утрата конфиденциальных документов, разглашение информации ограниченного доступа, незаконное ознакомление с информацией ограниченного доступа, влечет ответственность, предусмотренную действующим законодательством Российской Федерации.

**04.02.2021 г. №25**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КАЗАЧЬЕ**

**ПОСТАНОВЛЕНИЕ**

**ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В соответствии с статьей 5; пункта 6 части 1 статьи14; пункта 2 части 1 статьи 18.1; части 3, 4 статьи 21 Федерального закона №152 "О персональных данных", части 6 Постановления правительства №687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", статьями 86-90 Трудового Кодекса РФ, в соответствии с Уставом муниципального образования «Казачье», администрация муниципального образования «Казачье»

**постановляЕТ:**

1.Утвердить Положение об обработке персональных данных (Приложение 1)

2.Настоящее постановление подлежит официальному опубликованию на официальном сайте администрации муниципального образования «Казачье» и в муниципальном Вестнике

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к постановлению

МО Казачье

от 04.02.2021 № 25

**Положение об обработке персональных данных**

1.Общие положения

Положение об обработке персональных данных (далее — Положение) определяет условия и порядок обработки персональных данных, которую осуществляет администрация МО "Казачье" (далее — Оператор).

Положение разработано во исполнение Политики в отношении обработки персональных данных (далее — Политика) и в соответствии с п. 2 ч. 1 ст. 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — ФЗ «О персональных данных»), а также следующими нормативными правовыми актами:

часть вторая Гражданского Кодекса Российской Федерации от 26 января 1996 г. № 14-ФЗ (далее — часть вторая ГК РФ);

* Трудовой Кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ (далее — ТК РФ);
* часть первая Налогового Кодекса Российской Федерации от 31 июля 1998 г. № 146-ФЗ (далее — часть первая НК РФ);
* Федеральный закон «О бухгалтерском учёте» от 6 декабря 2011 г. № 402-ФЗ (далее — ФЗ «О бухгалтерском учёте»);
* постановление Правительства Российской Федерации от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
* постановление Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2.Организация обработки персональных данных

В целях обеспечения выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, Оператором назначается ответственный за организацию обработки персональных данных (далее — Ответственный).

Ответственный обязан:

* обеспечивать утверждение, приведение в действие, а также обновление в случае необходимости Политики, Положения и иных локальных актов по вопросам обработки персональных данных;
* обеспечить неограниченный доступ к Политике, копия которой размещается по адресу нахождения Оператора;
* проводить оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы Оператора;
* ежегодно проводить оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения ФЗ «О персональных данных»;
* ежегодно осуществлять внутренний контроль за соблюдением Оператором и его работниками законодательства о персональных данных, Политики, Положения и иных локальных актов по вопросам обработки персональных данных, в том числе требований к защите персональных данных (далее — Нормативные акты);
* доводить до работников под роспись положения Нормативных актов при заключении трудового договора, а также по собственной инициативе;
* осуществлять допуск работников к персональным данным, обрабатываемым в информационной системе Оператора, а также к их материальным носителям только для выполнения трудовых обязанностей;
* организовывать и контролировать приём и обработку обращений и запросов субъектов персональных данных, обеспечивать осуществление их прав;
* обеспечивать взаимодействие с уполномоченным органом по защите прав субъектов персональных данных (далее — Роскомнадзор).

3.Обеспечение безопасности персональных данных

Работники, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять их без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

В целях защиты персональных данных от неправомерных действий (в частности, неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения) Оператором применяется комплекс правовых, организационных и технических мер по обеспечению безопасности персональных данных, составляющий систему защиты персональных данных.

Применение комплекса мер по обеспечению безопасности персональных данных обеспечивает установленный уровень защищенности персональных данных при их обработке в информационной системе Оператора.

В целях обеспечения выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, Оператором назначается ответственный за обеспечение безопасности персональных данных в информационной системе.

Ответственный за обеспечение безопасности персональных данных в информационной системе обязан:

* ежегодно выполнять определение угроз безопасности персональных данных при их обработке в информационной системе Оператора;
* обеспечивать реализацию организационных и технических мер по обеспечению безопасности персональных данных и применение средств защиты информации, необходимых для достижения установленного уровня защищенности персональных данных при обработке в информационной системе Оператора;
* устанавливать правила доступа к персональным данным, обрабатываемым в информационной системе Оператора, а также обеспечивать регистрацию и учёт всех действий с ними;
* организовывать обнаружение фактов несанкционированного доступа к персональным данным и принятие мер по реагированию, включая восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
* ежегодно осуществлять внутренний контроль за обеспечением установленного уровня защищённости персональных данных при обработке в информационной системе Оператора.

4.Осуществление прав субъектов персональных данных

При обращении субъекта персональных данных или при получении его запроса (далее — Обращение) Ответственный обеспечивает предоставление субъекту персональных данных информации о наличии относящихся к нему персональных данных, а также возможности ознакомления с этими персональными данными в течение 30 дней с даты Обращения.

При наличии законных оснований для отказа в предоставлении субъекту персональных данных информации о наличии относящихся к нему персональных данных, а также возможности ознакомления с этими персональными данными Ответственный обеспечивает направление субъекту персональных данных мотивированного ответа в письменной форме, содержащего ссылку на положение ч. 8 ст. 14 ФЗ «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в течение 30 дней с даты Обращения.

При предоставлении субъектом персональных данных сведений, подтверждающих, что его персональные данные, обрабатываемые Оператором, являются неполными, неточными или неактуальными, Ответственный обеспечивает внесение необходимых изменений в персональные данные в течение 7 рабочих дней с даты обращения.

При предоставлении субъектом персональных данных сведений, подтверждающих, что его персональные данные, обрабатываемые Оператором, являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Ответственный обеспечивает уничтожение таких персональных данные в течение 7 рабочих дней с даты Обращения.

Ответственный обеспечивает уведомление субъекта персональных данных о внесенных в его персональные данные изменениях и предпринятых мерах, а также принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

В случае отзыва субъектом персональных данных согласия на их обработку она может быть продолжена при наличии оснований, указанных в п. 2—11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 ФЗ «О персональных данных».

5.Взаимодействие с Роскомнадзором

По запросу Роскомнадзора Ответственный организует предоставление локальных актов в отношении обработки персональных данных и документов, подтверждающих принятие мер по выполнению требований ФЗ «О персональных данных», в течение 30 дней с даты получения запроса.

По требованию Роскомнадзора Ответственный организует уточнение, блокирование или уничтожение недостоверных, или полученных незаконным путем персональных данных в течение 30 дней с даты получения требования.

В случаях, предусмотренных ст. 22 ФЗ «О персональных данных», Ответственный направляет в Роскомнадзор уведомление о намерении осуществлять обработку персональных данных.

В случае необходимости Ответственный направляет в Роскомнадзор обращения по вопросам обработки персональных данных, осуществляемой Оператором.

6.Ответственность за нарушение порядка обработки и обеспечения безопасности персональных данных

В случае нарушения работником положений законодательства в области персональных данных он может быть привлечён к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном ТК РФ и иными федеральными законами, в соответствии с ч. 1 ст. 24 ФЗ «О персональных данных» и ст. 90 ТКРФ.

В случае разглашения работником персональных данных, ставших ему известными в связи с исполнением его трудовых обязанностей, трудовой договор с ним может быть расторгнут в соответствии с пп. «в» п. 6 ст. 81 ТК РФ.

**04.02.2021 г. №26**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН**

**АДМИНИСТРАЦИЯ**

**МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КАЗАЧЬЕ**

**ПОСТАНОВЛЕНИЕ**

**ОБ УТВЕРЖДЕНИИ ИНСТРУКЦИИ ПО РАССМОТРЕНИЮ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ**

В соответствии с 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 актам», в соответствии с Уставом муниципального образования «Казачье», администрация муниципального образования «Казачье»

**постановляЕТ:**

1.Утвердить Инструкцию по рассмотрению запросов субъектов персональных данных или их представителей (Приложение 1)

2.Настоящее постановление подлежит официальному опубликованию на официальном сайте администрации муниципального образования «Казачье» и в муниципальном Вестнике

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к постановлению

МО Казачье

от 04.02.2021 № 26

**Инструкция по рассмотрению запросов субъектов персональных данных или их представителей**

Настоящей инструкцией по рассмотрению запросов субъектов персональных данных или их представителей в администрации МО "Казачье" определяются порядок учета (регистрации), рассмотрения запросов субъектов персональных данных или их представителей (далее – запросы).

Настоящие Правила разработаны в соответствии Федеральным законом от 27 июля 2006 г. № 152 ФЗ «О персональных данных» (далее – Федеральный закон), Федеральным законом от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» (в редакции от 29.06.2010 N 126-ФЗ, от 27.07.2010 N 227-ФЗ), Федеральным законом от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации», Трудовым кодексом Российской Федерации, Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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» и другими нормативными правовыми актами.

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных (часть 7 статьи 14 Федерального закона), в том числе содержащей:

* подтверждение факта обработки персональных данных в администрации МО "Казачье";
* правовые основания и цели обработки персональных данных;
* цели и применяемые в Управлении способы обработки персональных данных;
* наименование и место нахождения администрации МО "Казачье", сведения о лицах (за исключением работников администрации МО "Казачье"), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании федерального закона;
* обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
* сроки обработки персональных данных, в том числе сроки их хранения;
* порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
* информацию об осуществленной или о предполагаемой трансграничной передаче данных;
* наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению руководителя, если обработка поручена или будет поручена такому лицу;
* иные сведения, предусмотренные Федеральным законом или другими федеральными законами.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона.

Субъект персональных данных вправе требовать от администрации МО "Казачье" уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Сведения, указанные в части 7 статьи 14 Федерального закона, должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Сведения, указанные в части 7 статьи 14 Федерального закона, предоставляются субъекту персональных данных или его представителю администрации МО "Казачье" при обращении либо при получении запроса субъекта персональных данных или его представителя.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с администрации МО "Казачье" (номер заявки на возврат, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных администрации МО "Казачье", подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Рассмотрение запросов является служебной обязанностью уполномоченных должностных лиц, в чьи обязанности входит обработка персональных данных.

Должностные лица администрации МО "Казачье" обеспечивают:

* объективное, всестороннее и своевременное рассмотрения запроса;
* принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;
* направление письменных ответов по существу запроса.

Ведение делопроизводства по запросам осуществляется назначенным сотрудником администрации МО "Казачье".

Все поступившие запросы регистрируются в день их поступления. На запросе указывается входящий номер и дата регистрации.

Запрос прочитывается, проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской. В случае, если сведения, указанные в части 7 статьи 14 Федерального закона № 152-ФЗ, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в администрацию МО "Казачье" или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Субъект персональных данных вправе обратиться повторно в администрацию МО "Казачье" или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона № 152ФЗ, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в настоящем пункте, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимыми сведениями должен содержать обоснование направления повторного запроса.

Администрация МО "Казачье" вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона № 152ФЗ. Такой отказ должен быть мотивированным.

Прошедшие регистрацию запросы в тот же день докладываются руководителю администрации МО "Казачье" либо лицу, его заменяющему, который определяет порядок и сроки их рассмотрения, дает по каждому из них письменное указание исполнителям.

Глава администрации МО "Казачье", и другие должностные лица при рассмотрении и разрешении запроса обязаны:

* внимательно разобраться в их существе, в случае необходимости истребовать дополнительные материалы или направить сотрудников на места для проверки фактов, изложенных в запросах, принять другие меры для объективного разрешения поставленных заявителями вопросов, выявления и устранения причин и условий, порождающих факты нарушения законодательства о персональных данных;
* принимать по ним законные, обоснованные и мотивированные решения и обеспечивать своевременное и качественное их исполнение;
* сообщать в письменной форме заявителям о решениях, принятых по их запросам, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса - разъяснять также порядок обжалования принятого решения.

Администрация МО "Казачье" обязано сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя уполномоченные должностные лица администрации МО "Казачье" обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152 ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

Администрация МО "Казачье" обязана предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, уполномоченные должностные лица администрации МО "Казачье" обязаны внести в них необходимые изменения.

В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уполномоченные должностные лица администрации МО "Казачье" обязаны уничтожить такие персональные данные.

Администрация МО "Казачье" обязана уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица администрации МО "Казачье" обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения или получения указанного запроса на период проверки.

В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица администрации МО "Казачье" обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

В случае подтверждения факта неточности персональных данных уполномоченные должностные лица администрации МО "Казачье" на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязаны уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

В случае выявления неправомерной обработки персональных данных уполномоченные должностные лица администрации МО "Казачье" в срок, не превышающий трех рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, уполномоченные должностные лица администрации МО "Казачье" в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязаны уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных администрация МО "Казачье" обязана уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

Для проверки фактов, изложенных в запросах при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации.

По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения сотрудниками администрации МО "Казачье" действия (бездействия), содержащего признаки административного правонарушения или состава преступления информация передается незамедлительно в правоохранительные органы. Результаты служебной проверки докладываются начальнику администрации МО "Казачье".

Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

Ответы на запросы печатаются на бланке установленной формы и регистрируются за теми же номерами, что и запросы.

Глава администрации МО "Казачье" осуществляет непосредственный контроль за соблюдением установленного законодательством и настоящими Правилами порядка рассмотрения запросов.

Глава администрации МО "Казачье" осуществляет контроль за работой с запросами и организацией их приема как лично, так и через своих заместителей. На контроль берутся все запросы.

При осуществлении контроля обращается внимание на сроки исполнения поручений по запросам и полноту рассмотрения поставленных вопросов, объективность проверки фактов, изложенных в запросах, законность и обоснованность принятых по ним решений, своевременность их исполнения и направления ответов заявителям.

Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

**01.02.2021г. №6**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**О ВЫДЕЛЕНИИ ДЕНЕЖНЫХ СРЕДСТВ**

На основании договора №34560621/000594 от 01.01.2021г., заключенного с ООО «РН - Карт», для обеспечения служебной техники ГСМ.

1. Главному бухгалтеру Тураевой Н.Г. выделить денежные средства для приобретения ГСМ в сумме 29000 (двадцать девять тысяч руб.) на февраль 2021 г.

 2. Данное распоряжение опубликовать в муниципальном Вестнике.

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

**01.02.2021г. №7**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**О ВЫДЕЛЕНИИ ДЕНЕЖНЫХ СРЕДСТВ**

На основании актов оказания услуг №7102 от 20.10.2020г. №7103 от 20.11.2020г., №7104 от 18.12.2020г., по договору заключенного с ООО «Советникпроф»

1. Главному бухгалтеру Тураевой Н.Г. выделить денежные средства для приобретения ГСМ в сумме 25650 (двадцать пять тысяч шестьсот пятьдесят руб.)

 2. Данное распоряжение опубликовать в муниципальном Вестнике.

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

**02.02.2021г. №8**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**О ВЫДЕЛЕНИИ ДЕНЕЖНЫХ СРЕДСТВ**

На основании счета на оплату №048 от 27.01.2021г., по договору заключенного с ИП Рыбкин Д.В.

1. Главному бухгалтеру Тураевой Н.Г. выделить денежные средства для заправки картриджа в сумме 1870 (одна тысяча восемьсот семьдесят руб.)

 2. Данное распоряжение опубликовать в муниципальном Вестнике.

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

**02.02.2021г. №9**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**О ВЫДЕЛЕНИИ ДЕНЕЖНЫХ СРЕДСТВ**

На основании договора №10 от 19.01.2021г, заключенного с ООО «Дружина», акта выполненных работ №12 от 01.02.2021г.

1. Главному бухгалтеру Тураевой Н.Г. выделить денежные средства для оплаты за услуги по очистке дорог в сумме 32561 (тридцать две тысячи пятьсот шестьдесят один руб.)

 2. Данное распоряжение опубликовать в муниципальном Вестнике.

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

**04.02.2021г. №10**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**ОБ УТВЕРЖДЕНИИ ПЕРЕЧНЯ ЛИЦ, ДОПУЩЕННЫХ К ОБРАБОТКЕ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В целях исполнения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

1. Утвердить список должностей работников, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей (Приложение №1).

2.Ответственному за организацию обработки персональных данных проводить контроль актуальности списка 1 раз в полгода.

3.Ответственному за организацию обработки персональных данных проводить обучение новых работников в соответствии с Инструкцией по проведению инструктажа лиц, допущенных к работе с информационными системами персональных данных, до момента начала выполнения ими служебных (трудовых) обязанностей.

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к распоряжению администрации МО Казачье

от 04.02.2021 №6

**Список должностей работников, доступ которых к персональным данным, обрабатываемым в информационных системах администрации МО "Казачье", необходим для выполнения служебных (трудовых) обязанностей**

Глава администрации

Заместитель главы администрации

Главный бухгалтер

Финансист

Специалист по информационно техническому обеспечению

Специалист по имуществу и земле

**04.02.2021г. №11**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**О НАЗНАЧЕНИИ ОТВЕТСТВЕННЫХ В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В АДМИНИСТРАЦИИ МО "КАЗАЧЬЕ"**

В целях исполнения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), Приказа ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

1.Ввести в администрации МО "Казачье" режим обработки и защиты персональных данных.

2.Назначить ответственным за организацию обработки персональных данных следующего работника: Специалист по информационно техническому обеспечению - Бормотова Татьяна Сергеевна;

3.Назначить ответственным за обеспечение безопасности персональных данных в информационной системе персональных данных следующего работника: Специалист по информационно техническому обеспечению - Бормотова Татьяна Сергеевна.

4.Разработать и внедрить документы, определяющие политику в отношении обработки персональных данных, локальные акты по вопросам обработки и защиты персональных данных.

5.Обеспечить применение необходимых правовых, организационных и технических мер по защите персональных данных, в соответствии с законодательством РФ о персональных данных.

6.Утвердить Инструкцию ответственного за организацию обработки персональных данных (Приложение 1) и Инструкцию ответственного за обеспечение безопасности персональных данных (Приложение 2).

7.Возложить на ответственного за организацию обработки персональных данных обязанности, предусмотренные Инструкцией ответственного за организацию обработки персональных данных.

8.Возложить на ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных обязанности, предусмотренные Инструкцией ответственного за обеспечение безопасности персональных данных.

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к распоряжению администрации МО Казачье

от 04.02.2021 №7

**Инструкция ответственного за организацию обработки персональных данных**

Настоящая инструкция определяет функции, права и ответственность лица, ответственного за организацию обработки персональных данных (далее — Ответственный за организацию обработки) в администрации МО "Казачье" (далее — Оператор).

Оператор назначает Ответственного за организацию обработки «Приказом о назначении ответственных в отношении обработки персональных данных».

Ответственный за организацию обработки в своей деятельности руководствуется Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иными нормативными правовыми актами РФ в области защиты персональных данных, настоящей инструкцией. Ответственный за организацию обработки ознакомляется с настоящей инструкцией под роспись.

Ответственный за организацию обработки обязан:

- Организовывать работу Оператора по разработке и принятию организационно – распорядительных документов, регламентирующих деятельность по обработке и защите персональных данных, поддержанию их в актуальном состоянии;

- Организовывать принятие Оператором правовых, организационных и технических мер для защиты персональных данных;

- Проводить инструктаж работников в соответствии с Инструкцией по проведению инструктажа лиц, допущенных к работе с информационными системами персональных данных, вести «Журнал учета прохождения первичного инструктажа сотрудниками»;

- Осуществлять внутренний контроль выполнения Операторами работниками положений законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

- Инициировать проведение служебных расследований по фактам нарушения установленных правил обработки и защиты персональных данных;

- Направлять в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций уведомление об обработке персональных данных и информационное письмо о внесении изменений в реестр операторов при необходимости;

- Организовывать прием и обработку обращений субъектов персональных данных, контролировать заполнение «Журнала учёта обращений субъектов персональных данных»;

- Представлять интересы Оператора при проверках надзорных органов в сфере обработки персональных данных;

- При возникновении нештатной ситуации действовать в соответствии с «Инструкцией пользователя информационной системы персональных данных при возникновении внештатных ситуаций»;

- Обеспечивать размещение на официальном сайте Оператора документа, определяющего политику в отношении обработки персональных данных, в течение 10 дней после его утверждения.

Ответственный за организацию обработки имеет право:

- Требовать от работников выполнения установленных правил обработки и защиты персональных данных;

- Требовать от работников прекращения обработки персональных данных в случаях их неправомерного использования и нарушения установленного порядка обработки;

- Вносить предложения по совершенствованию организационных и технических мер;

- Принимать участие в рассмотрении обращений и запросов субъектов персональных данных.

Ответственный за организацию обработки несёт персональную ответственность за качество проводимых им работ по организации обработки персональных данных.

Ответственный за организацию обработки несёт ответственность за разглашение информации ограниченного доступа, ставшей известной ему породу работы, в соответствии с законодательством РФ.

Специалист по ИТО \_\_\_\_\_\_\_\_

Приложение 2

к распоряжению администрации МО Казачье

от 04.02.2021 №7

**Инструкция ответственного за обеспечение безопасности персональных данных**

Настоящая инструкция определяет функции, права и ответственность лица, ответственного за обеспечение безопасности персональных данных (далее — Ответственный за обеспечение безопасности) в администрации МО "Казачье" (далее — Оператор).

Оператор назначает Ответственного за обеспечение безопасности «Приказом о назначении ответственных в отношении обработки персональных данных».

Ответственный за обеспечение безопасности в своей деятельности руководствуется Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иными нормативными правовыми актами РФ в области защиты персональных данных, настоящей инструкцией. Ответственный за обеспечение безопасности ознакомляется с настоящей инструкцией под роспись.

Ответственный за обеспечение безопасности обязан:

- Применять технические меры защиты персональных данных;

- Обеспечивать функционирование и безопасность средств защиты информации;

- Обучать пользователей работе на персональных компьютерах с установленными средствами защиты информации;

- Контролировать выполнение установленных правил обеспечения защиты персональных данных лицами, допущенными к обработке персональных данных «Распоряжением о допуске к обработке персональных данных»;

- Инициировать проведение служебных расследований по фактам нарушения установленных правил обеспечения защиты персональных данных, несанкционированного доступа к персональным данным;

- Производить резервное копирование и восстановление в соответствии с «Инструкцией по организации резервирования и восстановления программного обеспечения, баз персональных данных информационной системы персональных данных»;

- Разъяснять пользователям порядок использования съемных носителей информации и контролировать заполнение «Журнала учёта съемных носителей персональных данных»;

- Информировать Ответственного за организацию обработки персональных данных об инцидентах и попытках несанкционированного доступа к защищаемой информации.

- Проводить антивирусную защиту в соответствии с «Инструкцией по антивирусной защите в информационных системах персональных данных».

Ответственный за обеспечение безопасности имеет право:

- Требовать от работников выполнения установленных правил обеспечения защиты персональных данных;

- требовать от работников прекращения обработки персональных данных в случаях их неправомерного использования и нарушения правил обеспечения защиты персональных данных;

- Вносить предложения по совершенствованию технических мер по защите персональных данных.

Ответственный за обеспечение безопасности несёт персональную ответственность за качество проводимых им работ по обеспечению безопасности персональных данных. Ответственный за обеспечение безопасности несёт ответственность за разглашение информации ограниченного доступа, ставшей известной ему по роду работы, в соответствии с законодательством РФ.

|  |  |  |
| --- | --- | --- |
| Специалист по информационно техническому обеспечению | (подпись) |  |

**04.02.2021г. №12**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**ОБ ОПРЕДЕЛЕНИИ ГРАНИЦ КОНТРОЛИРУЕМОЙ ЗОНЫ И ТРЕБОВАНИЙ К ЕЕ БЕЗОПАСНОСТИ В АДМИНИСТРАЦИИ МО "КАЗАЧЬЕ"**

В целях исключения неконтролируемого пребывания посторонних лиц при обработке персональных данных и в соответствии с требованиями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

1. Определить границами контролируемой зоны информационной системы персональных данных администрации МО "Казачье" периметр ограждающих конструкций помещений администрации МО "Казачье", находящихся по адресу: 669323, Иркутская область, Боханский район, село Казачье, улица Мира, д. 10;

2.Обеспечить доступ на территорию контролируемой зоны лицам, ответственным за обработку персональных данных в ИСПДн, в соответствии с «Порядком доступа сотрудников администрации МО "Казачье" в помещения, в которых ведется обработка персональных данных»;

3.Подписать «Обязательство о неразглашении информации, содержащей персональные данные», с сотрудниками, осуществляющими системно-техническое обслуживание программного обеспечения и оборудования ИСПДн;

4.Контроль за исполнением приказа оставляю за собой.

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

**04.02.2021г. №13**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**ОБ УТВЕРЖДЕНИИ ПЕРЕЧНЯ ЗАЩИЩАЕМЫХ ДАННЫХ В АДМИНИСТРАЦИИ МО "КАЗАЧЬЕ"**

В целях исполнения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)

1. Утвердить перечень персональных данных, подлежащих защите, обрабатываемых на бумажных носителях и в программных комплексах администрации МО "Казачье" (Приложение 1).

2.Ответственному за организацию обработки персональных данных проводить контроль актуальности перечня 1 раз в полгода.

3.Ознакомить под роспись всех должностных лиц, в части, касающейся обработки персональных данных в администрации МО "Казачье".

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к распоряжению администрации МО Казачье

от 04.02.2021 №9

**Перечень персональных данных, подлежащих защите, обрабатываемых на бумажных носителях и в программных комплексах администрации МО "Казачье"**

Персональные данные, обрабатываемые в администрации МО "Казачье" в связи с осуществлением хозяйственной деятельности, предусмотренной учредительными документами администрации МО "Казачье".

Фамилия, имя, отчество, дата рождения, место рождения, адрес, семейное положение, образование, профессия, доходы, предыдущие фамилия, имя, отчество, если изменялись; наименование и реквизиты (серия и номер, дата выдачи, наименование и код выдавшего органа) документа, удостоверяющего личность лица на территории Российской Федерации; адрес регистрации; Идентификационный номер налогоплательщика; страховой номер индивидуального лицевого счета (СНИЛС); сведения о доходах за предыдущий период до текущего трудоустройства; сведения о размере оклада; сведения о начисленной и удержанной заработной плате; сведения о начисленных и уплаченных страховых взносах; сведения о премиях; сведения о периодических выплатах; сведения о сумме дополнительного вознаграждения; страховые взносы на ОПС; страховые взносы на ОМС; налоговые вычеты; сведения о воинском учете; номер контактного телефона; контактный адрес электронной почты; сведения об образовании, квалификации, специальности, переподготовке; наименование и реквизиты (серия и номер, дата выдачи, наименование выдавшего органа) документа об образовании, квалификации, специальности; сведения (дата, период, наименование организации, проводившей обучение) о прохождении обучения (повышения квалификации, переподготовке); наименование и реквизиты (серия и номер, дата выдачи, наименование проводившей обучение организации, наименование выдавшего органа) документа о прохождении обучения (повышения квалификации, переподготовке); наименование мест предыдущих трудоустройств, а также занимаемых должностей; сведения о периоде и продолжительности работы в местах предыдущих трудоустройств; сведения о дополнительных компетенциях, знаниях и навыках; сведения о знании и об уровне владения иностранными языками; сведения о знании и об уровне владения программным обеспечением; наименование должности; наименование структурного подразделения; наименование и адрес текущего места трудоустройства; реквизиты (сведения о дате заключения и номер) трудового договора; дата приема на работу; дата вступления в должность; сведения о факте и дате прекращения трудового договора; реквизиты (серия и номер, дата выдачи, наименование выдавшего органа) трудовой книжки; наименование профессии; сведения о трудовом стаже; табельный номер; сведения о месте и дате направления в командировку; сведения о факте, периоде и продолжительности нахождения в командировке; сведения о сумме произведенных командировочных расходов.

Приложение

К перечню персональных данных,

подлежащих защите, обрабатываемых

на бумажных носителях и в

программных комплексах

администрации МО "Казачье"

**Лист ознакомления с перечнем защищаемых данных**

|  |  |  |  |
| --- | --- | --- | --- |
| ФИО | Должность | Дата ознакомления | Подпись |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**04.02.2021г. №14**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**ОБ УТВЕРЖДЕНИИ ПЕРЕЧНЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ**

В соответствии с ч. 1 ст. 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и п. 1 «Перечня мер, направленных на обеспечение обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», утверждённого Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211:

1.Утверждить Перечень информационных систем персональных данных (далее — ИСПДн) (Приложению 1).

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к распоряжению администрации МО Казачье

от 04.02.2021 №10

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Наименование ИСПДн | Адрес объекта | Исходные данные классификации ИСПДн | Необходимый уровень защищенности ИСПДн | Примечание |
| Тип актуальных угроз | Категория ПДн | Являются ли данные обобщедоступнымии | Число субъектов персональных данных, данные которых обрабатываются | Ведется ли обработка персональных данных сотрудников |
| 1. | 2. | 3. | 4. | 5. | 6. | 7. | 8. | 9. | 10. |
| 1. | Информационная система АДМИНИСТРАЦИЯ М.О. "КАЗАЧЬЕ" | 669323, Иркутская обл, Боханский р-н, село Казачье, ул Мира, д 10 | 3-й тип (недекларированные возможности отсутствуют) | Специальные | Нет | До 100 000 | Обрабатываются | 3 |  |

**04.02.2021г. №15**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**ОБ УТВЕРЖДЕНИИ ПЕРЕЧНЯ ПОМЕЩЕНИЙ АДМИНИСТРАЦИИ МО "КАЗАЧЬЕ"**

В соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» и Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

1.Утвердить перечень помещений в администрации МО "Казачье", в которых ведётся обработка персональных данных с использованием средств автоматизации и без использования таких средств.

2.Ответственному за организацию обработки персональных данных проводить контроль актуальности перечня 1 раз в год.

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

Приложение 1

к распоряжению администрации МО Казачье

от 04.02.2021 №11

**Перечень помещений администрации МО "Казачье", в которых ведется обработка персональных данных**

|  |
| --- |
| Помещение (адрес, № офиса\кабинета) |
| Офисные помещения администрации МО "Казачье" по адресу: 669323, Иркутская область, Боханский район, село Казачье, улица Мира, д. 10 |
| Помещения центра обработки данных администрации МО "Казачье" по адресу: 669323, Иркутская область, Боханский район, село Казачье, улица Мира, д. 10 |

**08.02.2021г. №16**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**О ВЫДЕЛЕНИИ ДЕНЕЖНЫХ СРЕДСТВ**

На основании счет фактуры №А-00017028/2150 от 11.02.2021г., от ООО «ДНС Ритейл»

1. Главному бухгалтеру Тураевой Н.Г. выделить денежные средства для оплаты ПО ESET в сумме 2900 (две тысячи девятьсот руб.)

 2. Данное распоряжение опубликовать в муниципальном Вестнике.

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

**09.02.2021г. №17**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**О ВЫДЕЛЕНИИ ДЕНЕЖНЫХ СРЕДСТВ**

На основании счета №8503005810-5189 от 02.02.2021г., по договору с ООО «ЕЦС»

1. Главному бухгалтеру Тураевой Н.Г. выделить денежные средства для оплаты услуг по разработке документации о защите персональных данных в сумме 5000 (пять тысяч руб.)

 2. Данное распоряжение опубликовать в муниципальном Вестнике.

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

**09.02.2021г. №18**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**О ВЫДЕЛЕНИИ ДЕНЕЖНЫХ СРЕДСТВ**

На основании муниципального контракта №1106-21 от 01.01.2021г., заключенного с ООО «Вир»

1. Главному бухгалтеру Тураевой Н.Г. выделить денежные средства для оплаты услуг по обновлению ИПК «РегистрМО» в сумме 6000 (шесть тысяч руб.)

 2. Данное распоряжение опубликовать в муниципальном Вестнике.

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

**17.02.2021г. №19**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**О ВЫДЕЛЕНИИ ДЕНЕЖНЫХ СРЕДСТВ**

На основании договора №НСК81-Д-63809000-000118-21 от 15.02.2021г., заключенного с ПАОСК «Росгосстрах»

1. Главному бухгалтеру Тураевой Н.Г. выделить денежные средства для оплаты услуг по страхованию в сумме 4000 (четыре тысячи руб.)

 2. Данное распоряжение опубликовать в муниципальном Вестнике.

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

**17.02.2021г. №20**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**О ВЫДЕЛЕНИИ ДЕНЕЖНЫХ СРЕДСТВ**

На основании договора №3 от 26.01.2021г., заключенного с ООО «Центр кадастра и землеустройства»

1. Главному бухгалтеру Тураевой Н.Г. выделить денежные средства для оплаты за кадастровые работы в сумме 7000 (семь тысяч руб.)

 2. Данное распоряжение опубликовать в муниципальном Вестнике.

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

**17.02.2021г. №21**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**О ВЫДЕЛЕНИИ ДЕНЕЖНЫХ СРЕДСТВ**

На основании договора №4 от 26.01.2021г., заключенного с ООО «Центр кадастра и землеустройства»

1. Главному бухгалтеру Тураевой Н.Г. выделить денежные средства для оплаты за кадастровые работы в сумме 7000 (семь тысяч руб.)

 2. Данное распоряжение опубликовать в муниципальном Вестнике.

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

**24.02.2021г. №22**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**О ВЫДЕЛЕНИИ ДЕНЕЖНЫХ СРЕДСТВ**

На основании договора №1193/21 от 01.02.2021г., заключенного с ООО «СоветникПроф»

1. Главному бухгалтеру Тураевой Н.Г. выделить денежные средства для оплаты за информационно – технологическому сопровождению программных продуктов «1С: Предприятие 8» в сумме 11904 (одиннадцать тысяч девятьсот четыре руб.)

 2. Данное распоряжение опубликовать в муниципальном Вестнике.

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

**24.02.2021г. №23**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**О ВЫДЕЛЕНИИ ДЕНЕЖНЫХ СРЕДСТВ**

1. Главному бухгалтеру Тураевой Н.Г. выделить денежные средства для оплаты земельного налога в сумме 59000 (пятьдесят девять тысяч руб.)

 2. Данное распоряжение опубликовать в муниципальном Вестнике.

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

**24.02.2021г. №24**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**О ПРОДЛЕНИИ СРОКА НАХОЖДЕНИЯ НА МУНИЦИПАЛЬНОЙ СЛУЖБЕ**

В соответствии с частью 2 статьи 19 Федерального закона «О муниципальной службе в российской Федерации» руководствуясь уставом муниципального образования «Казачье»

1.Продлить срок нахождения на муниципальной службе, заместителя главы администрации, Герасимовой Татьяны Григорьевны, достигшей предельного возраста, установленного для замещения должности муниципальной службы с 01.03.2021 по 31.12.2021г.

Основание: личное заявление Герасимовой Т.Г. от 25.02.2021г.

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева

**24.02.2021г. №25**

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ИРКУТСКАЯ ОБЛАСТЬ**

**БОХАНСКИЙ РАЙОН**

**Администрация муниципального образования «Казачье»**

**РАСПОРЯЖЕНИЕ**

**О ХРАНЕНИИ БУМАЖНЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ И НАЗНАЧЕНИИ ДОПУЩЕННЫХ ЛИЦ**

В соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», а также п. 6 и п. 13 «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утверждённого постановлением Правительства от 15 сентября 2008 г. № 687, руководствуясь уставом муниципального образования «Казачье»

1. Утвердить места хранения материальных носителей персональных данных:

Приказ (распоряжение) о приеме работника на работу (Форма N Т-1);

Штатное расписание (Форма N Т-3);

Приказ (распоряжение) о переводе работника на другую работу (Форма N Т-5);

Приказ (распоряжение) о предоставлении отпуска работнику (Форма N Т-6);

График отпусков (Форма N Т-7);

Приказ (распоряжение) о прекращении действия трудового договора (контракта) с работником (Форма N Т-8);

Приказ (распоряжение) о направлении работника в командировку (Форма N Т-9);

Командировочное удостоверение (Форма N Т-10);

Служебное задание для направления в командировку и отчет о его выполнении (Форма N Т-10а);

Приказ (распоряжение) о поощрении работника (Форма N Т-11);

Табель учета использования рабочего времени и расчета заработной платы (Форма N Т-12);

Табель учета использования рабочего времени (Форма N Т-13);

Расчетно-платежная ведомость (Форма N Т-49);

Расчетная ведомость (Форма N Т-51);

Платежная ведомость (Форма N Т-53);

Лицевой счет (Форма N Т-54);

Записка-расчет о предоставлении отпуска работнику (Форма N Т-60);

Записка-расчет при прекращении действия трудового договора (контракта) с работником (Форма N Т-61);

Акт о приемке работ, выполненных по трудовому договору (контракту), заключенному на время выполнения определенной работы (Форма N Т-73);

Договора с контрагентами;

Личная карточка муниципального служащего (Унифицированная форма N Т-2ГС(МС);

Заявление о приеме на работу;

 Анкета при приеме на работу;

Копия медицинского заключения о результатах обязательного предварительного медицинского осмотра;

Копия карты специальной оценки условий труда на рабочем месте;

Трудовой договор;

Дополнительные соглашения к трудовому договору;

Копия должностной инструкции;

Приказы о дисциплинарных взысканиях, кроме увольнения;

Заявления, служебные записки сотрудников (основания для приказов);

Копии актов о расследовании несчастного случая, по адресу 669323, Иркутская область, Боханский район, село Казачье, ул. Мира, д. 10

2.Ответственным за сохранность материальных носителей назначить ответственного за организацию обработки персональных данных.

3.Ответственному за организацию обработки персональных данных проводить информирование работников о факте обработки ими персональных данных без использования средств автоматизации.

4.Ответственному за организацию обработки персональных данных проводить контроль актуальности персональных данных 1 один раз в полгода.

Глава администрации муниципального образования «Казачье»

Т.С. Пушкарева