МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ «Усть-Чижапское сельское поселение»

КАРГАСОКСКИЙ РАЙОН ТОМСКАЯ ОБЛАСТЬ

**АДМИНИСТРАЦИЯ УСТЬ-ЧИЖАПСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ**

|  |
| --- |
| **РАСПОРЯЖЕНИЕ** |

|  |  |  |
| --- | --- | --- |
| 01.08.2019  с. Старая Берёзовка  Об утверждении Порядка доступа к техническим средствам информационных систем, средствам защиты информации, средствам обеспечения функционирования, а так же в помещения и сооружения, в которых они установлены (для 1, 2, 3 и 4 уровня и класса защищенности) |  | № 38 |

В целях исполнения Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и постановления Администрации Усть-Чижапского сельского поселения от 31.07.2019 № 26 «Об отдельных мерах, направленных на реализацию Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»

1. Утвердить Порядок доступа к техническим средствам информационных систем, средствам защиты информации, средствам обеспечения функционирования, а так же в помещения и сооружения, в которых они установлены (для 1, 2, 3 и 4 уровня и класса защищенности), согласно приложению №1 к настоящему распоряжению.

2. Специалисту 1 категории Администрации Усть-Чижапского сельского поселения Алексеевой Д.И. ознакомить с настоящим распоряжением всех работников Администрации Усть-Чижапского сельского поселения, осуществляющих обработку персональных данных, под роспись.

|  |  |
| --- | --- |
| Глава Усть-Чижапского сельского поселения | С.М. Голещихин |

УТВЕРЖДЕН

распоряжением Администрации

Усть-Чижапского сельского поселения от 01.08.2019 № 38

Приложение №1

Порядок доступа к техническим средствам информационных систем,

средствам защиты информации, средствам обеспечения функционирования,

а так же в помещения и сооружения, в которых они установлены

(для 1, 2, 3 и 4 уровня и класса защищенности)

I. Общие положение

1.1. Настоящий Порядок доступа к техническим средствам информационных систем, средствам защиты информации, средствам обеспечения функционирования, а так же в помещения и сооружения, в которых они установлены (для 1, 2, 3 и 4 уровня и класса защищенности) (далее – Порядок) разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон).

1.2. Настоящий Порядок является дополнением к действующим муниципальным правовым актам Администрации Усть-Чижапского сельского поселения по вопросам обеспечения безопасности персональных данных и не исключает обязательного выполнения их требований.

II. Требования к техническим средствам информационных систем

2.1. Система защиты информации, реализуемая в информационной системе, в зависимости от актуальных угроз безопасности информации и структурно-функциональных характеристик информационной системы должна включать следующие меры по защите информации:

- обеспечение доверенной загрузки программного обеспечения и его компонентов;

- идентификацию и аутентификацию субъектов доступа и объектов доступа;

- управление доступом субъектов доступа к объектам доступа;

- обеспечение замкнутой программной среды;

- регистрацию событий безопасности;

- обеспечение целостности информации и программного обеспечения;

- антивирусную защиту;

- обнаружение вторжений;

- контроль (анализ) защищенности информации;

- контроль потоков информации;

- управление потоками информации;

- защиту каналов передачи информации;

- защиту технических средств.

2.1.1. Меры по обеспечению доверенной загрузки должны исключать несанкционированное использование [средств](http://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80) вычислительной техники и получение возможности доступа к информации конфиденциального характера в обход системы защиты информации.

Меры по обеспечению доверенной загрузки включают:

- блокировку доступа к ресурсам средств вычислительной техники;

- блокировку загрузки нештатной операционной системы, в том числе со съемных машинных носителей информации.

2.1.2. Меры по идентификации и аутентификации должны обеспечивать присвоение субъектам доступа и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности).

Меры по идентификации и аутентификации включают:

- идентификацию и аутентификацию пользователей, процессов, иных субъектов доступа;

- идентификацию и аутентификацию устройств (в том числе стационарных, мобильных и портативных), объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным программным обеспечением, иных объектов доступа;

- управление идентификаторами и аутентификаторами;

- защиту обратной связи при аутентификации;

- разрешение (запрет) действий субъектов доступа до идентификации и аутентификации;

- идентификацию и аутентификацию внешних пользователей.

2.1.3. Меры по управлению доступом должны обеспечивать разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

Меры по управлению доступом включают:

- реализацию методов управления доступом;

- реализацию типов доступа (чтение, запись, выполнение или иные типы доступа);

- реализацию правил разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил);

- управление сеансами доступа;

- управление видами доступа (локальный, удаленный);

- управление подключением устройств (стационарных, мобильных, портативных).

2.1.4. Меры по обеспечению замкнутой программной среды должны исключать установку (инсталляцию) неиспользуемого в обработке информации конфиденциального характера или запрещенного к использованию программного обеспечения и его компонентов (в том числе средств разработки и отладки программ), а также их загрузку (запуск) после установки.

Меры по обеспечению замкнутой программной среды включают:

управление запуском (обращениями) компонентов программного обеспечения;

управление установкой (инсталляцией) компонентов программного обеспечения;

запрет установки (инсталляции) запрещенного к использованию программного обеспечения и(или) его компонентов, в том числе средств разработки и отладки;

управление записью временных файлов.

2.1.5. Меры по регистрации событий безопасности должны обеспечивать распознавание, запись, хранение и защиту информации о событиях в информационной системе, относящихся к безопасности информации, а также возможность просмотра информации о таких событиях и реагирования на них.

Меры по регистрации событий безопасности включают:

- распознавание и запись информации о событиях, относящихся к безопасности информации;

- хранение и просмотр информации о событиях, относящихся к безопасности информации;

- защиту информации о событиях, относящихся к безопасности информации, от несанкционированного доступа;

- реагирование на события, связанные с нарушением свойств безопасности информации.

2.1.6. Меры по обеспечению целостности должны обеспечивать неизменность информации и программного обеспечения при неправомерном доступе к информации и (или) воздействии на нее, а так же возможность их восстановления.

Меры по обеспечению целостности включают:

- обеспечение целостности информации и программного обеспечения;

- контроль целостности информации и программного обеспечения;

- обеспечение возможности восстановления информации и программного обеспечения.

2.1.7. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Меры по антивирусной защите включают:

- реализацию антивирусной защиты;

- управление антивирусной защитой.

2.1.8. Меры по обнаружению вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней, а также реагирование на эти действия.

Меры по обнаружению вторжений включают:

- обнаружение вторжений;

- управление обнаружением вторжений.

2.1.9. Меры по контролю (анализу) защищенности информации должны обеспечивать выявление и оценку уязвимостей информационной системы, которые могут быть использованы для реализации актуальных угроз безопасности информации.

Меры по контролю (анализу) защищенности информации включают:

- анализ уязвимостей;

- контроль установки обновлений программного обеспечения;

- контроль параметров настройки, правильности функционирования программного обеспечения и средств защиты информации;

- контроль соответствия состава субъектов доступа и их прав (привилегий) правилам разграничения доступа;

- контроль состава технических средств обработки информации и программного обеспечения;

- контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей.

2.1.10. Меры по контролю потоков информации должны предотвращать утечку информации конфиденциального характера из информационной системы и исключать нецелевое использование ресурсов информационной системы.

Меры по контролю потоков информации включают:

- анализ содержания информации (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), выходящей за пределы информационной системы;

- реагирование на попытки неправомерной передачи информации конфиденциального характера из информационной системы;

- контроль нецелевого использования ресурсов информационной системы пользователями;

- реагирование на попытки нецелевого использования ресурсов информационной системы пользователями.

2.1.11. Меры по управлению потоками информации должны обеспечивать безопасность взаимодействия между сегментами информационной системы, а также информационной системы с другими информационными системами или информационно-телекоммуникационными сетями.

Меры по управлению потоками информации включают:

- фильтрацию потоков информации;

- нормализацию протоколов обмена (блокирование скрытых каналов передачи информации);

- скрытие структурно-функциональных характеристик информационной системы;

- однонаправленную передачу информации (программную, программно-техническую) между информационной системой и иными информационными системами;

- однонаправленную передачу информации (программную, программно-техническую) между техническими средствами информационной системы.

2.1.12. Меры по защите каналов передачи информации должны обеспечивать защиту информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны путем использования организационных мер и (или) средств защиты информации.

2.1.13. Меры по защите технических средств информационной системы должны обеспечивать защиту технических средств, а также информации конфиденциального характера, представленной в виде информативных электрических сигналов, физических полей.

Меры по защите технических средств включают:

- защиту информации от ее утечки по техническим каналам;

- защиту от несанкционированного физического доступа к средствам обработки информации и средствам обеспечения функционирования информационной системы;

- защиту от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов).

3. Меры по защите информации реализуются в системе защиты информации информационной системы применительно ко всем объектам и субъектам доступа на аппаратном, системном, прикладном и сетевом уровнях.

Блокирование (нейтрализация) актуальных угроз безопасности информации, приведенных в модели угроз безопасности информации, может обеспечиваться одной или совокупностью мер по защите информации. Содержание мер по защите информации, реализуемых в системе защиты информации информационной системы, определяется в зависимости от класса защищенности информационной системы.

Для определения мер по защите информации, обеспечивающих блокирование (нейтрализацию) актуальных угроз безопасности информации, и их содержания в зависимости от класса защищенности информационной системы применяются методические документы ФСТЭК России, разработанные и утвержденные в пределах ее полномочий.

4. Меры по защите информации, подлежащие реализации в системе защиты информации информационной системы, должны обеспечивать:

в информационных системах 1 класса защищенности - нейтрализацию (блокирование) угроз безопасности информации, связанных с действиями нарушителя с высоким потенциалом;

в информационных системах 2 класса защищенности - нейтрализацию (блокирование) угроз безопасности информации, связанных с действиями нарушителя со средним (умеренным) потенциалом;

в информационных системах 3 и 4 классов защищенности – нейтрализацию (блокирование) угроз безопасности информации, связанных с действиями нарушителя с низким потенциалом.

По результатам определения актуальных угроз безопасности информации оператором может быть принято решение о применении в информационных системах соответствующего класса защищенности мер по защите информации, обеспечивающих защиту от актуальных угроз безопасности информации, реализуемых нарушителем с более высоким потенциалом.

5. Средства защиты информации, используемые в информационных системах 1 и 2 классов защищенности, должны соответствовать 4 уровню контроля отсутствия недекларированных возможностей.

III. Построение системы защиты персональных данных

3.1. Система защиты персональных данных представляет собой совокупность организационных и технических мероприятий для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также иных неправомерных действий с ними.

3.2. Безопасность персональных данных достигается путём исключения несанкционированного, в том числе случайного, доступа к ним, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

3.3. Структура, состав и основные функции системы защиты персональных данных определяются исходя из уровня защищённости и класса защищённости информационных систем Управления.

3.4. Система защиты персональных данных включает в себя организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

3.5. Система защиты персональных данных призвана обеспечить:

конфиденциальность информации (защита от несанкционированного ознакомления);

целостность информации (актуальность и непротиворечивость информации, её защищённость от разрушения и несанкционированного изменения);

доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

3.6. Организационные меры как составная часть системы защиты персональных данных включают в себя создание и поддержание правовой базы безопасности персональных данных и разработку (введение в действие) организационно-распорядительных документов, предусмотренных Политикой информационной безопасности информационных систем персональных данных Управления.

3.7. Технические средства защиты информации реализуются при помощи соответствующих программно-технических средств и методов защиты. Перечень необходимых мер и средств защиты информации определяется по результатам внутренней проверки обеспечения защиты персональных данных в информационных системах.

IV. Порядок обеспечения безопасности при обработке персональных данных, обрабатываемых в Администрации Усть-Чижапского сельского поселения с использованием информационной системы персональных данных

4.1. Обработка персональных данных с использованием информационной системы персональных данных (далее - ИСПДн) означает совершение действий (операций) с такими данными с помощью объектов вычислительной техники.

Безопасность персональных данных при их обработке обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации.

4.2. Технические и программные средства защиты информации должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

4.3. Работа с персональными данными ИСПДн должна быть организована таким образом, чтобы обеспечивалась сохранность носителей персональных данных и средств защиты информации.

4.4. Компьютеры, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа. Пароль должен быть соответствовать требованием Положения о парольной политике в Администрации Усть-Чижапского сельского поселения, утвержденного распоряжением Администрации Усть-Чижапского сельского поселения от 31.07.2019 № 30 «Об утверждении Положения о парольной политике в Администрации Усть-Чижапского сельского поселения». Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

4.5. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

V. Ответственность

5.1. Сотрудники (работники) Администрации, виновные в нарушении требований настоящего Порядка, несут персональную ответственность в соответствии с законодательством Российской Федерации.