****

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

КРАСНОЯРСКИЙ КРАЙ

ТАЙМЫРСКИЙ ДОЛГАНО-НЕНЕЦКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН

**АДМИНИСТРАЦИЯ СЕЛЬСКОГО ПОСЕЛЕНИЯ ХАТАНГА**

**ПОСТАНОВЛЕНИЕ**

18.12.2013 г. № 177 - П

**Об утверждении Положения об обеспечении безопасности автоматизированной информационной системы, Положения о парольной защите при обработке персональных данных и иной конфиденциальной информации и Инструкции о применении средств антивирусной защиты информации в администрации сельского поселения Хатанга**

# Руководствуясь требованиями Федерального Закона Российской Федерации от 27.07. 2006  г. N 152-ФЗ "О персональных данных", Федерального Закона Российской Федерации от 27.07. 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", иных нормативных правовых актов в сфере защиты персональных данных, совершенствования системы антивирусной защиты информации,

**ПОСТАНОВЛЯЮ:**

1. Утвердить:
   1. Положение об обеспечении безопасности автоматизированной информационной системы администрации сельского поселения Хатанга (далее – Положение № 1), согласно приложению № 1.
   2. Положение о парольной защите при обработке персональных данных и иной конфиденциальной информации в администрации сельского поселения Хатанга (далее – Положение № 2), согласно приложению № 2.
   3. Инструкцию о применении средств антивирусной защиты информации в администрации сельского поселения Хатанга (далее – Инструкция), согласно приложению № 3.
2. Общему отделу администрации сельского поселения Хатанга (Майнагашева Е.В.):

2.1. Ознакомить с Положением № 1, Положением № 2 начальников структурных подразделений и самостоятельных отделов: Финансовый отдел (Смирнова О.В.), Отдел культуры (Майнагашев А.С.), Отдел по управлению муниципальным имуществом (Клыпина Н.Б.), работающих с автоматизированными информационными системами и осуществляющих обработку персональных данных и иной конфиденциальной информации, а так же до сведения Пользователей, допущенных к обработке персональных данных и иной конфиденциальной информации администрации сельского поселения Хатанга, в срок до 31.12.2013 г. под роспись в Листе ознакомления, согласно приложению № 4.

1. Начальникам структурных подразделений и самостоятельных отделов: Финансовый отдел (Смирнова О.В.), Отдел культуры (Майнагашев А.С.), Отдел по управлению муниципальным имуществом (Клыпина Н.Б.) администрации сельского поселения Хатанга:

3.1. Обеспечить выполнение Инструкции;

3.2. Довести настоящее Постановление в части пп.1.3,3.1 до сведения подчиненных сотрудников под роспись в Листе ознакомления согласно приложению № 4.

1. Назначить ответственным за систему антивирусной защиты информации и автоматизированную информационную систему:

- Третьякова Б.П., главного специалиста Отдела информационных ресурсов администрации сельского поселения Хатанга.

1. Ответственному за работу автоматизированной информационной системы администрации сельского поселения Хатанга (Третьяков Б.П.):

4.1. Организовать работу по обеспечению безопасности автоматизированных информационных систем администрации сельского поселения Хатанга в соответствии с утвержденным Положением № 1.

4.2. Обеспечить режим парольной защиты при обработке персональных данных и иной конфиденциальной информации в соответствии с утвержденным Положением № 2.

4.3. Обеспечить в соответствии с Инструкцией установку, настройку и обновление средств антивирусной защиты информации на серверах и рабочих станциях.

1. Настоящее Постановление вступает в силу с момента подписания, подлежит официальному опубликованию и размещению на официальном сайте органов местного самоуправления сельского поселения Хатанга.
2. Контроль за исполнением настоящего Постановления оставляю за собой.

Руководитель администрации

сельского поселения Хатанга Н.А. Клыгина

**Приложение № 1**

к Постановлению администрации

сельского поселения Хатанга

от 18.12. 2013 г. № 177 - П

Положение № 1

Об обеспечении безопасности автоматизированной информационной системы администрации сельского поселения Хатанга

**1. Общие положения**

Настоящее Положение определяет требования по обеспечению безопасности автоматизированной информационной системы (далее - АИС) администрации сельского поселения Хатанга (далее – Администрация).

АИС представляет собой IT-систему, предназначенную для автоматизации процессов формирования, обработки и анализа информации по основным направлениям деятельности Администрации.

Основными функциональными возможностями АИС Администрации являются:

* формирование, хранение и обновление сведений о сотрудниках Администрации;
* формирование, хранение и обновление сведений о клиентах (получателях услуг);
* формирование, хранение и обновление сведений о выполнении договоров с клиентами (получателями услуг);
* формирование и хранение сведений о структуре и объёмах оказываемых услуг;
* формирование, хранение и обновление сведений о плане работы Администрации;
* формирование, хранение и обновление сведений об использовании производственных ресурсов Администрации;
* формирование, хранение и обновление сведений о заключённых Администрацией договорах;
* обработка иной информации с учётом специфики деятельности организации.

В качестве информации, подлежащей защите в АИС Администрации, рассматриваются:

* персональные данные сотрудников Администрации (далее – работников);
* персональные данные клиентов (получателей услуг).

Основными группами угроз, на противостояние которым направлены цели и требования безопасности, являются:

* угрозы, связанные с осуществлением несанкционированного доступа (ознакомления) с информацией, содержащей сведения о персональных данных работников и клиентов (получателей услуг) при ее обработке и хранении;
* угрозы, связанные с несанкционированным копированием (хищением) информации, содержащей сведения о персональных данных работников и клиентов (получателей услуг);
* угрозы, связанные с осуществлением доступа к информации, содержащей сведения о персональных данных работников и клиентов (получателей услуг), без разрешения на то её владельца (субъекта персональных данных);
* угрозы, связанные с нарушением порядка доступа к информации, содержащей сведения о персональных данных работников и клиентов, передаваемой заинтересованным лицам;
* угрозы, связанные с перехватом информации, содержащей сведения о персональных данных работников и клиентов (получателей услуг), из каналов передачи данных с использованием специализированных программно-технических средств;
* угрозы, связанные с потерей (утратой) информации, содержащей сведения о персональных данных работников и клиентов (получателей услуг), вследствие сбоев (отказов) программного и аппаратного обеспечения;
* угрозы, связанные с внедрением компьютерных вирусов и другого вредоносного программного обеспечения;
* угрозы, связанные с осуществлением несанкционированных информационных воздействий (направленных на «отказ в обслуживании» для сервисов, модификацию конфигурационных данных программно-аппаратных средств, подбор идентификационной информации и т.п.).

**2. Основные функциональные возможности АИС, связанные**

**с обеспечением безопасности (защитой информации)**

#### 2.1. Защита данных пользователя

АИС должна осуществлять функции и политику избирательного (дискреционного) управления доступом. Избирательное управление доступом должно предоставлять возможность ограничивать и контролировать доступ к системе и к информации, содержащей сведения о персональных данных.

Каждый Пользователь, получающий доступ к АИС, сначала должен проходить процедуру идентификации.

В АИС доступ к информации должен быть разрешен только уполномоченным на это Пользователям.

#### 2.2. Идентификация

АИС должна требовать, чтобы все субъекты доступа уникально идентифицировались при доступе к АИС с помощью ввода идентификатора и пароля. Идентификация должна осуществляться до выполнения субъектом доступа каких-либо действий.

#### 

**3. Среда безопасности АИС**

**3.1. Модели угроз, характерные для АИС**

3.1.1.Осуществление несанкционированного ознакомления с персональными данными работников и клиентов (получателей услуг).

**Источники угрозы –** внешний злоумышленник.

**Способ (метод) реализации угрозы –** перехват информации из каналов передачи данных с использованием специализированных программно-технических средств.

**Используемые уязвимости –** возможные недостатки механизмов защиты информации при ее передаче по каналам передачи данных, связанные с возможностью несанкционированного ознакомления с передаваемой информацией третьих лиц.

**Вид информации, потенциально подверженной угрозе –** персональные данные работников и клиентов (получателей услуг).

**Нарушаемое свойство безопасности –** конфиденциальность.

**Возможные последствия реализации угрозы –** нанесения морального и/или материального ущерба лицу, фигурирующему в перехваченной информации. Нанесение косвенного материального ущерба Администрации.

3.1.2. Осуществление несанкционированного ознакомления с персональными данными работников и клиентов (получателей услуг) и их модификация (в том числе подмена).

**Источники угрозы –** внешний злоумышленник.

**Способ (метод) реализации угрозы –** перехват информации из каналов передачи данных с использованием специализированных программно-технических средств; модификация (в том числе подмена) перехваченной информации и навязывание ложной информации.

**Используемые уязвимости –** недостатки механизмов защиты информации при ее передаче по каналам передачи данных, связанные с возможностью несанкционированного ознакомления и модификации (в том числе подмены) передаваемой информации.

**Вид информации, потенциально подверженной угрозе –** персональные данные работников и обучаемых.

**Нарушаемые свойства безопасности –** конфиденциальность, целостность.

**Возможные последствия реализации угрозы –** нанесения морального и/или материального ущерба лицу, фигурирующему в перехваченной информации из-за несанкционированного раскрытия конфиденциальной информации или распространения раскрытых данных. Нанесение косвенного материального ущерба Администрации.

3.1.3.Нарушение доступности, утрата или искажение предоставляемых персональных данных работников и клиентов вследствие сбоев (отказов) программного и аппаратного обеспечения.

**Источники угрозы –** программное и аппаратное обеспечение.

**Способ (метод) реализации угрозы –** сбои (отказы) программного и аппаратного обеспечения.

**Используемые уязвимости –** недостатки механизмов обеспечения доступности требуемой информации, связанные с возможностью блокирования предоставления информации на недопустимое время.

**Вид информации, потенциально подверженной угрозе –** персональные данные работников и клиентов (получателей услуг).

**Нарушаемое свойство безопасности –** доступность, достоверность.

**Возможные последствия реализации угрозы –** нарушение со стороны взятых на себя обязательств по обработке персональных данных работников и клиентов (получателей услуг) и может привести к прямому или косвенному материальному ущербу Администрации.

3.1.4. Нарушение согласованности данных в персональных данных работников и клиентов (получателей услуг) вследствие сбоев (отказов) программного и аппаратного обеспечения, а также ошибок работников Администрации.

**Источники угрозы –** программное и аппаратное обеспечение, работники Администрации.

**Способ (метод) реализации угрозы –** сбои (отказы) программного обеспечения и ошибки работников Администрации.

**Используемые уязвимости –** недостатки механизмов обеспечения согласованности данных в базе данных (далее БД) АИС, связанные с возможностью нарушения согласованности.

**Вид информации, потенциально подверженной угрозе –** персональные данные работников и клиентов (получателей услуг).

**Нарушаемые свойства безопасности активов –** достоверность, целостность.

**Возможные последствия реализации угрозы –** рассогласование в персональных данных работников и клиентов, хранимых в БД АИС, что, в свою очередь, приведет к возможному нанесения морального и/или материального ущерба Администрации.

3.1.5.Осуществление доступа (ознакомления) с персональными данными клиентов (получателей услуг), хранимыми и обрабатываемыми в АИС по окончании срока действия договора, выполнение обязательств по которому предусматривает обработку персональных данных.

**Источники угрозы –** уполномоченные на доступ к персональным данным внутренние и внешние пользователи.

**Способ (метод) реализации угрозы** – осуществление доступа к персональным данным обучаемых с использованием штатных средств, предоставляемых программно-аппаратным обеспечением АИС.

**Используемые уязвимости –** недостатки механизмов защиты персональных данных обучаемых, связанные с возможностью доступа к ним без письменного согласия субъекта персональных данных или после окончания срока его действия.

**Вид информации, потенциально подверженной угрозе** – персональные данные клиентов (получателей услуг).

**Нарушаемые свойства безопасности** – конфиденциальность.

**Возможные последствия реализации угрозы** – несанкционированное ознакомление с персональными данными ведет к нанесению морального и/или материального ущерба клиенту из-за несанкционированного раскрытия конфиденциальной информации.

3.1.6.Внедрение в АИС вирусов и другого вредоносного программного обеспечения при взаимодействии с внешними системами, а также Пользователями с носителей информации, используемых на автоматизированных рабочих местах.

**Источники угрозы –** внутренние пользователи Администрации, внешние системы.

**Способ (метод) реализации угрозы –** внедрение вирусов и другого вредоносного программного обеспечения при взаимодействии с внешними системами (файловый обмен, электронная почта и т.п.), а также при использовании съемных носителей информации на автоматизированных рабочих местах.

**Используемые уязвимости –** недостатки механизмов защиты АИС от внедрения вирусов и другого вредоносного программного обеспечения, связанные с возможностью внедрения вирусов и другого вредоносного программного обеспечения.

**Вид информации, потенциально подверженной угрозе –** программное обеспечение информационной системы Администрации.

**Нарушаемое свойство безопасности активов –** целостность.

**Возможные последствия реализации угрозы –** нарушение режимов функционирования АИС, потеря (утрата) и искажение информации, снижение уровня защищенности АИС. Ведет к возможному материальному ущербу Администрации.

**Способ (метод) реализации угрозы –** несанкционированные информационные воздействия с использованием специализированного программно-аппаратного обеспечения.

**Используемые уязвимости –** недостатки механизмов защиты АИС от несанкционированных внешних воздействий.

**Вид информации, потенциально подверженной угрозе –** программно-аппаратное обеспечение АИС.

**Нарушаемые свойства безопасности активов –** конфиденциальность, целостность.

**Возможные последствия реализации угрозы –** нарушение режимов функционирования АИС, снижение уровня защищенности АИС. Ведет к возможному материальному ущербу Администрации.

**3.2. Политика и цели безопасности для АИС**

АИС должна обеспечить следование приведенным ниже правилам безопасности:

1. Должна быть обеспечена регистрация и учет обработки предоставленных Администрации персональных данных работников и клиентов (получателей услуг).
2. Должна быть обеспечена возможность надежного хранения персональных данных работников и клиентов (получателей услуг) (в течение действия срока трудового договора и договоров на оказание услуг соответственно).
3. Должна быть обеспечена защита информации, составляющей персональные данные работников и клиентов (получателей услуг), при ее обработке, хранении и передаче специализированными средствами защиты.

**3.3. Политика и цели безопасности для среды функционирования АИС**

Среда функционирования АИС должна обеспечить следование приведенным ниже правилам безопасности:

1. Должна быть исключена возможность несанкционированного физического доступа к программно-аппаратным элементам системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, со стороны посторонних лиц.
2. На объектах системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должны быть обеспечено наличие и надлежащее использование средств антивирусной защиты, сертифицированных по требованиям безопасности. Должно быть обеспечено регулярное обновление антивирусных баз.
3. Объекты системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть подключены к внешним вычислительным сетям общего пользования с использованием надлежащих средств межсетевого экранирования, сертифицированных по требованиям безопасности.
4. Уполномоченные на работу с АИС Пользователи должны быть благонадежными, руководствоваться в своей работе эксплуатационной документацией на АИС, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.

**Приложение № 2**

к Постановлению администрации

сельского поселения Хатанга

от 18.12. 2013 г. № 177 - П

Положение № 2

О парольной защите при обработке персональных данных и иной конфиденциальной информации

Данное Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (учетных записей Пользователей) в информационных системах (ИС) администрации сельского поселения Хатанга (далее - Администрация), а также контроль за действиями Пользователей и обслуживающего персонала при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех ИС и контроль за действиями Пользователей и обслуживающего персонала при работе с паролями возлагается на ответственного за работу автоматизированных информационных систем (далее АИС) - парольной защиты.

2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИС самостоятельно с учетом следующих требований:

* длина пароля должна быть не менее 8 символов;
* в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры;
* при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
* личный пароль Пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3. В случае если формирование личных паролей Пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на ответственного за АИС. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

4. При наличии технологической необходимости (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) использования имен и паролей некоторых сотрудников (Пользователей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей передавать на хранение руководителю своего подразделения их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте. Опечатанные конверты с паролями Пользователей должны храниться в сейфе. Для опечатывания конвертов должна применяться Главная печать Администрации.

5. Полная плановая смена паролей Пользователей должна проводиться регулярно, не реже одного раза в квартал *(или в иные установленные Оператором сроки)*.

6. Внеплановая смена личного пароля или удаление учетной записи Пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться ответственным за АИС немедленно после окончания последнего сеанса работы данного Пользователя с системой.

7. Внеплановая полная смена паролей всех Пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственного за средства защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.

8. В случае компрометации личного пароля Пользователя ИС должны быть немедленно предприняты меры в соответствии с п. 6 или п. 7 настоящего Положения в зависимости от полномочий владельца скомпрометированного пароля.

9. Хранение Пользователем своих паролей на бумажном носителе допускается только в сейфе у начальника структурного подразделения в опечатанном Главной печатью конверте.

10. Повседневный контроль за действиями Пользователей системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на начальников структурных подразделений и самостоятельных отделов Администрации, периодический контроль – возлагается на ответственного за АИС.

**Приложение № 3**

к Постановлению администрации

сельского поселения Хатанга

от 18.12. 2013 г. № 177 - П

Инструкции о применении средств антивирусной защиты информации в администрации сельского поселения Хатанга

**1. Термины и определения**

В Инструкции о применении средств антивирусной защиты информации (далее - Инструкция) использованы следующие термины и определения:

*Пользователи* - должностные лица, а также все другие лица и организации, использующие в работе средства электронно-вычислительной техники.

*Администраторы антивирусной защиты информации* (далее -администраторы АВЗ) - должностные лица подразделений информационной безопасности (технических подразделений), назначенные ответственными за эксплуатацию средств антивирусной защиты информации и обеспечивающие организацию и эффективное использование системы антивирусной защиты информации.

*Локально-вычислительная сеть* (далее - ЛВС) - группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными (неарендуемыми) высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

*Антивирусная защита информации* - система организационно-технических мероприятий, требований и условий использования электронно-вычислительной техники, предназначенная для предотвращения заражения программными вирусами информационно-вычислительных ресурсов посредством применения средств антивирусной защиты информации.

*Вредоносная программа* - программа для электронно-вычислительных машин (ЭВМ), заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети.

*Программные вирусы* - разновидность вредоносных программ, отличительной особенностью которых является способность к размножению

(саморепликации). В дополнение к этому они могут повреждать или полностью уничтожать данные, подконтрольные пользователю, от имени

которого была запущена зараженная программа.

*Отдел информационных ресурсов* – структурное подразделение организации, ответственное за функционирование автоматизированных информационных систем и электронно-вычислительной техники. На него возложены функции службы информационной безопасности.

**2. Общие положения**

1. Настоящая Инструкция разработана в целях осуществления антивирусной защиты информации, содержащейся и обрабатываемой на рабочих станциях Администрации, от несанкционированного копирования, модификации и разрушения данных, используемых в деятельности учреждения, а также нарушения работы

используемого программного обеспечения при воздействии вирусов и других вредоносных программ посредством комплекса организационно-технических мероприятий по обеспечению информационной безопасности.

2. Настоящая Инструкция определяет порядок применения средств антивирусной защиты в Администрации, задачи, обязанности и права администраторов АВЗ, пользователей средств антивирусной защиты информации, порядок установки и применения обновлений, подключения средств антивирусной защиты, а также порядок ликвидации последствий воздействия программных вирусов.

3. Требования настоящей Инструкции обязательны для выполнения всеми пользователями и администраторами АВЗ, а также иными лицами, использующими средства вычислительной техники.

4. Общее руководство обеспечением антивирусной защиты информации в осуществляется информационно-технической службой (далее - АВЗ) и ответственным за информационную безопасность и техническую защиту информации АВЗ.

5. Ответственный за информационную безопасность и техническую защиту информации АВЗ осуществляет непосредственное руководство организацией проведения работ по антивирусной защите информации в организации через сотрудников АВЗ.

6. Практическое решение задач, связанных с организацией антивирусной защиты информации и применением средств антивирусной защиты информации в структурных подразделениях, осуществляется сотрудниками АВЗ.

7. При возникновении ситуаций, не включенных в положения настоящей Инструкции, решение принимается администратором АВЗ по согласованию с ответственным за информационную безопасность и техническую защиту информации АВЗ.

**3. Порядок применения средств антивирусной защиты**

**информации в Администрации**

1. Средства антивирусной защиты информации должны устанавливаться на всех средствах вычислительной техники, эксплуатируемых в Администрации. При технологической необходимости на отдельные средства вычислительной техники средства антивирусной защиты информации могут не устанавливаться. Список таких исключений утверждается руководителем АВЗ и пересматривается ежегодно.

2. Порядок применения средств антивирусной защиты информации устанавливается с учетом соблюдения следующих требований:

- обязательный входной контроль за отсутствием программных вирусов во всех поступающих на объект информатизации электронных носителях информации, информационных массивах, программных средствах общего и специального назначения;

- обязательная проверка всех электронных писем на предмет отсутствия программных вирусов;

- периодическая проверка на предмет отсутствия программных вирусов жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка съемных носителей информации перед началом работы с ними;

- внеплановая проверка жестких магнитных дисков и съемных носителей информации в случае подозрения на наличие программных вирусов;

- восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами.

3. Уполномоченное лицо Администрации по антивирусной защите информации обеспечивает:

- управление конфигурацией и логической структурой всего программного обеспечения системы антивирусной защиты информации;

- управление установкой и обновлением лицензионных ключей средств антивирусной защиты информации;

- управление рассылкой и установкой обновлений баз средств антивирусной защиты информации;

- ограничение доступа пользователей на рабочих местах к настройкам установленных средств антивирусной защиты информации;

- настройку рассылки сообщений об обнаружении вирусов, о сбоях в работе средств антивирусной защиты и т.п.;

- удаленное решение проблем, возникающих в процессе использования средств антивирусной защиты информации.

4. Для рабочих станций и серверов, которые не имеют подключения к ЛВС, средства антивирусной защиты информации для них устанавливаются локально в порядке, определенном администратором АВЗ, с учетом требований настоящей Инструкции.

5. Инсталляция и настройка средств антивирусной защиты информации осуществляются в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.

6. Копирование любой информации, переносимой с помощью любых съемных носителей информации, должно производиться только после проведения процедуры полного антивирусного контроля съемного носителя.

7. Антивирусная профилактика является необходимым элементом защиты информационных ресурсов учреждения от их модификации и

уничтожения. Антивирусная профилактика состояния средств антивирусной

защиты информации на серверах и рабочих станциях должна проводиться по

согласованию с администраторами АВЗ в нерабочее время, за исключением внештатных ситуаций.

**4. Порядок обновления баз данных средств антивирусной**

**защиты информации**

1. Своевременное обновление баз данных средств антивирусной защиты информации в структурных подразделениях является неотъемлемой частью обеспечения эффективной политики антивирусной защиты информации.

2. Обновление баз данных средств антивирусной защиты информации на рабочих станциях, установленных локально в структурных подразделениях, должно производиться не реже одного раза в неделю в порядке, устанавливаемом администратором АВЗ, с учетом требований настоящей Инструкции.

3. На рабочем месте администратора АВЗ могут быть установлены средства, позволяющие через ЛВС управлять компонентами системы антивирусной защиты, установленными на рабочих станциях и серверах в структурных подразделениях, а также проводить обновления баз средств антивирусной защиты информации. В случае если рабочая станция пользователя не подключена к ЛВС, обновление средств антивирусной защиты информации производится пользователем через съемные носители информации. Периодичность обновления определяется программными требованиями средств антивирусной защиты информации или устанавливается администратором АВЗ.

**5. Обязанности, права и порядок назначения**

**администраторов АВЗ**

1. Администраторы АВЗ обязаны обеспечивать соблюдение в учреждении политики антивирусной защиты информации и выявление фактов заражения программными вирусами.

2. К основным задачам администратора АВЗ относятся организация процесса установки и обновления средств антивирусной защиты информации

на рабочих станциях пользователей и обеспечение технического сопровождения действий пользователей в случаях обнаружения программных вирусов, а также осуществление контроля за состоянием системы антивирусной защиты информации.

3. Администратор АВЗ несет ответственность: за своевременную установку средств антивирусной защиты информации;

- за эксплуатацию системы антивирусной защиты информации;

- за своевременное обновление лицензий на средства антивирусной защиты информации;

- за своевременное обновление баз данных средств антивирусной защиты информации.

4. Администратор АВЗ имеет право:

- вносить предложения по совершенствованию системы антивирусной защиты информации в структурных подразделениях организации;

- принимать участие в планировании мероприятий по антивирусной защите информации в организации и планировании оснащения средствами антивирусной защиты информации структурных подразделений;

- осуществлять контроль состояния средств антивирусной защиты информации в структурных подразделениях;

- проводить служебные проверки по фактам заражения программными вирусами автоматизированных систем обработки информации и средств вычислительной техники в структурных подразделениях организации;

- оказывать помощь в решении проблем, возникающих при эксплуатации средств антивирусной защиты информации в структурных подразделениях организации.

5. Назначение администраторов АВЗ организации осуществляется на основании приказа Администрации с обязательным отражением обязанностей в должностной инструкции.

6. Обязанности администраторов АВЗ могут совмещать должностные лица, назначенные администраторами баз данных (автоматизированных информационных систем), специалисты АВЗ. Администраторами АВЗ не могут быть должностные лица сторонних организаций. Должностные лица, исполняющие обязанности администраторов АВЗ, утверждается приказом руководителя Администрации.

7. Обязанности администраторов АВЗ Администрации другие лица могут исполнять только на основании приказа руководителя Администрации о временном исполнении обязанностей администратора АВЗ, в котором указан срок исполнения обязанностей администратора АВЗ.

**6. Обязанности пользователей средств антивирусной**

**защиты информации**

1. Пользователь обязан изучить настоящую Инструкцию и ознакомиться с необходимостью несения ответственности за выполнение ее требований под роспись.

2. Пользователям запрещается:

- отключать средства антивирусной защиты информации во время работы;

- использовать средства антивирусной защиты информации, отличные от поддерживаемых АВЗ, перечень которых доводится до сведения пользователей АВЗ или администраторов АВЗ;

- без разрешения администратора ЛВС и администратора АВЗ копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

3. Ввод информации с магнитных, оптических, магнитооптических и любых других съемных носителей информации неслужебного характера должен осуществляться пользователем только с разрешения администраторов ЛВС или администраторов АВЗ.

4. В случае появления подозрений на наличие программных вирусов в ЛВС пользователи должны немедленно проинформировать об этом администратора АВЗ. В случае выявления инцидентов (фактов и т.п.), связанных со сбоями в работе средств антивирусной защиты, пользователь обязан незамедлительно сообщить об этом ответственному за информационную безопасность и техническую защиту информации АВЗ.

**7. Порядок действий пользователей и администраторов АВЗ**

**при обнаружении вирусов**

1. Основными путями проникновения вирусов в информационно - вычислительную сеть организации являются: гибкие магнитные диски, компакт-диски, иные съемные накопители информации, электронная почта, файлы, получаемые из сети Интернет, ранее зараженные рабочие станции. В случае обнаружения программных вирусов при входном контроле отчуждаемых носителей информации, файлов или почтовых сообщений, поступивших в структурные подразделения, пользователь должен:

- приостановить процесс приема-передачи информации;

- сообщить администратору АВЗ или ответственному за информационную безопасность и техническую защиту информации АВЗ о факте обнаружения программного вируса;

- принять по согласованию с администратором АВЗ меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации;

- сообщить о факте обнаружения программного вируса в структурное подразделение, из которого поступили зараженные съемные электронные носители информации, файлы или почтовые сообщения.

2. При обнаружении программных вирусов в процессе обработки информации пользователь обязан:

- немедленно приостановить все работы;

- сообщить администратору АВЗ или ответственному за информационную безопасность и техническую защиту информации АВЗ о факте обнаружения программных вирусов;

- принять по согласованию с администратором АВЗ меры по локализации и удалению программного вируса с использованием средств антивирусной защиты информации.

3. Программные средства общего и специального назначения, используемые в структурных подразделениях для обработки информации, отнесенной к служебной тайне, в случае обнаружения программных вирусов подлежат обязательной переустановке с рабочих копий эталона.

4. При невозможности ликвидации последствий заражения программными вирусами администратору АВЗ необходимо:

- заархивировать зараженные файлы с внедренными программными вирусами и направить с приложением соответствующего сопроводительного документа в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;

- осуществить полную переустановку программного обеспечения на зараженном компьютере.

5. При получении информации о возможном нарушении либо выявлении факта нарушения требований настоящей Инструкции работа на рабочей станции данного пользователя незамедлительно блокируется по решению администратора АВЗ.

6. Все факты модификации и разрушения данных на серверах или рабочих станциях, заражение их вирусами, а также обнаружение других вредоносных программ классифицируются как значимые нарушения информационной безопасности и должны анализироваться посредством проведения служебного расследования, проводимого по распоряжению руководителя Администрации.

**8. Ответственность за выполнение требований Инструкции**

1. За нарушение настоящей Инструкции администратор АВЗ и пользователи несут ответственность, установленную действующим законодательством Российской Федерации и нормативными правовыми актами.

2. Руководители структурных подразделений несут ответственность за выполнение мероприятий по антивирусной защите информации на средствах вычислительной техники, эксплуатируемых подчиненными должностными лицами, и за ознакомление их (под роспись) с настоящей Инструкцией в своем структурном подразделении.

3. Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации на своих рабочих местах, в том числе за своевременное обновление антивирусных баз средств антивирусной защиты информации и получение новых лицензионных ключей, несет администратор АВЗ, за которым закреплены средства вычислительной техники.

4. В случае нарушения требований настоящей Инструкции, связанных с применением пользователем средств антивирусной защиты информации, пользователь несет персональную ответственность, установленную действующим законодательством Российской Федерации и локальными нормативными актами организации.

5. Ответственность за выполнение требований настоящей Инструкции администраторами АВЗ несут непосредственно администраторы АВЗ и руководители подразделений, в которых работают администраторы АВЗ.

**9. Порядок оснащения организации средствами антивирусной**

**защиты информации**

1. Оснащение средствами антивирусной защиты информации является видом материального обеспечения и осуществляется в организации централизованно.

2. Передача полученных средств антивирусной защиты на объекты, не входящие в состав организации, запрещена. За несанкционированное распространение средств антивирусной защиты информации виновные несут ответственность в соответствии с законодательством Российской Федерации.

**Приложение № 4**

к Постановлению администрации

сельского поселения Хатанга

от 18.12. 2013 г. № 177 - П

Лист ознакомления

С Постановлением администрации сельского поселения Хатанга «Об утверждении Положения об обеспечении безопасности автоматизированной информационной системы администрации сельского поселения Хатанга, Положения о парольной защите при обработке персональных данных и иной конфиденциальной информации в администрации сельского поселения Хатанга*»* ознакомлен(а):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Должность | Ф. И. О. | Подпись | Дата |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |