**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**АДМИНИСТРАЦИЯ ТРУБЧЕВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА**

**Р А С П О Р Я Ж Е Н И Е**

от 01.06.2021г. № 472-р

г. Трубчевск

Об утверждении инструкций в сфере защиты персональных данных

в администрации Трубчевского муниципального района

Во исполнение требований Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», иных нормативных документов по защите информации:

1. Утвердить:

1.1. Инструкцию № 1-ИБ ответственного за организацию обработки персональных данных в администрации Трубчевского муниципального района (приложение 1).

1.2. Инструкцию № 2-ИБ ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных администрации Трубчевского муниципального района (приложение 2).

1.3. Инструкцию № 3-ИБ ответственного за администрирование средств защиты информации (администратора безопасности) в информационных системах персональных данных администрации Трубчевского муниципального района (приложение 3).

1.4. Инструкцию № 4-ИБ ответственного за эксплуатацию информационной системы персональных данных в администрации Трубчевского муниципального района (приложение 4).

1.5. Инструкцию № 5-ИБ по выполнению режимных мер и допуску к информационной системе персональных данных администрации Трубчевского муниципального района (приложение 5).

1.6. Инструкцию № 6-ИБ пользователю информационной системы персональных данных в части обеспечения безопасности персональных данных при их обработке в информационной системе в администрации Трубчевского муниципального района (приложение 6).

1.7. Инструкцию № 7-ИБ по организации парольной защиты в информационных системах персональных данных администрации Трубчевского муниципального района (приложение 7).

1.8. Инструкцию № 8-ИБ по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, защищаемой информации и средств защиты в администрации Трубчевского муниципального района (приложение 8).

1.9. Инструкцию № 9-ИБ по антивирусной защите в администрации Трубчевского муниципального района (приложение 9).

1.10. Инструкцию № 10-ИБ по ведению журналов в администрации Трубчевского муниципального района (приложение 10).

1.11. Инструкцию № 11-ИБ по проверке электронного журнала обращений к информационной системе персональных данных администрации Трубчевского муниципального района (приложение 11).

1.12. Инструкцию № 12-ИБ по порядку обращения с сертифицированными средствами криптографической защиты информации, предназначенными для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах администрации Трубчевского муниципального района, и криптоключами к ним (приложение 12).

1.13. Инструкцию № 13-ИБ по использованию съемных носителей информации в администрации Трубчевского муниципального района (приложение 13).

1.14. Инструкцию № 14-ИБ о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения информационных систем обработки персональных данных администрации Трубчевского муниципального района (приложение 14).

1.15. Инструкцию № 15-ИБ по работе с инцидентами информационной безопасности в администрации Трубчевского муниципального района (приложение 15).

1.16. Инструкцию № 16-ИБ по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств информационной системы персональных данных в администрации Трубчевского муниципального района (приложение 16);

1.7. Инструкцию № 17-ИБ по контролю защищенности информации в информационных системах администрации Трубчевского муниципального района (приложение 17).

2. Признать утратившими силу распоряжение администрации Трубчевского муниципального района от 26.10.2015 № 817-р «Об утверждении инструкций в сфере защиты персональных данных в администрации Трубчевского муниципального района», от 17.08.2016 № 680-р «Об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты информации».

3. Начальнику организационно-правового отдела администрации Трубчевского муниципального района Москалевой О.А. довести настоящее распоряжение до сведения уполномоченных должностных лиц администрации Трубчевского муниципального района.

4. Ответственному за обеспечение безопасности, администраторам безопасности ИСПДн администрации Трубчевского муниципального района в 2-хмесячный срок со дня принятия настоящего распоряжения обеспечить организацию обработки ПДн администрации Трубчевского муниципального района в соответствии с нормативными документами по защите информации и настоящим распоряжением.

5. Настоящее распоряжение разместить на официальном сайте администрации Трубчевского муниципального района в сети Интернет по адресу: http://www.trubech.ru/ в течение 10 дней после его принятия.

6. Контроль за исполнением настоящего распоряжения возложить на заместителя главы администрации Трубчевского муниципального района С.Н. Тубол.

**Глава администрации**

**Трубчевского муниципального района И.И. Обыдённов**

Приложение 1

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 472-р

**ИНСТРУКЦИЯ № 1-ИБ**  
ответственного за организацию обработки персональных данных

в администрации Трубчевского муниципального района

1. Общие положения

Настоящая инструкция определяет права, обязанности и ответственность лица, ответственного за организацию обработки персональных данных в администрации Трубчевского муниципального района.

Ответственный за организацию обработки персональных данных в администрации Трубчевского муниципального района (далее – Администрация) в своей деятельности руководствуется:

* Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
* Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;
* Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687;
* Приказом Федеральной службы по техническому и экспортному контролю 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»;
* Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1. Обязанности

Ответственный за организацию обработки персональных данных обязан:

* Доводить до сведения работников положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к обеспечению безопасности персональных данных;
* Осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, а именно организовывать проведение периодических (не менее одного раза в год) проверок соответствия обработки персональных данных. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывать непосредственному руководителю в письменном виде;
* Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и/или осуществлять контроль за приемом и обработкой таких обращений и запросов.

1. Ответственность

За неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей инструкцией, ответственный за организацию обработки персональных данных несет персональную ответственность в соответствии с законодательством Российской Федерации.

1. Права

Ответственный за организацию обработки персональных данных имеет право:

* Требовать от работников письменных объяснений по фактам нарушения ими требований законодательства Российской Федерации, локальных актов о персональных данных и защите персональных данных;
* Вносить предложения непосредственному руководителю об отстранении работников от обработки персональных данных, применению к ним дисциплинарных взысканий, при обнаружении нарушения ими требований законодательства Российской Федерации, локальных актов по вопросам обработки персональных данных или требований к защите персональных данных.

Приложение 2

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 472-р

**ИНСТРУКЦИЯ № 2-ИБ**  
ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных

администрации Трубчевского муниципального района

1. Общие положения

Настоящая инструкция определяет права и обязанности лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных в администрации Трубчевского муниципального района (далее – ИСПДн, Администрация).

Лицо ответственное за обеспечение безопасности персональных данных в ИСПДн (далее – администратор информационной безопасности) это лицо, отвечающее за обеспечение заданных характеристик информации, содержащей персональные данные (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

Администратор информационной безопасности в ИСПДн осуществляет контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных при их обработке в ИСПДн с использованием автоматизированных рабочих мест.

1. Обязанности администратора информационной безопасности

Администратор информационной безопасности обязан:

* Знать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в ИСПДн;
* Знать перечень обрабатываемых персональных данных, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных.
* Уметь пользоваться средствами защиты информации и осуществлять их непосредственное администрирование;
* Еженедельно осуществлять резервное копирование информации, содержащей персональные данные (при необходимости);
* Обязан осуществлять периодический контроль за выполнением сотрудниками, эксплуатирующими ИСПДн (пользователями ИСПДн), мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн;
* Участвовать в работе по проведению внутреннего контроля соответствия обработки персональных данных требованиям по защите информации;
* Обязан анализировать журнал системы защиты информации от несанкционированного доступа (НСД), проводить проверки электронного журнала обращений к информационным системам персональных данных;
* Обязан обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания АРМ;
* Обязан вести журнал учета средств защиты информации, используемых в ИСПДн;
* Обязан присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ;
* Обязан проводить инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и средствами защиты информации в соответствии с технической документацией на используемые средства защиты;
* Обязан проводить мероприятия по организации антивирусной защиты;
* Осуществлять организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями, согласно инструкции по организации парольной защиты в информационных системах персональных данных;
* Обязан организовать ведение журнала учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации;
* Обязан немедленно сообщать ответственному за организацию обработки персональных данных, информацию об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ, а также принимать необходимые меры по устранению нарушений:
* Установить причины, по которым стал возможным НСД;
* Установить последствия, к которым привел НСД;
* Зафиксировать случай НСД в виде документа (акта, служебной записки и т.д.) с описанием причин НСД, предполагаемых или установленных нарушителей и последствий;
* Провести проверку настроек средств защиты информации и операционных систем на соответствие требованиям руководящих документов и разрешительной системы доступа пользователей к защищаемым информационным ресурсам и объектам доступа ИСПДн, при необходимости провести настройку;
* Провести инструктаж пользователей ИСПДн по выполнению требований по обеспечению защиты персональных данных.

1. Права администратора информационной безопасности.

Администратор информационной безопасности имеет право:

* + Требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкции о порядке работы пользователей в ИСПДн в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;
  + Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;
  + Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности персональных данных к ответственному за организацию обработки персональных данных в ИСПДн и/или ответственному за эксплуатацию ИСПДн.

1. Ответственность администратора информационной безопасности

На администратора информационной безопасности возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн;

Администратор информационной безопасности в ИСПДн несет ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение 3

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 472-р

**ИНСТРУКЦИЯ № 3-ИБ**

ответственного за администрирование средств защиты информации (администратора безопасности) в информационных системах персональных данных администрации Трубчевского муниципального района

1. Общие положения

1.1. Инструкция ответственного за администрирование средств защиты информации (администратора безопасности) в информационных системах персональных данных администрации Трубчевского муниципального района (далее – ИС Администрации) (далее – Инструкция) определяет функции, права и обязанности Администратора информационной безопасности (далее – Администратор ИБ) по вопросам обеспечения информационной безопасности при подготовке и исполнении документов в ИС Администрации.

* 1. Администратор ИБ назначается из числа сотрудников Администрации распоряжением Администрации и обеспечивает правильность использования и нормальное функционирование установленной системы защиты ИС Администрации.
  2. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения режима конфиденциальности и не исключает обязательного выполнения их требований.
  3. Администратор ИБ обладает правами доступа к любым программно-аппаратным средствам защиты информации (далее – СЗИ) на технических средствах пользователей. Он несет ответственность за реализацию принятой политики безопасности.
  4. На Администратора ИБ возлагаются обязанности по администрированию ИСПДн Администрации.

1. Должностные обязанности
   1. Администратор ИБ обязан:
      1. Осуществлять учет и периодический контроль за составом и полномочиями пользователей ИС Администрации.
      2. Осуществлять оперативный контроль за работой пользователей ИС Администрации, анализировать содержимое системных журналов средств вычислительной техники (далее – СВТ) и адекватно реагировать на возникающие нештатные ситуации. Обеспечивать своевременное архивирование системных журналов СВТ и надлежащий режим хранения данных архивов.
      3. Осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых в ИС Администрации СЗИ.
      4. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных СВТ, обеспечивать и контролировать установку и настройку СЗИ.
      5. Не реже одного раза в месяц проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки (выборочное тестирование).
      6. Управлять учётными записями пользователей, реализовывать правила разграничения доступа, а также осуществлять контроль соблюдения этих правил в информационных системах Администрации.
      7. Управлять идентификаторами (осуществлять создание, присвоение и уничтожение идентификаторов пользователей и устройств) и средствами аутентификации (аутентификационной информацией) внутренних пользователей в ИС Администрации, обеспечивать соблюдение правил идентификации и аутентификации пользователей и устройств в соответствии с Правилами идентификации и аутентификации субъектов доступа и объектов доступа в информационных системах.
      8. Осуществлять контроль за хранением, выдачей, инициализацией, блокированием средств аутентификации и принятием мер в случае утраты и (или) компрометации средств аутентификации в соответствии с Правилами идентификации и аутентификации субъектов доступа и объектов доступа в информационных системах.
      9. Осуществлять контроль не реже одного раза в три месяца установленного (инсталлированного) в ИС Администрации программного обеспечения в соответствии с Правилами по ограничению программной среды в информационных системах.
      10. Настраивать параметры журналов регистрации событий безопасности в соответствии с Правилами регистрации событий безопасности в ИС.
      11. Проводить мониторинг и анализ результатов регистрации событий безопасности и реагирование на них не реже одного раза в неделю.
      12. Управлять средствами антивирусной защиты в соответствии с Инструкцией по антивирусной защите в информационных системах.
      13. Осуществлять контроль уровня защищенности информации, обрабатываемой в ИС Администрации.
      14. Осуществлять контроль выполнения условий и сроков действия сертификатов соответствия на СЗИ и принятие мер, направленных на устранение выявленных недостатков.
      15. Обеспечивать сохранность СЗИ, эксплуатационной и технической документации к СЗИ, а также порядок обращения с СЗИ в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты информации, обрабатываемой с использованием средств автоматизации в соответствии с Инструкцией по порядку обращения с сертифицированными средствами криптографической защиты информации, предназначенными для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах администрации Трубчевского муниципального района, и криптоключами к ним.
      16. Проводить не реже одного раза в 6 месяцев контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в соответствии с Инструкцией по организации парольной защиты в Администрации.
      17. Своевременно и точно отражать изменения в организационно-распорядительных документах по управлению СЗИ, установленных на СВТ ИС Администрации.
      18. Осуществлять поэкземплярный учет в соответствующем журнале:

* СЗИ (носителей дистрибутивов, системных блоков с установленными СЗИ);
* эксплуатационной и технической документации к СЗИ.
  + 1. Осуществлять хранение:
* носителей дистрибутивов СЗИ;
* лицензий и сертификатов на СЗИ.
  + 1. Не реже одного раза в месяц осуществлять проверки:
* состояния защищенности информационных ресурсов от сбоев в системе электропитания (система резервирования и автоматического ввода резерва);
* состояния линейно-кабельного оборудования локально-вычислительных сетей (наличие запирающих и опечатывающих устройств, оборудования распределительных шкафов).
  + 1. Проводить первоначальный, плановый и внеплановый инструктаж обслуживающего и эксплуатирующего персонала ИС Администрации по вопросам работы с СЗИ.
    2. Отвечать на вопросы обслуживающего и эксплуатирующего персонала ИС Администрации, связанные с работой СЗИ.
    3. Составлять инструкции по работе с СЗИ.
    4. Докладывать руководству Администрации об имевших место попытках несанкционированного доступа к информации и техническим средствам ИС.
    5. Участвовать в выявлении инцидентов информационной безопасности и реагировании на них.

В ходе выявления инцидентов и реагирования на них осуществляются:

* обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
* анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;
* планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИС Администрации в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
* планирование и принятие мер по предотвращению повторного возникновения инцидентов.
  + 1. Управлять системой защиты информации ИС Администрации.

В ходе управления системой защиты информации ИС Администрации осуществляются:

* поддержание системы защиты информации (структуры системы защиты информации ИС Администрации, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты;
* управление изменениями системы защиты информации, в том числе определение типов возможных изменений системы защиты информации, санкционирование внесения изменений в системы защиты информации, документирование действий по внесению изменений в системы защиты информации, сохранение данных об изменениях системы защиты информации, контроль действий по внесению изменений в системы защиты информации;
* анализ потенциального воздействия планируемых изменений в системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИС Администрации;
* определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИС Администрации и их системы защиты информации;
* внесение информации (данных) об изменениях в базовой конфигурации ИС Администрации и их системы защиты информации в эксплуатационную документацию на систему защиты информации ИС Администрации.
  + 1. В случае возникновения нештатных ситуаций и аварийных ситуаций принимать меры по реагированию в пределах функций и полномочий с целью ликвидации последствий. Оперативно докладывать вышестоящему руководству о случаях возникновения внештатных ситуаций и аварийных ситуаций. В кратчайшие сроки принимать меры по восстановлению работоспособности элементов ИС Администрации. Предпринимаемые меры по возможности согласовывать с вышестоящим руководством.

1. Права
   1. Администратор ИБ имеет право:
      1. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИС Администрации.
      2. Непосредственно обращаться к пользователям АРМ с требованием прекращения работы в ИС Администрации при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.
      3. В пределах своей компетенции сообщать своему непосредственному руководителю обо всех недостатках в работе ИС Администрации и их системы защиты.
      4. Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей.
      5. Подписывать и визировать документы в пределах своих обязанностей в соответствии с настоящей Инструкцией.
      6. Получать доступ к информации, материалам, техническим средствам, помещениям, необходимый для надлежащего исполнения своих прав и обязанностей (в т.ч. вести мониторинг действий пользователей и обслуживающего персонала ИС Администрации).
      7. Вносить свои предложения по совершенствованию мер защиты информации в ИС Администрации.
2. Ответственность
   1. Администратор ИБ ИС Администрации несет ответственность:
      1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, – в пределах, определенных действующим трудовым законодательством Российской Федерации.
      2. За правонарушения, совершенные в процессе осуществления своей деятельности, – в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.
      3. За причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

Приложение 4

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 472-р

**ИНСТРУКЦИЯ № 4-ИБ**

ответственного за эксплуатацию информационной системы персональных данных в администрации Трубчевского муниципального района

1. Общие положения

1.1. Ответственный за эксплуатацию информационной системы персональных данных (далее – ИСПДн) в администрации Трубчевского муниципального района (далее – Администрация) назначается распоряжением Администрации.

1.2. Методическое руководство работой ответственного за эксплуатацию ИСПДн осуществляется ответственным за организацию обработки персональных данных в Администрации.

1.3. Ответственный за эксплуатацию в своей работе руководствуется положениями, руководящими и нормативными документами ФСТЭК и ФСБ России по защите информации и организационно-распорядительными документами для данной ИСПДн, а также иными нормативными документами в части защиты информации.

1.4. Ответственный за эксплуатацию ИСПДн несет ответственность за свои действия, и действия сотрудников вверенного структурного подразделения в соответствии с действующим законодательством РФ.

2. Функции ответственного за эксплуатацию ИСПДн

* 1. Осуществление контроля за целевым использованием ИСПДн, всех периферийных устройств и технических средств, входящих в состав ИСПДн.
  2. Контроль за отсутствием в период обработки защищаемой информации в помещении, где осуществляется обработка, посторонних лиц, не допущенных к обрабатываемой информации.
  3. Контроль использования сотрудниками структурных подразделений, эксплуатирующими ИСПДн, средств защиты информации, установленных на АРМ, входящих в состав ИСПДн.
  4. Контроль за правильностью использования и хранения сотрудниками структурных подразделений, эксплуатирующими ИСПДн, машинных носителей информации и документов, содержащих персональные данные.
  5. Представление заявок на пользователей, допускаемых к защищаемым ресурсам ИСПДн, с целью закрепления за ними носителей информации устройств блокировки, паролей и других средств разграничения доступа к информации, а также прав пользования средствами вычислительной техники.
  6. Организация повышения уровня осведомленности подчиненных должностных лиц по вопросам информационной безопасности.

3. Обязанности ответственного за эксплуатацию ИСПДн

* 1. Четко знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководств по защите информации и распоряжений, регламентирующих порядок действий по защите информации.
  2. Обеспечивать функционирование ИСПДн в пределах возложенных на него функций.
  3. Обеспечивать контроль выполнения установленного комплекса мероприятий по обеспечению безопасности ПДн.
  4. Контролировать целостность печатей (пломб) на устройствах ИСПДн.
  5. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств ИСПДн и отправке их в ремонт.
  6. Присутствовать при выполнении технического обслуживания ИСПДн при установке (модификации) программного обеспечения.
  7. Информировать администратора информационной безопасности о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.
  8. Контролировать соответствие состава ИСПДн техническому паспорту на ИСПДн.

Приложение 5

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 472-р

**ИНСТРУКЦИЯ № 5-ИБ**

по выполнению режимных мер и допуску

к информационной системе персональных данных администрации Трубчевского муниципального района

Обозначения и сокращения

Администрация – Администрация Трубчевского муниципального района;

АРМ               – автоматизированное рабочее место;

ИС                  – информационная система персональных данных;

ОТСС             – основные технические средства и системы;

ПДн                – персональные данные;

ПЭВМ           – персональная электронно-вычислительная машина;

СВТ                – средства вычислительной техники;

СЗИ                – средства защиты информации;

СЗПДн           – система (подсистема) защиты персональных данных;

УБПДн           – угрозы безопасности персональных данным.

1. Общие положения

1.1. Инструкция по выполнению режимных мер и допуску к ИС (далее - Инструкция) предназначена для руководящего состава Администрации, руководителей структурных подразделений Администрации, и регулирует порядок допуска пользователей к работе в ИС.

1.2. Правила, устанавливаемые положениями Инструкции обязательны для исполнения.

2. Порядок допуска к ИС и в помещения размещения ОТСС

2.1. Приведённый в инструкции порядок направлен на достижение следующих задач:

- допуск к информации, обрабатываемой в ИС строго определённого перечня лиц;

-  самостоятельный допуск в помещения с установленными в них ОТСС ИС строго определённого перечня лиц;

- закрепление за каждым пользователем определённого ему для работы АРМ ИС и определённых ему информационных ресурсов в ИС.

2.2. Для выполнения задач, обозначенных в п. 2.1 Инструкции, создаются следующие распорядительные инструменты:

-  Перечень лиц, имеющих право доступа к обработке персональных данных, содержащихся в информационной системе персональных данных. Содержит перечень лиц (ФИО, должность), имеющих право допуска к АРМ ИС. Разрабатывается и актуализируется администратором информационной безопасности в порядке, описанном данной инструкцией. Копия списка вывешивается в каждом помещении размещения ОТСС ИС в целях исключения допуска к работе с АРМ не закреплённых за ними пользователей;

- Перечень лиц, имеющих право самостоятельного (неконтролируемого) пребывания в помещениях размещения ОТСС информационной системы персональных. Содержит сведения о помещениях и перечень лиц (ФИО, должность), имеющих право самостоятельного доступа в помещение, снятия помещения с охраны и получения ключей от него. Готовится и поддерживается в актуальном состоянии администратором информационной безопасности.

Все указанные документы утверждаются ответственным за организацию обработки персональных данных в Администрации.

2.3. Для работы в ИС каждый пользователь должен получить соответствующий допуск. Под допуском к ИС понимается возможность самостоятельного доступа пользователя к средствам информатизации ИС. Право допуска предоставляется пользователю только после включения его в «Перечень лиц, имеющих право доступа к обработке персональных данных, содержащихся в информационной системе персональных данных.

Устные указания кого бы то ни было об установлении права доступа пользователю к ИС либо об изменении его прав доступа не имеют юридической силы и необязательны для исполнения. Сотрудники Администрации и администратор информационной безопасности не могут быть наказаны за невыполнение подобного указания от вышестоящего руководителя.

Процедура получения (лишения прав) соответствующего права допуска пользователя для сотрудника Администрации инициируется заявкой руководителя структурного подразделения, в котором числится сотрудник в адрес ответственного за организацию обработки персональных данных в Администрации. (Приложение 1), только после назначения сотрудника на должность распоряжением Администрации, и подписания новым сотрудником обязательства о неразглашении персональных данных (Приложение 2). Подписание и хранение обязательства о неразглашении персональных данных в личном деле организовывается сотрудниками кадровой службы Администрации.

Ответственный за организацию обработки персональных данных в Администрации передает заявку администратору информационной безопасности.

Администратор информационной безопасности:

-  Вносит соответствующие изменения в «Перечень лиц, имеющих право доступа к обработке персональных данных, содержащихся в информационной системе персональных данных» и «Разрешительную систему доступа персонала к сведениям конфиденциального характера в информационной системе персональных данных».

- Обновлённый «Перечень лиц, имеющих право доступа к обработке персональных данных, содержащихся в информационной системе персональных данных» и «Разрешительная система доступа персонала к сведениям конфиденциального характера в информационной системе персональных данных» представляется на утверждение ответственному за организацию обработки персональных данных в Администрации.

- После утверждения указанных документов администратор информационной безопасности обеспечивает:

1) Регистрацию (удаление) персонального имени (учетная запись пользователя) и пароля, под которым пользователь регистрируется и работает в системе в соответствии с Инструкцией по организации парольной защиты в информационной системе персональных данных;

2) Внесение необходимых изменений администратором сети, серверов, баз данных в списки пользователей соответствующих подсистем и СУБД;

3) Настройку средств защиты и программного обеспечения АРМ пользователя, соответствующим категориям защиты.

Заявки хранятся у администратора информационной безопасности.

- Обновлённый «Перечень лиц, имеющих право доступа к обработке персональных данных, содержащихся в информационной системе персональных данных» рассылается администратором информационной безопасности заинтересованным сотрудникам Администрации.

- Руководитель структурного подразделения Администрации, в котором числится пользователь, контролирует внесение изменений в должностные инструкции пользователя и допускает сотрудника к работе в ИС. Ответственным за организацию обработки персональных данных в Администрации утверждаются необходимые изменения в Перечень лиц, имеющих право самостоятельного (неконтролируемого) пребывания в помещениях размещения ОТСС информационной системы персональных данных.

- При исключении пользователя ИС из Перечня лиц, имеющих право доступа к обработке персональных данных, содержащихся в информационной системе персональных данных руководителю структурного подразделения Администрации, в котором числится пользователь, необходимо направлять заявку в адрес ответственного за организацию обработки персональных данных в Администрации до момента объявления пользователю о лишении его прав на допуск к ИС. Обязательным является заведомое уведомление ответственным за организацию обработки персональных данных в Администрации о планируемом лишении прав доступа или изменения полномочий сотрудника по доступу к ресурсам ИС администратора информационной безопасности. Администратором информационной безопасности принимаются меры по исключению возможности нарушения данным лицом характеристик безопасности информации ИС.

2.4. По таким же правилам происходит включение (исключение) в Перечень лиц, имеющих право самостоятельного (неконтролируемого) пребывания в помещениях размещения ОТСС информационной системы персональных данных.

2.5. Действующими утверждёнными Перечнем лиц, имеющих право доступа к обработке персональных данных, содержащихся в информационной системе персональных данных и Перечень лиц, имеющих право самостоятельного (неконтролируемого) пребывания в помещениях размещения ОТСС информационной системы персональных данных в своей повседневной деятельности руководствуются руководители структурных подразделений Администрации, эксплуатирующих ИС, технические специалисты и администратор информационной безопасности. Перечни лиц находятся в рабочем кабинете администратора информационной безопасности, в целях использования сотрудниками Администрации в ежедневной деятельности и с целью контроля соблюдения установленных перечней допущенных лиц.

3. Требования по организации режимных мер

3.1. Состав ИС должен соответствовать техническому паспорту. Обработка не учтённых в техпаспорте технических средств запрещается. Все технические средства ИС должны размещаться в соответствии с техническим паспортом.

Изменение состава ОТСС в составе ИС допускается только после согласования с органом по аттестации. В адрес органа по аттестации направляется письменное уведомление о планируемых изменениях. Изменения осуществляются после получения рекомендаций органа по аттестации. Ответственным за данные мероприятия является ответственный за организацию обработки персональных данных в Администрации.

Полный порядок действий при модификации, обновлении программного обеспечения и других изменениях в ИС приведён в Инструкция по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств информационной системы персональных данных.

Контроль соблюдения данных требований и ведения учета средств информатизации ИС возлагается на администратора информационной безопасности.

3.2. Помещения, в которых размещаются средства информатизации ИС, должны исключать возможность бесконтрольного проникновения в них посторонних лиц. Помещения должны быть оборудованы пожарной сигнализацией, находящейся в работоспособном состоянии.

Пропуск в здание осуществляется на основании инструкции по обеспечению безопасности Администрации. Ключи от кабинетов хранятся у сотрудников, дубликаты хранятся на посту охраны, ведётся журнал выдачи ключей.

Уборка помещений должна осуществляться в присутствии сотрудников, имеющих право самостоятельного допуска в помещения.

Передача ключа посторонним лицам строго запрещена. Вскрытие помещений возможно только в присутствии лиц, имеющих право самостоятельного доступа в помещение в соответствии с утвержденным списком или в присутствии администратора информационной безопасности.

При обнаружении факта несанкционированного проникновения в помещения лиц, не входящих в Перечень лиц, имеющих право самостоятельного (неконтролируемого) пребывания в помещениях размещения ОТСС информационной системы персональных данных, администратор информационной безопасности или другие лица (в зависимости от обнаружившего данный факт) обязаны немедленно сообщить о происшедшем главе Администрации.

По данному происшествию проводится служебная проверка с установлением последствий проникновения для безопасности информации (нарушение целостности, доступности и конфиденциальности), обрабатываемой в ИС.

При утере ключа от помещения сотрудники, имеющие право допуска в помещение, обязаны сообщить о случившемся администратору информационной безопасности. Руководством принимаются меры по исключению возможности хищения носителей информации и ОТСС ИС (замена замков или другие меры).

3.3. Технические средства АРМ в помещении размещаются таким образом, чтобы исключить возможность просмотра экрана видеомонитора и распечаток принтера лицами, не имеющими отношения к обрабатываемой информации. Не допускается перемещение АРМ в другие помещения.

3.4. Ключи от сейфа, используемого для хранения дистрибутивов (резервных копий) средств защиты информации и резервных копий ПДн, хранятся у руководителя аппарата администрации.

3.5. Техническое обслуживание и ремонт средств информатизации проводится в соответствии с «Инструкцией по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств информационной системы персональных данных».

1. Ответственность за нарушение режимных мер

Ответственность за обеспечение безопасности информации в ИС, своевременную разработку и осуществление необходимых мероприятий по обеспечению безопасности информации несёт администратор информационной безопасности. Контроль за обеспечением режима безопасности информации и требований настоящей Инструкции возлагается на ответственного за организацию обработки персональных данных.

За соблюдение непосредственно подчинёнными сотрудниками действующего законодательства в области защиты информации, Инструкции пользователю информационной системы персональных данных, Инструкции по проведению антивирусного контроля в информационной системе персональных данных, Инструкции по организации парольной защиты в информационной системе персональных данных, Инструкции по резервному копированию и восстановлению данных в информационной системе персональных данных, и других документов Администрации в части обеспечения безопасности информации отвечает ответственный за организацию обработки персональных данных. При методической поддержке администратора информационной безопасности они организуют изучение подчинёнными сотрудниками требований организационно – распорядительных документов Администрации при работе в ИС. Каждому сотруднику Администрации должна быть предоставлена возможность изучить свои обязанности и правила работы в ИС.

Факт нарушения требований настоящей Инструкции является чрезвычайным происшествием. По каждому случаю проводится служебная проверка.

Невыполнение требований настоящей Инструкции рассматривается как нарушение трудовой дисциплины и влечет за собой наложение дисциплинарного взыскания.

Настоящая Инструкция доводится до заинтересованных сотрудников Администрации под роспись.

Приложение 1

к Инструкции по выполнению режимных мер и допуску

к информационной системе персональных данных

администрации Трубчевского муниципального района

Заместителю главы администрации

Трубчевского муниципального района

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ЗАЯВКА

на внесение изменений в списки пользователей

информационной системы персональных данных администрации Трубчевского муниципального района «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_»

и наделение пользователей полномочиями доступа к ресурсам системы

Прошу зарегистрировать пользователем (исключить из списка пользователей, изменить полномочия пользователя) в

*(ненужное зачеркнуть)*

ИС «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(должность с указанием подразделения)* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *(фамилия имя и отчество сотрудника)*

предоставив ему полномочия, необходимые (лишив его полномочий, необходимых)

*(ненужное зачеркнуть)*

для решения задач: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(список задач согласно формуляров задач)*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_на следующих рабочих местах (АРМ): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(номер помещения, зав.или инвент.номера АРМ)*

Обязательство о неразглашении персональных данных, обрабатываемых в ИС, мною подписано и хранится в кадровой службе администрации Трубчевского муниципального района.

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                                            \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

            (подпись)                      (ФИО)

Приложение 2

к Инструкции по выполнению режимных мер и допуску

к информационной системе персональных данных

администрации Трубчевского муниципального района

Обязательство

о неразглашении информации, обрабатываемой в информационной системе персональных данных администрации Трубчевского муниципального района «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_»

Я,\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(*фамилия, имя, отчество, должность)*

Администрации Трубчевского муниципального района, далее по тексту – Администрация, в период трудовых (служебных) отношений с Администрацией и в течение 5 лет после их окончания обязуюсь:

1. не разглашать сведения конфиденциального характера, содержащие персональные данные, которые станут мне известны при выполнении служебных (трудовых) обязанностей или иным путем;

2. не передавать третьим лицам и не раскрывать публично сведения конфиденциального характера, содержащие персональные данные, без согласия субъектов персональных данных;

3. выполнять относящиеся ко мне требования приказов, инструкций и положений по обеспечению безопасности персональных данных, обрабатываемых в Администрации;

4. в случае попытки посторонних лиц получить от меня персональные данные, обрабатываемые в Администрации немедленно сообщить об этом непосредственному руководителю и ответственному за организацию обработки персональных данных в Администрации;

5. в случае моего увольнения, все носители персональных данных, которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей во время работы в Администрации, сдать лицу, ответственному за учет и хранение;

6. об утрате или недостаче носителей персональных данных, а также о причинах и условиях возможной утечки персональных данных немедленно сообщить непосредственному руководителю и ответственному за организацию обработки персональных данных в Администрации.

Я предупрежден(а), что разглашение персональных данных, обрабатываемых в Департаменте, утрата носителей персональных данных, передача третьим лицам, публикация без согласия субъекта персональных данных, а также использование для занятия любой деятельностью, которая может нанести ущерб субъекту персональных данных, влечет уголовную, административную, гражданско-правовую или иную ответственность в соответствии с действующим законодательством, в виде лишения свободы, денежного штрафа и других наказаний.

До моего сведения также доведены с разъяснениями соответствующие положения, инструкции, приказы по обеспечению безопасности персональных данных.

«\_\_\_»\_\_\_\_\_\_\_\_\_\_ 20\_\_\_г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

                                                                                     (ФИО)

Один экземпляр обязательств получил                                    \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

                                                                                                                 (подпись)

Приложение 6

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 472-р

**ИНСТРУКЦИЯ № 6-ИБ**

пользователю информационной системы персональных данных в части обеспечения безопасности персональных данных при их обработке в информационной системе в администрации Трубчевского муниципального района

Обозначения и сокращения

Администрация – администрация Трубчевского муниципального района;

АРМ – автоматизированное рабочее место;

ИС –информационная система персональных данных;

ИБ – информационная безопасность;

ЗИ – защита информации;

ОТСС – основные технические средства и системы;

ПДн – персональные данные;

ПЭВМ – персональная электронно-вычислительная машина;

СВТ – средства вычислительной техники;

СЗИ – средства защиты информации;

СЗПДн – система (подсистема) защиты персональных данных;

УБПДн – угрозы безопасности персональным данным;

НСД – не санкционированный доступ.

1. Общие положения

 1.1. Инструкция пользователя (далее Инструкция) ИС предназначена для пользователей всех уровней (руководителей и сотрудников) и регулирует порядок работы пользователей в ИС в Администрации, определяет общие обязанности, права и ответственность по обеспечению информационной безопасности при работе в ИС.

1.2. Пользователем ИС (далее Пользователь) является сотрудник Администрации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИС, в соответствии с перечнем лиц, допущенных к ИС. Пользователь должен принимать все необходимые меры по защите информации и контролю за соблюдением прав доступа к ней.

1.3. Положения Инструкции обязательны для исполнения всеми пользователями.

1.4.Все пользователи должны быть ознакомлены под роспись с Инструкцией и предупреждены об ответственности за её нарушение.

1.5.По уровню ответственности и правам доступа к ИС пользователи разделяются на следующие категории: администратор информационной безопасности и пользователи.

2.Основные положения Инструкции

 2.1.При первичном допуске к работе в ИС Пользователь изучает требования настоящей инструкции, разрешительную систему доступа к ИС, и руководящие, нормативно-методические и организационно-распорядительные документы по вопросам обеспечения безопасности информации.

2.2.Каждый пользователь ИС, имеющий в рамках своих обязанностей доступ к аппаратным средствам, программному обеспечению и данным ИС, несет персональную ответственность за свои действия и обязан:

* строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС, в том числе положения настоящей Инструкции;
* знать и строго выполнять правила работы со средствами защиты информации, установленными на его рабочей станции;
* располагать ОТСС в соответствии с техническим паспортом;
* хранить в тайне свой пароль (пароли). Парольную защиту организовывать в соответствии с Инструкцией по организации парольной защиты;
* выполнять требования Инструкции по проведению антивирусной защиты;
* немедленно вызывать администратора информационной безопасности и ставить в известность руководителя подразделения при подозрении компрометации личных ключей и паролей или при обнаружении фактов совершения в его отсутствие попыток НСД к ОТСС ИС;
* в случае появления у пользователя сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах или попытках несанкционированного удаленного доступа к информации, размещенной на контролируемом в ИС компьютере, пользователь должен немедленно сообщить об этом администратору информационной безопасности;
* немедленно сообщать администратору информационной безопасности об обнаруженных фактах нарушения настоящей Инструкции кем-либо;
* сообщать администратору информационной безопасности об отклонениях в нормальной работе установленных на АРМ средств защиты информации;
* при работе в ИС выполнять только служебные задания;
* при отсутствии необходимости работы выключить компьютер;
* при работе в ИС использовать только учтенные съемные носители, при обоснованной необходимости использования неучтённых носителей согласовывать использование с администратором информационной безопасности. После того как цель переноса информации на носители достигнута (переданы третьим лицам и т.п.) информация незамедлительно удаляется с носителей;
* осуществлять установленным порядком уничтожение информации (сочетанием клавиш Shift+Del), содержащей сведения конфиденциального характера, с машинных (съемных) носителей информации;
* немедленно выполнять предписания администратора информационной безопасности в части обеспечения безопасности информации;
* экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на нем информацией посторонними лицами;
* соблюдать установленный режим разграничения доступа к информационным ресурсам;
* не разглашать известную им информацию, составляющую ПДн лицам, не имеющим допуска к этой информации;
* все изменения конфигурации технических и программных средств ИС, ремонт, модификация и техническое обслуживание технических средств и систем, входящих в состав ИС, производить только на основании инструкции по модернизации, ремонту, техобслуживанию.

2.3. Пользователю запрещается:

* + самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств, устанавливать или удалять установленные техническим специалистом (администратором информационной безопасности) сетевые программы на компьютерах, вскрывать компьютеры, сетевое и периферийное оборудование, подключать к компьютеру дополнительное оборудование, вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и  аппаратные средства без согласования с администратором информационной безопасности;
* привлекать посторонних лиц для производства ремонта ОТСС без письменной заявки и согласования с администратором информационной безопасности;
* запускать любые системные или прикладные программы, не входящие в состав программного обеспечения;
* работать с неучтенными машинными (съемными) носителями информации;
* отключать (блокировать) средства защиты информации;
* производить какие-либо изменения в размещении технических средств;
* обрабатывать на СВТ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам;
* сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам АРМ;
* хранить на учтенных носителях программы и данные, не относящиеся к рабочей информации;
* выполнять работы с документами ограниченного распространения на дому, выносить их за пределы контролируемой зоны;
* передавать свои учтённые носители кому-либо;
* вводить в ОТСС персональные данные под диктовку или с микрофона;
* осуществлять попытки несанкционированного доступа к ресурсам ИС, проводить или участвовать в сетевых атаках и сетевом взломе;
* производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и серверов;
* закрывать доступ к информации паролями без согласования с администратором информационной безопасности;
* оставлять без личного присмотра на рабочем месте или где бы то ни было персональное устройство идентификации, машинные (съемные) носители и распечатки, содержащие защищаемую информацию.

2.4.Пользователь обязан обеспечить:

* блокирование своей учетной записи в случае кратковременного оставления АРМ(нажатием клавиш Windows+L);
* обязательное выключение компьютера после завершения работы.

2.5.Права пользователя:

* участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИС, если данное нарушение произошло под его идентификационными данными;
* своевременно получать доступ к информационным ресурсам ИС, необходимым ему для выполнения своих должностных обязанностей;
* требовать от администратора информационной безопасности смены идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

2.6.Ответственность:

2.6.1.Пользователь несет персональную ответственность за соблюдение установленных требований во время работы. Пользователи, виновные в нарушении законодательства Российской Федерации о защите прав собственности и охраняемых по Закону сведений, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством и организационно распорядительными документами;

2.6.2.Пользователь компьютера отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной техники;

2.6.3.Нарушение данной инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации, нарушение работы компьютеров пользователей или ИС в целом, может повлечь ответственность в соответствии с действующим законодательством.

Приложение 7

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 472-р

**ИНСТРУКЦИЯ № 7-ИБ**

по организации парольной защиты в информационных системах персональных данных администрации Трубчевского муниципального района

Обозначения и сокращения

Администрация – администрация Трубчевского муниципального района;

АРМ – автоматизированное рабочее место;

ИС –информационная система персональных данных;

ПДн – персональные данные.

Данная инструкция регламентирует организационно-техническое обеспечение процессов смены и прекращения действия паролей в ИС.

1.         Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на администратора информационной безопасности.

2.         Настройки средств защиты информации должны препятствовать повторному использованию старого пароля после процедуры его смены (допускается изменение как минимум хотя бы 1 символа).

3.         Личный пароль должен генерироваться и распределяться централизованно либо выбираться пользователем ИС самостоятельно с учетом следующих требований:

* длина пароля должна быть не менее 6 символов;
* в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, \*, % и т.п.);
* пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
* личный пароль пользователь не имеет права сообщать никому.

Настройки средств защиты должны препятствовать заданию пароля, не удовлетворяющего данным требованиям.

4. Администратор информационной безопасности имеет доступ к АРМ ИС только под своей учётной записью и своим паролем.

5. Плановая смена паролей пользователя должна проводиться регулярно, не реже одного раза в 3 месяца, контроль за процедурой смены паролей возлагается на администратора информационной безопасности. В случае необходимости смена паролей проводится по решению администратора.

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

7. Пользователь имеет право в любой момент изменить свой личный пароль, либо потребовать смены своего пароля у администратора информационной безопасности.

8. В случае компрометации личного пароля пользователя ИС должны быть немедленно предприняты меры в соответствии с п.5 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

9. Контроль, за действиями пользователей системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора информационной безопасности.

Приложение 8

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 472-р

**ИНСТРУКЦИЯ № 8-ИБ**  
по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, защищаемой информации и средств защиты в администрации Трубчевского муниципального района

1. Общие положения

Настоящая инструкция разработана с целью обеспечения возможности оперативного восстановления 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 (далее – ИСПДн) в администрации Трубчевского муниципального района (далее – Администрация).

1. Резервируемое программное обеспечение и базы персональных данных

В ИСПДн резервированию подлежит:

* Общее программное обеспечение (операционная система и программные драйверы устройств (принтера, монитора, видеокарты и т.п.), поставляемые с компонентами автоматизированных рабочих мест (далее – АРМ), входящими в состав ИСПДн);
* Прикладное программное обеспечение, используемое для обработки персональных данных (средства обработки текстов и таблиц, специализированные программы и т.п.);
* Базы персональных данных (тестовые и табличные файлы, а также файлы баз данных специализированных программ);
* Программное обеспечение средств защиты информации, в том числе средств антивирусной защиты.

1. Порядок резервирования и хранения резервных копий

Резервирование общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации обеспечивается путем хранения у администратора информационной безопасности в ИСПДн машинных носителей информации, содержащих дистрибутивы данного программного обеспечения.

Машинные носители информации обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации должны также храниться у администратора информационной безопасности в ИСПДн.

Допускается хранение машинных носителей прикладного программного обеспечения и машинных носителей с обновлениями к нему в структурных подразделениях, эксплуатирующих ИСПДн.

Резервирование баз персональных данных, а также текстовых и табличных файлов, содержащих персональные данные, допускается только на учтенные установленным порядком машинные носители информации.

Резервирование осуществляется ежемесячно.

Резервные носители персональных данных хранятся в структурных подразделениях, эксплуатирующих ИСПДн, в порядке, предусмотренном для носителей информации персональных данных.

К резервному носителю персональных данных должна быть приложена учетная карточка, в которой делаются отметки о дате резервирования.

Резервные носители персональных данных не могут быть переданы за пределы структурных подразделений, эксплуатирующих ИСПДн.

Копирование информации с резервных носителей персональных данных, за исключением случая восстановления работоспособности ИСПДн, запрещается.

1. Порядок восстановления работоспособности ИСПДн

Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также   
ее программного обеспечения.

Данные работы осуществляются администратором информационной безопасности в ИСПДн в соответствии с эксплуатационной документацией   
на программное обеспечение до полного восстановления работоспособности.

В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с персональными данными. Ответственность за выполнение данного требования возлагается на администратора информационной безопасности в ИСПДн и ответственного за эксплуатацию соответствующей ИСПДн.

|  |  |  |  |
| --- | --- | --- | --- |
| Учетная карточка резервного носителя персональных данных № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |
| Дата  резервного копирования | Объект  копирования | Кто производил копирование | Подпись |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Приложение 9

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 472-р

**ИНСТРУКЦИЯ № 9-ИБ**  
по антивирусной защите в администрации Трубчевского муниципального района

1. Общие требования

Настоящая инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных (далее – ИСПДн) администрации Трубчевского муниципального района (далее – Администрация) от разрушающего воздействия вирусов и вредоносных программ и устанавливает ответственность руководителя и работников структурных подразделений, эксплуатирующих и сопровождающих ИСПДн, за их выполнение. Инструкция распространяется на все существующие и вновь разрабатываемые ИСПДн. Для отдельных ИСПДн могут быть разработаны свои инструкции, учитывающие особенности работы.

К использованию в ИСПДн допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

Установка и настройка средств антивирусного контроля осуществляется администратором информационной безопасности в ИСПДн или специально назначенным лицом в соответствии с эксплуатационной документацией на антивирусные средства.

1. Применение средств антивирусного контроля

При загрузке АРМ в автоматическом режиме должен проводиться антивирусный контроль служб операционной системы, исполняемых приложений, находящихся в автозагрузке, реестра операционной системы.

Полному антивирусному контролю автоматизированные рабочие места (АРМ) должны подвергаться не реже одного раза в неделю.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, оптических и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов и других вредоносных программ. Непосредственно после установки (изменения) программного обеспечения, администратором информационной безопасности в ИСПДн должна быть выполнена антивирусная проверка на защищаемых серверах и пользовательских АРМ.

При возникновении подозрения на наличие вируса либо вредоносной программы (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник структурного подразделения самостоятельно или вместе с администратором информационной безопасности в ИСПДн должен провести внеочередной антивирусный контроль своего АРМ.

В случае обнаружения при проведении антивирусной проверки зараженных вирусами либо вредоносными программами файлов, необходимо:

* Приостановить работу в ИСПДн;
* Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя структурного подразделения и администратора информационной безопасности в ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
* Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
* Провести лечение или уничтожение зараженных файлов.

1. Ответственность

Ответственность за проведение мероприятий антивирусного контроля в подразделениях и соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности в ИСПДн и всех работников, являющихся пользователями ИСПДн.

Приложение 10

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 472-р

**ИНСТРУКЦИЯ № 10-ИБ**по ведению журналов в администрации Трубчевского муниципального района

1. Общие положения

1.1. Настоящая Инструкция определяет порядок ведения журналов администрацией Трубчевского муниципального района (далее – оператор, Администрация), а также лицами, ответственными за правильность и полноту ведения журналов.

1.2. Оператору для выполнения требований законодательства в области обеспечения безопасности персональных данных необходимо предусмотреть ведение следующих журналов:

периодического тестирования средств защиты информации;

учета лиц, допущенных к работе с персональными данными в инфор­мационной системе;

учета мероприятий по контролю обеспечения защиты персональных данных;

учета машинных носителей информации;

учета обращений субъектов персональных данных о реализации их законных прав при обработке данных в информационной системе;

учета применяемых средств защиты информации, эксплуатационной и технической документации к ним;

учета средств криптографической защиты информации.

1.3. Все журналы должны быть утверждены руководством оператора.

2. Ведение журнала периодического тестирования средств защиты информации

2.1. Ответственный за администрирование средств защиты информа­ции (администратор безопасности) должен осуществлять периодическое тестирование средств защиты информации (далее - СЗИ) не реже одного раза в месяц с отметкой в журнале периодического тестирования средств защиты информации. Журнал должен храниться у ответственного за администри­рование средств защиты информации, ответственного пользователя средств криптографической защиты информации (администратора безопасности).

2.2. В журнале указываются следующие сведения: наименование тестируемого СЗИ, регистрационный номер СЗИ (в соответствии с журналом учета применяемых средств защиты информации, эксплуатационной и технической документации к ним или журналом учета средств криптографической защиты информации), дата проведения, исполнитель (тестирование может проводиться сотрудниками оператора самостоятельно или с привлечением сторонних организаций) и конечный результат (успешное/неуспешное тестирование, при необходимости - примечание).

2.3. Контроль за правильностью и полнотой ведения журнала, а также за своевременностью устранения выявленных недостатков осуществляется ответственным за организацию обработки ПДн.

3. Ведение журнала учета лиц, допущенных к работе с персональными

данными в информационной системе

3.1. Учет лиц, допущенных к работе с персональными данными в информационной системе оператора, ведется в журнале учета лиц, допущенных к работе с персональными данными в информационной системе.

3.2. Журнал ведется ответственным за администрирование информа­ционных систем персональных данных.

3.3. Основанием для допуска сотрудника к персональным данным является перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных обязанностей, утвержденный руководством оператора.

3.4. Основанием для прекращения допуска сотрудника к персональным данным является распоряжение об увольнении сотрудника или переводе на работу, не связанную с необходимостью доступа к персональным данным.

3.5. Контроль за правильностью и полнотой ведения журнала осуществляется ответственным за организацию обработки ПДн.

4. Ведение журнала учета мероприятий по контролю обеспечения защиты персональных данных

4.1. Журнал учета мероприятий по контролю обеспечения защиты персональных данных содержит перечень периодически проводимых мероприятий.

4.2. Ведение журнала осуществляется ответственным за администри­рование средств защиты информации (администратором безопасности).

4.3. Ответственный сотрудник ведет журнал, вносит в него подробную информацию, связанную с изменением режима защиты персональных данных, а также информацию о результатах внутренних проверок выпол­нения режима защиты персональных данных.

4.4. В журнале указываются следующие сведения: название прове­денного мероприятия, дата проведения, исполнитель мероприятия (сотруд­ник оператора или привлекаемая организация) и результат (отчет, акт, действия, при необходимости -- примечание).

5. Ведение журнала учета машинных носителей информации

5.1. Носители информации, используемые для обработки и хранения персональных данных оператором, должны быть зарегистрированы в журнале учета машинных носителей информации.

5.2. Ведение журнала осуществляется ответственным за администри­рование средств защиты информации (администратором безопасности) совместно с ответственным за администрирование информационных систем персональных данных (далее - ответственные).

5.3. У каждого носителя должен быть уникальный номер, которым является его заводской номера соответствии с технической документацией, либо учетный номер, который может быть присвоен оператором.

5.4. В качестве «тип» указывается тип носителя (HDD, DVD-RW, CD-R, USB-флэш-накопитель и т.д.).

5.5. В журнале должны быть отражены все перемещения носителей в процессе работы оператора, передача во внешние по отношению к оператору организации, а также факт уничтожения носителей.

5.6. Отметка об уничтожении проставляется в графе «Примечание» с проставлением номера, даты акта уничтожения носителя и подписи ответственных.

6. Ведение журнала учета обращений субъектов персональных данных о реализации их законных прав при обработке данных в информационной системе

6.1. Журнал учета обращений субъектов персональных данных о реализации их законных прав при обработке данных в информационной системе.

6.2. Ведение журнала осуществляется ответственным за администри­рование информационных систем персональных данных. Другие сотрудники, участвующие в обработке запросов (в составлении ответов на запросы) могут вносить необходимые пометки в журнал под контролем ответственного.

6.3. В журнале указываются следующие сведения: Ф.И.О. субъекта ПДн, дата обращения, регистрационный номер запроса, присваиваемый в соответствии с требованиями делопроизводства оператора, цель обращения и результат.

Например, при получении запроса от субъекта в журнал заносятся информация о субъекте, суть и цель запроса (информирование, уточнение, блокирование, удаление ПДн и т.д.). После обработки запроса перед отправкой ответа в журнал (графа «Результат») заносится окончательная информация: был составлен ответ или отказ, правовое обоснование ответа или отказа, дата, собственноручная подпись лица, составлявшего ответ, и, при необходимости, примечание.

7. Ведение журнала учета применяемых средств защиты информации,

эксплуатационной и технической документации к ним

7.1. Используемые или хранимые оператором средства защиты информации, эксплуатационная и техническая документация к ним подлежат поэкземплярному учету в Журнале учета применяемых средств защиты информации, эксплуатационной и технической документации к ним.

7.2. Ведение журнала осуществляется ответственным за администри­рование средств защиты информации (администратором безопасности).

7.3. Все полученные экземпляры средств защиты информации, эксплуа­тационной и технической документации к ним должны быть выданы под расписку в журнале лицом, несущим персональную ответственность за их сохранность (раздел «Отметка о получении»). В графе «От кого получены» указывается наименование организации, отгрузившей средства защиты информации, а в графе «Дата и № сопроводительных документов» указывается номер закрывающих бухгалтерских документов на поставку средств защиты информации (акт или товарная накладная).

7.4. Все экземпляры средств защиты информации, эксплуатационной и технической документации к ним должны выдаваться пользователям, несущим персональную ответственность за их сохранность под роспись в Журнале (раздел «Отметка о выдаче»).

7.5. Программные средства учитываются совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование (графа «Х. аппаратных средств, в которые установлены или к которым подключены средства защиты»).

7.6. По решению Ответственного за администрирование средств защиты информации СЗИ могут изыматься из употребления. Отметка об изъятии проставляется в графе «Примечание» с проставлением номера, даты акта об изъятии и подписи ответственного.

8. Ведение журнала учета средств криптографической защиты информации, эксплуатационной и технической документации к ним

8.1. Используемые или хранимые Оператором средства криптографической защиты информации, эксплуатационная и техническая документация к ним подлежат поэкземплярному учету в Журнале учета средств криптографической защиты информации.

8.2.Ведение Журнала осуществляется ответственным за администрирование средств защиты информации (администратором безопасности).

8.3. Все полученные экземпляры средств криптографической защиты информации, эксплуатационной и технической документации к ним должны быть выданы под расписку в Журнале лицом, несущим персональную ответственность за их сохранность (раздел «Отметка о получении»). В графе «От кого получены» указывается наименование организации, отгрузившей средства криптографической защиты информации, а в графе «Дата и № сопроводительных документов» указывается номер закрывающих бухгалтер­ских документов на поставку средств криптографической защиты информа­ции (акт или товарная накладная).

8.4. Все экземпляры средств криптографической защиты, эксплуата­ционной и технической документации к ним должны выдаваться пользо­вателям, несущим персональную ответственность за их сохранность, под роспись в журнале (раздел «Отметка о выдаче»).

8.5. Программные средства учитываются совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование (графа <д аппаратных средств, в которые установлены или к которым подключены средства криптографической защиты»).

8.6. По решению ответственного за администрирование средств защиты информации СКЗИ могут изыматься из употребления. Отметка об изъятии проставляется в графе «Примечание» с проставлением номера, даты акта об изъятии и подписи ответственного.

Приложение 11

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 472-р

**ИНСТРУКЦИЯ № 11-ИБ**по проверке электронного журнала обращений к информационной системе персональных данных администрации Трубчевского муниципального района

1. Задачи проверки

Под проверкой понимается отслеживание событий, происходивших   
на автоматизированных рабочих местах (далее – АРМ) в течение определенного времени.

Общими задачами проверки являются:

* Контролирование состояния защищенности системы;
* Выявление причин произошедших изменений;
* Определение лиц или процессов, деятельность которых привела   
  к изменению состояния защищенности системы или к НСД;
* Установление времени изменений.

Проверку средств защиты осуществляет администратор информационной безопасности.

1. Журналы записей о событиях

События, происходящие на АРМ, входящем в состав ИСПДн, регистрируются в журналах.

Каждому событию соответствует отдельная запись в журнале, содержащая подробную информацию для анализа события.

В состав используемых в ИСПДн средств защиты информации может входить специальное программное средство для аудита журналов событий, предназначенное для загрузки и просмотра журналов (далее — программа просмотра журналов). В программу просмотра журналов могут быть загружены записи следующих журналов:

* Штатные журналы операционной системы Windows;
* Журналы событий средств защиты информации.

1. Штатные журналы операционной системы

В штатных журналах ОС Windows регистрируются только те события, которые имеют отношение к операционной системе. События используемых средств защиты информации в них не регистрируются.

Информация о событиях, происходящих на АРМ под управлением ОС Windows, сохраняется в следующих штатных журналах:

* Журнал приложений – содержит сведения об ошибках, предупреждениях и других событиях, возникающих при исполнении приложений;
* Системный журнал – содержит сведения об ошибках, предупреждениях и других событиях, возникающих в операционной системе;
* Журнал безопасности – хранит информацию о попытках регистрации, а также о событиях, связанных с использованием ресурсов.

Подробное описание содержимого штатных журналов ОС Windows отражено в документации к операционной системе.

Загрузка и просмотр записей штатных журналов может осуществляться как в программе просмотра журналов средств защиты, так и с помощью стандартных средств работы с журналами ОС Windows — в оснастке «Просмотр событий» («Eventviewer»).

1. Журнал событий средств защиты информации

Журналы средств защиты информации (далее – СЗИ) хранят информацию о событиях, отслеживаемых средствами самих СЗИ, в этом журнале регистрируются события, заданные параметрами СЗИ для локальной политики безопасности.

1. Аудит

Сведения, содержащиеся в журнале, позволяют отслеживать использование механизмов защиты, которые предоставляют средства защиты информации АРМ (шифрование файлов, полномочное управление, замкнутая программная среда и др.) подробное описание регистрируемых событий указано в соответствующих руководствах к используемым СЗИ.

1. Просмотр событий электронных журналов

Администратор информационной безопасности в ИСПДн производит проверку электронных журналов.

В случае обнаружения нарушений администратор информационной безопасности докладывает о данном факте ответственному за организацию обработки персональных данных.

Приложение 12

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 472-р

**ИНСТРУКЦИЯ № 12-ИБ**  
по порядку обращения с сертифицированными средствами криптографической защиты информации, предназначенными для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах администрации Трубчевского муниципального района, и криптоключами к ним

1. Общие положения

1.1 Инструкция по порядку обращения с сертифицированными средствами криптографической защиты информации (далее - СКЗИ), предназначенными для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее - Информация), обрабатываемой в информационных системах администрации Трубчевского муниципального района (далее - ИС Администрации), и криптоключами к ним регламентирует порядок обращения с криптосредствами в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты Информации.

1.2 Под криптосредством в настоящей Инструкции понимается шифровальное (криптографическое) средство, предназначенное для защиты информации.

1.3 К криптосредствам (шифровальным, криптографическим средствам) относятся:

1.3.1 Средства шифрования - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

1.3.2 Средства имитозащиты - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.

1.3.3 Средства электронной подписи - аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи.

1.3.4 Средства кодирования-средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.

1.3.5 Средства изготовления ключевых документов (независимо от вида носителя ключевой информации).

1.3.6 Ключевые документы (независимо от вида носителя ключевой информации).

1.4 В настоящей Инструкции используются следующие понятия и определения:

1.4.1 Доступ к информации- возможность получения информации и ее использования.

1.4.2 Закрытый ключ - криптоключ, который хранится пользователем системы в тайне.

1.4.3 Ключевой документ- физический носитель определенной структуры, содержащий криптоключи.

1.4.4 Компрометация криптоключа- утрата доверия к тому, что используемые криптоключи обеспечивают безопасность информации.

1.4.5 Контролируемая зона - пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

1.4.6 Криптографический ключ (криптоключ)- совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

1.4.7 Модель нарушителя - предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

1.4.8 Модель угроз - перечень возможных угроз.

1.4.9 Пользователь криптосредства- лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

1.4.10 Средство защиты информации- техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

1.5 Для обеспечения безопасности Информации при её обработке в ИС Администрации должны использоваться сертифицированные в системе сертификации ФСБ России криптосредства (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации).

1.6 Класс криптосредства определяется в соответствии с Приказом Федеральной службы безопасности Российской Федерации (ФСБ России) [от 10.07.2014 № 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»](https://docs.cntd.ru/document/420208484).

2. Организационная структура

Безопасность обработки Информации в ИС Администрации с использованием криптосредств организует и обеспечивает Ответственный за эксплуатацию СКЗИ в ИС Администрации.

3. Обязанности пользователей криптосредств

3.1 Пользователи криптосредств допускаются к работе с ними только после получения заключения о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации и ознакомления под роспись с настоящей Инструкцией, другими документами, регламентирующими организацию и обеспечение безопасности Информации при ее обработке в ИС Администрации.

3.2 При наличии двух и более пользователей криптосредств обязанности между ними должны быть распределены с учетом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

3.3 Пользователи криптосредств обязаны:

3.3.1 Не нарушать конфиденциальность закрытых ключей.

3.3.2 Не допускать снятие копий с ключевых документов, содержащих закрытые ключи.

3.3.3 Не допускать вывод закрытых ключей на дисплей (монитор) автоматизированного рабочего места (далее - АРМ) или принтер.

3.3.4 Не допускать записи на ключевой документ посторонней информации.

3.3.5 Не допускать установки ключевых документов на другие АРМ.

3.3.6 Обеспечить конфиденциальность информации о криптосредствах, других мерах защиты.

3.3.7 Точно соблюдать требования к обеспечению безопасности Информации, требования к обеспечению безопасности криптосредств и ключевых документов к ним.

3.3.8 Хранить ключевые документы к криптосредствам в защищаемых хранилищах.

3.3.9 Сдавать ключевые документы к криптосредствам при увольнении или отстранении от исполнения обязанностей.

3.3.10 Своевременно выявлять и сообщать Ответственному за эксплуатацию СКЗИ в Администрации о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним.

3.3.11 Немедленно уведомлять Ответственного за эксплуатацию СКЗИ в Администрации и принимать меры по предупреждению нарушения конфиденциальности Информации при утрате или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей, удостоверений, пропусков, при других фактах, которые могут привести к компрометации закрытых ключей, снижению уровня защищенности обрабатываемой Информации.

4. Учет ключевых документов

4.1 Ключевые документы подлежат поэкземплярному учету. Единицей поэкземплярного учета ключевых документов считается ключевой носитель информации.

4.2 Все экземпляры ключевых документов выдаются пользователям криптосредств под роспись в соответствующем журнале поэкземплярного учета.

4.3 Передача ключевых документов допускается только между пользователями криптосредств и Ответственным за эксплуатацию СКЗИ под роспись в соответствующем Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов. Аналогичная передача между пользователями криптосредств осуществляется с письменного разрешения Ответственного за эксплуатацию СКЗИ.

4.4 Для исключения компрометации ключевых документов на период отсутствия пользователя и в нерабочее время, ключевые документы убираются в защищенные хранилища (ящики, шкафы) индивидуального пользования, которые, в свою очередь, закрываются на ключ и опечатываются.

4.5 Учет эксплуатационной и технической документации к криптосредствам:

4.5.1 Эксплуатационная и техническая документация к криптосредствам подлежит поэкземплярному учету.

4.5.2 Все экземпляры эксплуатационной и технической документации к криптосредствам выдаются пользователям криптосредств под роспись.

4.5.3 Передача эксплуатационной и технической документации к криптосредствам допускается только между пользователями криптосредств и Ответственным пользователем за эксплуатацию СКЗИ под роспись. Аналогичная передача между пользователями криптосредств осуществляется с санкции Ответственного за эксплуатацию СКЗИ.

4.6 Плановая смена ключевых документов:

4.6.1 Заказ на изготовление очередных ключевых документов, их изготовление и получение пользователем производится заблаговременно для своевременной замены действующих ключевых документов.

4.7 Внеплановая смена ключевых документов:

4.7.1 Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи немедленно выводятся из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам.

4.8 Уничтожение ключевых документов:

4.8.1 Ключевые документы с неиспользованными или выведенными из действия криптоключами (исходной ключевой информацией) возвращаются Ответственному за эксплуатацию СКЗИ, или по его указанию уничтожаются на месте пользователями криптосредств.

4.8.2 Уничтожение ключевых документов производится путем стирания (разрушения) криптоключей без повреждения ключевого документа.

4.8.3 Бумажные и прочие сгораемые ключевые документы уничтожаются путем сжигания или с помощью любых бумагорезательных машин с составлением соответствующего акта.

4.8.4 Ключевые документы уничтожаются в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы уничтожаются не позднее 10 (десяти) суток после вывода их из действия (окончания срока действия).

4.8.5 Пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) ключевые документы. После уничтожения пользователи криптосредств уведомляют об этом Ответственного за эксплуатацию СКЗИ.

4.9 Уничтожение эксплуатационной и технической документации к криптосредствам:

4.9.1 Эксплуатационная и техническая документация к криптосредствам уничтожается путем сжигания или с помощью любых бумагорезательных машин с составлением соответствующего акта.

5. Техническое обслуживание криптосредств

5.1 Техническое обслуживание криптосредств, а также другого оборудования, функционирующего с криптосредствами, смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

5.2 На время отсутствия пользователей криптосредства, а также другое оборудование, функционирующее с криптосредствами, при наличии технической возможности, выключается, отключается от линии связи и убирается в опечатываемые хранилища. В противном случае необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

6. Опечатывание аппаратных средств

6.1 Системные блоки АРМ, на которых установлены криптосредства, должны оборудоваться средствами контроля за их вскрытием (опечатываются, опломбируются). Место опечатывания (опломбирования) системного блока должно быть таким, чтобы его можно было визуально контролировать.

7. Порядок доступа к хранилищам

7.1 Эксплуатация хранилищ:

7.1.1 Пользователи криптосредств хранят эксплуатационную и техническую документацию к криптосредствам, ключевые документы в хранилищах (ящиках, шкафах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

7.1.2 Должно быть предусмотрено раздельное безопасное хранение пользователями криптосредств действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

7.2 При необходимости доступа к содержимому хранилища работник, ответственный за данное хранилище, проверяет целостность хранилища, открывает механический замок хранилища с использованием ключа.

7.3 По окончании работы работник закрывает и опечатывает хранилище, за которое он ответственен.

7.4 Печати, предназначенные для опечатывания хранилищ, должны находиться у работников, ответственных за данные хранилища.

8. Контроль безопасности криптосредств

Текущий контроль за организацией и обеспечением функционирования криптосредств возлагается на ответственного за эксплуатацию СКЗИ в пределах его полномочий.

9. Ответственность за нарушение требований

9.1 Пользователи криптосредств несут персональную ответственность за сохранность полученных криптосредств, эксплуатационной и технической документации к криптосредствам, ключевых документов, за соблюдение положений настоящей Инструкции.

9.2 Ответственный за эксплуатацию СКЗИ несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности обработки Информации с использованием криптосредств лицензионным требованиям и условиям эксплуатационной и технической документации к криптосредствам, а также настоящей Инструкции.

Приложение 13

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 472-р

**ИНСТРУКЦИЯ № 13-ИБ**

по использованию съемных носителей информации в администрации Трубчевского муниципального района

1. Использование съемных носителей информации

Под использованием съемных носителей информации в ИС понимается их подключение к АРМ с целью обработки, приема/передачи информации между АРМ и носителями информации.

В ИС допускается использование только учтенных съемных носителей информации, которые являются собственностью Администрации и подвергаются регулярной ревизии и контролю.

Съемные носители информации предоставляются пользователям ИС по инициативе руководителей структурных подразделений в случаях:

* необходимости выполнения вновь принятым работником своих должностных обязанностей;
* возникновения у сотрудника Администрации производственной необходимости.

2. Порядок учета, хранения и обращения со съемными носителями, твердыми копиями и их утилизации

Все находящиеся на хранении и в обращении съемные носители в ИС подлежат учёту.

Каждый съемный носитель должен иметь этикетку, на которой указывается его уникальный учетный номер.

Для получения электронного внешнего носителя, пользователь обращается к руководителю структурного подразделения, руководитель структурного подразделения пишет служебную записку на имя ответственного за организацию обработки персональных данных о выдаче пользователю внешнего электронного носителя, далее ответственный за организацию обработки персональных данных принимает решение и передает служебную записку администратору информационной безопасности.

Учет и выдачу съемных носителей осуществляет администратор информационной безопасности, на которого возложена эта функция. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации.

При использовании сотрудниками съемных носителей информации необходимо:

* соблюдать требования настоящей Инструкции;
* использовать носители информации исключительно для выполнения своих служебных обязанностей;
* ставить в известность администратора информационной безопасности о любых фактах нарушения требований настоящей Инструкции;
* бережно относиться к носителям информации;
* извещать администратора информационной безопасности о фактах утраты (кражи) носителей информации;

При использовании носителей конфиденциальной информации запрещено:

* использовать носители конфиденциальной информации в личных целях;
* передавать носители конфиденциальной информации другим лицам (за исключением администратора информационной безопасности);
* хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
* выносить съемные носители с конфиденциальной информацией (персональными данными) за пределы контролируемой зоны для работы с ними на дому и т. д.

Любое взаимодействие (обработка, прием/передача информации), инициированное пользователем ИС между АРМ и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с администратором информационной безопасности). Администратор информационной безопасности оставляет за собой право блокировать или ограничивать использование носителей информации.

В случае выявления фактов несанкционированного и/или нецелевого использовании носителей информации инициализируется служебная проверка, проводимая комиссией, состав которой определяется ответственным за организацию обработки персональных данных.

По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Администрации и действующему законодательству.

Информация, хранящаяся на съемных носителях, подлежит обязательной проверке на отсутствие вредоносного ПО.

В случае утраты или уничтожения съемных носителей конфиденциальной информации (персональных данных) либо разглашения содержащихся в них сведений немедленно ставится в известность руководитель структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей конфиденциальной информации (персональных данных).

Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение таких съемных носителей с конфиденциальной информацией осуществляется администратором информационной безопасности после сдачи пользователями, с отметкой в журнале.

В случае увольнения или перевода работника в другое структурное подразделение предоставленные носители конфиденциальной информации сдаются администратору информационной безопасности.

Приложение 14

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 472-р

**ИНСТРУКЦИЯ № 14-ИБ**

о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения информационных систем обработки персональных данных администрации Трубчевского муниципального района

1. Общие положения

1. Настоящая инструкция разработана в соответствии с требованиями законодательства Российской Федерации в области защиты персональных данных, с целью обеспечения возможности незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
2. Инструкция определяет правила и объёмы резервирования, а также порядок восстановления работоспособности информационных систем персональных данных (далее - ИСПДн) Администрации Трубчевского муниципального района (далее - Администрация).
3. Носители информации, используемые для резервирования конфиденциальной информации Администрации (в том числе и персональных данных), подлежат защите в той же степени, что и резервируемая конфиденциальная информация.
4. Контроль за исполнением настоящей инструкции осуществляет ответственный за обработку персональных данных Администрации.
5. Назначение и область действия

2.1 Данная инструкция предназначена для ответственного за техническое обслуживание информационных систем персональных данных (далее -администратор) Администрации, а также сотрудников Администрации, участвующих в обработке персональных данных в ИСПДн (далее - пользователи).

2.2 Инструкция описывает действия Администратора и пользователей по обеспечению резервного копирования и восстановления персональных данных, обрабатываемых в информационных системах персональных данных Администрации.

3. Информационные ресурсы, подлежащие резервированию

3.1. Резервному копированию подлежат все информационные ресурсы  
Администрации, содержащие персональные данные субъектов, а именно:

* файлы баз данных;
* электронные документы;
* файлы сообщений электронной почты;
* отсканированные и хранящиеся в ИСПДн изображения (документы).
  1. Резервному копированию могут так же подвергаться:
* системное и прикладное программное обеспечение ИСПДн;
* средства защиты информации в ИСПДн.

4. Порядок резервирования

4.1 Резервирование информационных ресурсов ИСПДн, содержащих персональные данные (далее - резервирование персональных данных), выполняется администратором ИСПДн.

4.2 Определяется 2 вида резервирования персональных данных:

- полное резервирование персональных данных - резервное копирование всех персональных данных, хранящихся в ИСПДн;

- неполное резервирование персональных данных - резервное копирование части персональных данных, хранящихся в ИСПДн.

Целью неполного резервирования является сохранение изменений в ИСПДн с момента полного резервирования персональных данных.

4.3. Периодичность проведения работ по резервированию персональных данных определяется администратором безопасности с учётом специфики работы ИСПДн, но не менее 1 раза в месяц для полного резервирования и 1 раза в неделю для неполного резервирования.

4.4. В случаях, когда информационные ресурсы персональных данных хранятся на компьютерах пользователей локально, допустимо перекладывать ответственность за проведение неполного резервирования персональных данных на пользователей ИСПДн.

4.5. Администратор ИСПДн использует средства резервного копирования ИСПДн для резервирования персональных данных на отчуждаемый носитель. В случаях, когда резервирование персональных данных средствами ИСПДн не представляется возможным, администратор ИСПДн по согласованию с ответственным за обработку персональных данных Администрация может использовать средство резервного копирования, не входящее в состав ИСПДн.

4.6. Резервное копирование с использованием незащищённых каналов связи общего пользования не допустимо.

4.7. Резервное копирование по локальной сети на устройство, находящееся вне ИСПДн, не допустимо.

4.8. При резервировании персональных данных не допускается хранение на одном носителе резервных копий персональных данных, извлечённых из различных ИСПДн. Для осуществления резервирования персональных данных различных ИСПДн, для каждой ИСПДн должен быть предусмотрен отдельный носитель информации.

4.9. В случае удаления персональных данных субъекта из ИСПДн должна быть так же удалена резервная копия этих данных.

5. Порядок хранения резервных копий

5.1. Хранение резервных копий персональных данных должно исключать любой несанкционированный доступ посторонних лиц к носителям информации.

5.2. Хранение резервных копий необходимо осуществлять в сейфах, несгораемых шкафах, металлических шкафах с устройством опечатывания. Доступ к местам хранения резервных копий должен быть предоставлен только администратору ИСПДн и ответственному за обработку ПДн Администрации.

5.3. Не допускается хранение резервных копий персональных данных совместно с другими носителями информации.

5.4. На носителе информации, содержащем резервные копии персональных данных, не должна храниться посторонняя информация.

5.5. Должно быть обеспечено одновременное хранение не менее двух носителей информации, хранящих полную резервную копию персональных данных ИСПДн.

6. Порядок восстановления информации после сбоя

6.1. В случае сбоя в работе ИСПДн, восстановление персональных данных из резервных копий осуществляет администратор ИСПДн.

6.2. Администратор ИСПДн обязан срочно уведомить ответственного за обработку персональных данных Администрации о факте сбоя в работе ИСПДн, повлёкшего нарушение целостности персональных данных.

6.3. Временной норматив по восстановлению персональных данных устанавливается ответственным за обработку персональных данных Администрации с учётом специфики работы ИСПДн.

Приложение 15

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 472-р

**ИНСТРУКЦИЯ № 15-ИБ**

по работе с инцидентами информационной безопасности в администрации Трубчевского муниципального района

Обозначения и сокращения

Администрация – Администрация Трубчевского муниципального района;

АРМ – автоматизированное рабочее место;

ИС –информационная система персональных данных;

ИБ – информационная безопасность

ПДн – персональные данные;

СЗИ – средства защиты информации.

Ответственность за выявление инцидентов ИБ и реагирование на них в Администрации возлагается на администратора информационной безопасности.

Администратор информационной безопасности имеет полномочия инициировать проведение служебных проверок (ходатайствовать о наложении дисциплинарного взыскания перед главой Администрации) по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

Администратор информационной безопасности обязан вести журнал учёта инцидентов ИБ (событий, действий, повлекших за собой риски безопасности защищаемой информации и создающих предпосылки к нарушению критериев безопасности информации). Сюда относятся нарушения пользователями положений организационно-распорядительных документов, установленных порядков и технологии работы в ИС, разглашение защищаемой информации и любые действия, направленные на это, не антропогенные инциденты (сбои ПО, стихийные бедствия).

В журнале в свободной форме описывается инцидент с указанием следующих данных:

* даты и времени;
* причин (умышленные и неумышленные действия, не антропогенные инциденты и т.п.)  и описания инцидента и задействованных лиц;
* информации о последствиях;
* информации о возможных последствиях (экономические убытки (в связи с заменой СЗИ, повторной аттестации; временные и трудозатраты на устранение последствий, нарушение работы пользователей, ущерб субъектам ПДн и юридические последствия для Администрации и т.п.).

Журнал с данным отчётом об инциденте предоставляется на ознакомление ответственному за организацию обработки персональных данных для принятия мер по предотвращению рецидива (возникновения повторного инцидента).

В случае возникновения рецидива со стороны пользователя или администратора информационной безопасности, по ходатайству ответственного за организацию обработки персональных данных главой Администрации накладывается дисциплинарное взыскание.

Сокрытие нарушений и инцидентов ИБ, вызванных любыми должностными лицами Объекта, является грубым нарушением трудовой дисциплины. Сокрытие нарушений и инцидентов ИБ, вызванных действиями администратора информационной безопасности и ответственным за организацию обработки персональных данных, является ГРУБЕЙШИМ НАРУШЕНИЕМ ДИСЦИПЛИНЫ, и при выяснении данного факта должно строго наказываться.

Любой сотрудник должен согласовывать следующие действия с администратором информационной безопасности:

* замена прикладного оборудования (мышь, клавиатура, принтер, монитор);
* установка дополнительного ПО;
* изменение сетевых настроек рабочего места;
* замена, изменение любой аппаратной части рабочего места.

Ответственный за организацию обработки персональных данных не может требовать от администратора информационной безопасности действий, направленных на нарушение настоящего руководства и других ОРД Администрации, требовать сокрытия инцидентов ИБ, вызванных любыми должностными лицами, требовать сообщения ему паролей на СЗИ и нарушения установленного разграничения прав по допуску к информационным ресурсам, установленным матрицей доступа к информационными ресурсам ИС.

Приложение 16

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 472-р

**ИНСТРУКЦИЯ № 16-ИБ**

по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств информационной системы персональных данных в администрации Трубчевского муниципального района

Обозначения и сокращения

Администрация – Администрация Трубчевского муниципального района;

АРМ – автоматизированное рабочее место;

ИС –информационная система персональных данных;

СВТ – средства вычислительной техники (системный блок, монитор, клавиатура, мышь, принтер/сканер);

ПДн – персональные данные;

ПО ­ - Программное обеспечение (офисные программы, архиватор, веб-браузер, программы для обработки конфиденциальной информации, антивирусы, кроме операционной системы и средств защиты информации);

АРМ ­- Автоматизированное рабочее место.

Настоящей инструкцией регламентируется проведении любых модификаций и изменений, технического обслуживания и устранения нештатных ситуаций в работе СВТ и ПО АРМ, входящих в состав ИС Администрации.

Все изменения конфигурации СВТ и ПО АРМ, входящих в состав ИС, ремонт, модификация, а также неконтролируемое со стороны администратора информационной безопасности техническое обслуживание СВТ и ПО АРМ, входящих в состав ИС, должны производиться только на основании письменных заявок (Приложение 1) администратору информационной безопасности. Ответственность за выполнение данного требования несёт сотрудник, эксплуатирующий данные средства информатизации.

При всех вышеуказанных работах на объектах информатизации сотрудниками подразделений (или сторонних организаций), занимающихся ремонтом, модификацией программных и аппаратных средств, инженерных коммуникаций, кабельных линий и систем объекта и выступающих в качестве инициаторов данных действий в соответствии с планом работ либо внепланово, руководитель структурного подразделения, эксплуатирующего ИС, либо пользователь ИС допускает указанных исполнителей к данным работам только по согласованию с администратором информационной безопасности.

Передача СВТ в другое подразделение или в распоряжение другой организации для ремонта или решения иных задач осуществляется только после того, как администратор информационной безопасности снимет средства защиты и предпримет необходимые меры для затирания или резервного копирования (при необходимости) защищаемой информации, которая хранилась на дисках.

О факте выполнения всех без исключения, вышеуказанных работ администратором информационной безопасности делается соответствующая отметка в «Журнале учета нештатных ситуаций, выполнения профилактических и ремонтных работ на объекте, установки и модификации аппаратных и программных средств ИС». Формат записей «Журнала учета нештатных ситуаций, выполнения профилактических и ремонтных работ на объекте, установки и модификации аппаратных и программных средств ИС»:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Дата записи | Краткое описание выполненной работы, основание | Дата и время начала работы | Дата и время окончания работы | ФИО исполнителей работ и их подписи | Подпись администратора информационной безопасности | Примечание |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

Пользователям и администратору информационной безопасности необходимо знать, что контролю со стороны администратора информационной безопасности и регистрации в журнале подлежат:

* замена (модификация) СВТ, входящих в состав ИС, в соответствии с техническим паспортом на ИС;
* замена, изъятие, добавление СВТИС;
* техническое обслуживание и ремонт СВТ без замены комплектующих и составных частей;
* обновление (замена) на конкретном автоматизированном рабочем месте или сервере ПО, необходимого для решения определенной задачи (обновление версий, используемых для решения определенной задачи программ);
* изменение местоположения СВТ и вспомогательных средств и систем, указанных в схеме технического паспорта.

В случае внесения изменений в состав СВТ АРМ (замена комплектующих, изменение местоположения СВТ внутри кабинета), входящих в ИС, кроме замены системного блока администратор информационной безопасности вносит необходимые изменения в лист регистрации изменений в «Техническом паспорте информационной системы персональных данных». Далее изменение согласовывается с ответственным за организацию обработки ПДн (делается роспись в листе регистрации изменений).

В случае внесения изменений в состав ПО (переустановка, удаление, изменение версий офисных программ, архиваторов, веб-браузеров, программ для обработки конфиденциальной информации, антивирусов, кроме операционной системы и средств защиты информации) на АРМ, входящих в состав ИС, администратор информационной безопасности вносит необходимые изменения в «Разрешительную систему доступа персонала к сведениям конфиденциального характера в информационной системе персональных данных». Далее разрешительная система утверждается директором.

В случае замены системного блока, жёсткого диска в составе СВТ АРМ, входящих в состав ИС, переустановки операционной системы, средств защиты администратор информационной безопасности связывается с представителем компании, выдавшей аттестат соответствия требованиям по безопасности информации для принятия решения о необходимости повторной аттестации ИС. До выполнения мероприятий по повторной аттестации ИС, выданный аттестат соответствия является НЕДЕЙСТВИТЕЛЬНЫМ.

Нештатные ситуации и форс-мажор

В условиях необходимого немедленного реагирования на нештатные ситуации разрешается модификация, замена, ремонт и т.д. без согласования с администратором информационной безопасности.

К нештатным ситуациям относятся:

* выход из строя или неустойчивое функционирование узлов ПЭВМ, периферийных устройств, средств защиты информации по различным причинам;
* выход из строя системы электроснабжения.

При возникновении необходимости оперативной модификации, замены, ремонта и т.п. пользователи извещают администратора информационной безопасности. Необходимые работы выполняются под контролем пользователей и последующим написанием объяснительной записки на имя ответственного за организацию обработки персональных данных с обоснованием экстренных изменений и описанием произведённых действий, ответственный за организацию обработки персональных данных передает объяснительную записку администратору информационной безопасности. По результатам рассмотрения объяснительной записки администратор информационной безопасности выполняет все действия, предусмотренные инструкциями.

Приложение 17

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 472-р

**ИНСТРУКЦИЯ № 17-ИБ**  
по контролю защищенности информации в информационных системах администрации Трубчевского муниципального района

1. Общие положения

  1.1. Настоящая инструкция регламентирует контроль уровня защищенности информации, обрабатываемой в информационных системах администрации Трубчевского муниципального района (далее - ИС Администрации), путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты информации.

2. Выявление, анализ и устранение уязвимостей информационной системы

2.1. В ИС Администрации при выявлении (поиске), анализе и устранении уязвимостей проводятся:

-      выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;

- разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;

- анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;

- устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;

- информирование должностных лиц Администрации (пользователей, администраторов) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

2.2. В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей.

2.3. Выявление (поиск), анализ и устранение уязвимостей проводится на этапах создания и эксплуатации информационной системы. На этапе эксплуатации поиск и анализ уязвимостей проводится администраторами не реже одного раза в месяц. При этом в обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в ИС Администрации.

2.4. В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (корректировка настроек средств защиты информации, изменение режима и порядка использования ИС Администрации), направленные на устранение возможности использования выявленных уязвимостей.

2.5. В ИС Администрации используются для выявления (поиска) уязвимостей средства анализа (контроля) защищенности (сканеры безопасности), имеющие стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования информационной системы на наличие уязвимостей, оценки последствий уязвимостей, имеющие возможность оперативного обновления базы данных выявляемых уязвимостей.

2.6. В ИС Администрации осуществляется получение из доверенных источников и установка обновлений базы признаков уязвимостей (для системы анализа защищенности).

2.7. Доступ к функциям выявления (поиска) уязвимостей предоставляется только администратору информационной безопасности и администратору виртуальной инфраструктуры. Администратор информационной безопасности проводит анализ журналов регистрации событий безопасности (журнала аудита) в целях определения, были ли выявленные уязвимости ранее использованы в ИС Администрации для нарушения безопасности информации.

3. Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации

3.1. В ИС Администрации администраторами в рамках своих полномочий осуществляется контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

3.2. В ИС Администрации администраторами в рамках своих полномочий осуществляется получение из доверенных источников и установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

3.3. При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в ИС Администрации и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

3.4. Контроль установки обновлений проводится не реже одного раза в месяц.

3.5. При контроле установки обновлений осуществляются проверки установки обновлений баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты в соответствии с Инструкцией по антивирусной защите в информационных системах Администрации, баз признаков уязвимостей средств анализа защищенности и иных баз данных, необходимых для реализации функций безопасности средств защиты информации.

4. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

4.1. При контроле работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации, осуществляется:

- контроль работоспособности (неотключения) программного обеспечения и средств защиты информации;

- проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации;

- контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;

- восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

4.2. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится администраторами в рамках своих полномочий не реже одного раза в три месяца.

5. Контроль состава технических средств, программного обеспечения и средств защиты информации

5.1. При контроле состава технических средств, программного обеспечения и средств защиты информации (инвентаризации) осуществляется:

- контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации ИС Администрации и принятие мер, направленных на устранение выявленных недостатков;

- контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;

- контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

- исключение (восстановление) из состава ИС Администрации несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

5.2. Контроль состава технических средств, программного обеспечения и средств защиты информации проводится администраторами в рамках своих полномочий не реже одного раза в месяц.

6. Контроль правил генерации и смены паролей пользователей, заведения и удаления учётных записей, реализации правил разграничения доступом, полномочий пользователей в информационной системе

6.1. При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС Администрации осуществляется:

- контроль правил генерации и смены паролей пользователей в соответствии с Правилами идентификации и аутентификации пользователей в информационных системах Администрации;

- контроль заведения и удаления учетных записей пользователей в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в информационных системах Администрации;

- контроль реализации правил разграничения доступом в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в информационных системах Администрации;

- контроль реализации полномочий пользователей в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в информационных системах Администрации;

- контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей, предусмотренных организационно-распорядительными документами по защите информации в Администрации;

-  устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

 6.2. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС Администрации проводится администратором информационной безопасности не реже одного раза в три месяца.