ИВАНОВСКАЯ ОБЛАСТЬ
АДМИНИСТРАЦИЯ ЮЖСКОГО МУНИЦИПАЛЬНОГО РАЙОНА

РАСПОРЯЖЕНИЕ

от 29.12.2017г. № 1092-р
г. Южа

О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района

В целях соблюдения требований, установленных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами,

1. Назначить лицом, ответственным за организацию обработки персональных данных Капралова Владимира Николаевича – начальника отдела общественной и информационной политики Администрации Южского муниципального района
2. Назначить лицом, ответственным за защиту информации, за обеспечение безопасности персональных данных в информационных системах Администрации Южского муниципального района – Администратором безопасности информации: Капралова Владимира Николаевича – начальника отдела общественной и информационной политики Администрации Южского муниципального района
3. Назначить лицом, ответственным за обслуживание и обеспечение бесперебойной работоспособности средств вычислительной техники и программного обеспечения в информационных системах Администрации Южского муниципального района – Администратором информационной системы: Капралова Владимира Николаевича – начальника отдела общественной и информационной политики Администрации Южского муниципального района
4. В целях исполнения требований действующего законодательства РФ в области защиты информации ограниченного распространения при уничтожении в Администрации Южского муниципального района материальных носителей информации, содержащих персональные данные, назначить комиссию по уничтожению материальных носителей информации содержащих персональные данные, в составе:

Председатель: Капралов Владимир Николаевич – начальник отдела общественной и информационной политики Администрации Южского муниципального района

Члены комиссии: Максимов Сергей Альбертович - начальник отдела по делам ГО и ЧС Администрации Южского муниципального района;

Липатов Сергей Владимирович - заведующий хозяйственным

отделом Администрации Южского муниципального района;

Шутова Ольга Юрьевна -- главный специалист отдела правового обеспечения, муниципальной службы и контроля Администрации Южского муниципального района

5. Утвердить документы и типовые формы документов:

5.1. Инструкция по проведению аудита средств защиты информации в информационной системе Администрации Южского муниципального района (Приложение № 1)

5.2. Инструкция ответственного за организацию обработки персональных данных в информационной системе Администрации Южского муниципального района (Приложение № 2);

5.3. Инструкция Администратора безопасности информации (Приложение № 3);

5.4. Инструкция Администратора информационной системы (Приложение № 4);

5.5. Инструкция Пользователя информационной системы (Приложение № 5);

5.6. Инструкция по обеспечению безопасности конфиденциальной информации и персональных данных при возникновении нештатных ситуаций при эксплуатации информационной системы (Приложение № 6);

5.7. Инструкция по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационной системы Администрации Южского муниципального района (Приложение № 7);

5.8. Инструкция по организации парольной защиты (Приложение № 8);

5.9. Инструкция по организации резервного копирования (Приложение № 9);

5.10. Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы Администрации Южского муниципального района (Приложение № 10);

5.11. Инструкция по обеспечению безопасности персональных данных при их обработке в информационной системе Администрации Южского муниципального района (Приложение № 11);

5.12. Инструкция по проведению антивирусного контроля (Приложение № 12);

5.13. Положение о разрешительной системе доступа к информационным ресурсам информационной системы Администрации Южского муниципального района (Приложение № 13);

5.14. Перечень должностей работников, доступ которых к конфиденциальной информации и персональным данным, обрабатываемым в информационной системе Администрации Южского муниципального района, и к техническим средствам необходим для выполнения ими трудовых обязанностей (Приложение № 14);

5.15. Перечень должностей работников, имеющих физический доступ к машинным носителям информации в информационной системе Администрации Южского муниципального района, для выполнения ими трудовых обязанностей (Приложение № 15);

5.16. Список должностей работников с указанием методов управления доступом, типа доступа и правил доступа к ресурсам информационной системы Администрации Южского муниципального района системы (Приложение № 16);

5.17. Положение об использовании мобильных устройств и носителей информации в Администрации Южского муниципального района (Приложение № 17);

5.18. Перечень конфиденциальной информации, обрабатываемой в информационной системе Администрации Южского муниципального района (Приложение № 18);

5.19. Правила обработки персональных данных в информационной системе

Администрации Южского муниципального района (Приложение № 19);

5.20. Перечень программного обеспечения и (или) его компонентов, разрешенных к установке («белый список») в информационной системе, и перечень программного обеспечения и (или) его компонентов, запрещенных к установке («черный список») в информационной системе (Приложение № 20);

5.21. Перечень событий безопасности в информационной системе Администрации Южского муниципального района (Приложение № 21);

5.22. Типовая форма Журнала антивирусных проверок в информационных системах Администрации Южского муниципального района (Приложение № 22);

4.23. Типовая форма Журнала учета машинных носителей конфиденциальной информации и персональных данных в информационных системах Администрации Южского муниципального района (Приложение № 23);

5.24. Типовая форма Журнала учета средств защиты информации, технической и эксплуатационной документации в информационных системах Администрации Южского муниципального района (Приложение № 24);

5.25. Типовая форма Журнала учета ремонтно-восстановительных работ на основных технических средствах в информационных системах Администрации Южского муниципального района (Приложение № 25);

5.26. Типовая форма Журнала учета мероприятий по контролю режима защиты конфиденциальной информации и персональных данных и выполнения обязательных процедур в информационной системе в информационных системах Администрации Южского муниципального района (Приложение № 26);

5.27. Типовая форма Журнала учета учетных записей пользователей информационной системы в информационных системах Администрации Южского муниципального района (Приложение № 27);

5.28. Типовая форма журнала учета печатных документов в информационных системах Администрации Южского муниципального района (Приложение № 28);

5.29. Типовая форма Акта об уничтожении персональных данных субъекта(ов) персональных данных (в случае достижения целей обработки) (Приложение № 29);

5.30. Типовая форма Журнала учета мероприятий по контролю эффективности использования применяемых средств защиты информации в информационных системах Администрации Южского муниципального района (Приложение № 30);

6. Работникам, непосредственно осуществляющим обработку конфиденциальной информации и персональных данных в информационной системе Администрации Южского муниципального района, в целях соблюдения требований законодательства Российской Федерации в области персональных данных, руководствоваться документами, утвержденными настоящим распоряжением.

7. Руководителям структурных подразделений:

7.1. Направлять информацию о необходимости внесения изменений в утвержденные документы, в письменной форме на имя Администратора безопасности информации;

7.2. Ознакомить под роспись с настоящим распоряжением работников, непосредственно осуществляющих обработку конфиденциальной информации и персональных данных в информационной системе.

Глава Южского муниципального района **В.И. Мальцев**

Приложение № 1
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Инструкция
по проведению аудита средств защиты информации в информационной системе Администрации Южского муниципального района

I. Общие положения

1.1. Настоящая Инструкция определяет действия работников Администрации Южского муниципального района (далее Администрация) по проведению аудита средств защиты информации в информационной системе Администрации.

1.2. Настоящая Инструкция предназначена для уполномоченных работников Администрации: Администратора информационной системы и Администратора безопасности информации.

1.3. Средства защиты информации в составе системы защиты персональных данных (СЗПДн), должны обеспечивать конфиденциальность, целостность и доступность персональных данных при их обработке в информационной системе персональных данных (ИСПДн) во всех структурных элементах, на технологических участках обработки и во всех режимах функционирования информационной системы.

II. Требования к реализации аудита средств защиты информации в информационной системе

2.1. Контроль соответствия состава средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации информационной системы и принятие мер, направленных на устранение выявленных недостатков.

2.2. Осуществление контроля установки обновлений программного обеспечения средств защиты информации.

2.3. Контроль работоспособности (неотключения) программного обеспечения и средств защиты информации.

2.4. Проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации, объем и содержание которой определяется оператором.

2.5. Контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации.

2.6. 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.

2.7. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.

2.8. Контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков.

2.9. Исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) средств защиты информации.

III. Заключительные положения

3.1. Проверка и пересмотр настоящей инструкции осуществляются в следующих случаях:

- при изменении законодательства Российской Федерации в области персональных данных и пересмотре отраслевых требований обеспечения безопасности персональных данных;
- при внедрении новой техники и (или) технологий;
- по результатам анализа материалов расследования нарушений требований законодательства по обеспечению безопасности персональных данных;
- при появлении новых актуальных угроз безопасности персональных данных;
- изменением уровня защищенности персональных данных при их обработке в информационной системе персональных данных в зависимости от угроз безопасности этих данных;
- по требованию представителей контролирующих (надзорных) органов.

3.2. Ответственность за своевременную корректировку настоящей инструкции возлагается на лицо, назначенное ответственным за организацию обработки персональных данных в Администрации.

Приложение № 2
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Инструкция
ответственного за организацию обработки персональных данных в информационной системе Администрации Южского муниципального района

I. Общие положения

1.1. Настоящая инструкция разработана в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

1.2. Ответственный за организацию обработки персональных данных в Администрации Южского муниципального района (далее Администрация) назначается распоряжением руководителя Администрации.

1.3. Ответственный за организацию обработки персональных данных в Администрации в своей деятельности руководствуется Федеральным законом от 27 июля 2006 г. № 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 ноября 2012 г. № 1119, Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687, приказом Федеральной службы по техническому и экспортному контролю № 17 от 11 февраля 2013 года «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», другими законодательными и нормативно-правовыми актами по вопросам обработки и защиты персональных данных.

II. Обязанности ответственного за организацию обработки персональных данных

2.1. Ответственный за организацию обработки персональных данных обязан:

- осуществлять внутренний контроль за соблюдением работниками Администрации законодательства Российской Федерации, локальных актов по обработке персональных данных, требований к защите персональных данных и принимать меры по устранению выявленных нарушений;
- организовывать проведение занятий и (или) доведение до сведения работников Администрации положений законодательства Российской Федерации о персональных данных, локальных актов Администрации по вопросам обработки персональных данных, требований к защите персональных данных;

- руководить разработкой в Администрации распоряжений, положений, инструкций, правил, порядков, перечней и других документов, регламентирующих порядок обработки персональных данных по вопросам защиты персональных данных в соответствии с требованиями законодательства и нормативно-правовых актов Российской Федерации;
- организовывать и контролировать прием и обработку обращений и запросов субъектов персональных данных или их представителей;
- при организации обработки персональных данных принимать необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного намеренного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных;
- докладывать руководителю Администрации о выявленных нарушениях обработки персональных данных или требований по их защите, принимаемых мерах и способах устранения выявленных нарушений.

III. Ответственность лица, ответственного за организацию обработки персональных данных

3.1. В соответствии с законодательством Российской Федерации ответственный за организацию обработки персональных данных несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность за невыполнение или халатное выполнение обязанностей по организации, контролю и обеспечению выполнения требований законодательства, нормативно-правовых актов Российской Федерации по вопросам обработки и защиты персональных данных в Администрации.

IV. Права ответственного за организацию обработки персональных данных

4.1. Ответственный за организацию обработки персональных данных имеет право:
- требовать от работников Администрации письменных объяснений по фактам нарушения ими требований законодательства Российской Федерации, локальных актов о персональных данных и защите персональных данных;
- вносить предложения руководителю Администрации об отстранении работников от обработки персональных данных, применению к ним дисциплинарных взысканий, в том числе об увольнении работников, при обнаружении нарушения ими требований законодательства Российской Федерации, локальных актов по вопросам обработки персональных данных или требований к защите персональных данных.

Приложение № 3
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Инструкция
Администратора безопасности информации

I. Общие положения

1.1. Для обеспечения защиты информации, содержащейся в информационной системе, руководителем Администрации Южского муниципального района (далее Администрация) назначается должностное лицо (работник), ответственный за защиту информации – Администратор безопасности информации, который также является ответственным за обеспечение безопасности персональных данных в информационной системе, при обработке в информационной системе персональных данных.

1.2. Администратор безопасности информации является ответственным должностным лицом Администрации уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты информационной системы и ее ресурсов на этапах эксплуатации и модернизации.

1.3. Администратор безопасности информации должен иметь специальное рабочее место, размещенное в здании Администрации так, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.4. Рабочее место Администратора безопасности информации должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф и т.д.), а также средствами контроля за техническими средствами защиты.

1.5. Администратор безопасности информации осуществляет методическое руководство Администратором информационной системы и Пользователями информационной системы по вопросам обеспечения безопасности обрабатываемой конфиденциальной информации и персональных данных.

1.6. Требования Администратора безопасности информации, по обеспечению защиты информации, содержащейся в информационной системе, обязательны для исполнения всеми Пользователями информационной системы.

1.7. Администратор безопасности информации несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в информационной системе, состояние и поддержание установленного уровня защиты информационной системы.

II. Функции, осуществляемые Администратором безопасности информации

2.1. Администратор безопасности информации осуществляет следующие основные функции:

- Разрабатывает предложения по определению класса защищенности объектов информационной системы (ИС) и автоматизированной системы (АС).
- Участвует в организации работ по выявлению актуальных угроз безопасности информации, в т.ч. персональных данных.
- Осуществляет методическое руководство и участвует в разработке (согласовании) конкретных требований по защите конфиденциальной информации и персональных данных, разработке технического (частного технического) задания на создание системы защиты информации (персональных данных).
- Согласовывает выбор конкретных средств обработки информации, технических и программных средств защиты.
- Осуществляет контроль реализации проектных решений на создание системы защиты информации (персональных данных).
- Участвует в организации работ по оценке соответствия информационной системы предъявляемым требованиям по обеспечению безопасности информации.
- Участвует в организации разработки организационно-распорядительной документации по защите информации в информационной системе.
- Проводит контроль требуемого уровня обеспечения защищенности информации при эксплуатации системы защиты информации, в том числе контроль соблюдения условий использования средств защиты информации.
- Участвует в организации обучения должностных лиц (работников) – пользователей информационной системы Администрации, ответственных за эксплуатацию средств защиты информации.
- Участвует в организации охраны и физической защиты помещений Администрации, в которых размещены средства обработки информации, исключающих несанкционированный доступ к техническим средствам информационной системы, их хищение и нарушение работоспособности, хищение машинных носителей информации.
- Оказывает методическую помощь должностным лицам (работникам) Администрации.

III. Обязанности Администратора безопасности информации

3.1. Администратор безопасности информации **обязан**:

- 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.
- Осуществлять установку, настройку и сопровождение технических средств защиты, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.
- Обеспечивать методическое руководство, разработку требований к мерам защиты информационной системы и контроль за эффективностью использования предусмотренных мер защиты информации.
- Участвовать в контрольных и тестовых испытаниях и проверках элементов информационной системы.
- Обеспечивать подготовку предложений по совершенствованию и реализации положений Политики информационной безопасности информационной системы и

контролировать выполнение установленных требований в структурных подразделениях Администрации.

- Организовывать приобретение и установку лицензионного программного обеспечения.
- Обеспечивать доступ к защищаемой информации Пользователям информационной системы на основании заявок руководителей структурных подразделений, согласно занимаемой должности и в соответствии с возложенными полномочиями.
- Уточнять в установленном порядке инструкции Администратора информационной системы и Пользователей информационной системы.
- Обеспечивать обновление базы решающих правил системы обнаружения вторжений, применяемой в информационной системе.
- Вести контроль над процессом осуществления резервного копирования и хранения информации, подлежащей защите.
- Организовывать и осуществлять контроль по выполнению защиты конфиденциальной информации и персональных данных.
- Организовывать и реализовывать функции управления учетными записями пользователей, в том числе внешних пользователей (при необходимости).
- Анализировать состояние защиты информационной системы и ее отдельных подсистем.
- Контролировать неизменность состояния средств защиты их параметров и режимов защиты.
- Осуществлять обновление базы «черных» («белых») списков и контроль целостности базы «черных» («белых») списков программного обеспечения и его компонентов, а также отправителей электронных сообщений.
- Контролировать физическую сохранность средств и оборудования информационной системы.
- Контролировать исполнение Пользователями информационной системы введенного режима безопасности, а также правильность работы с элементами информационной системы и средствами защиты.
- Периодически контролировать исполнение Пользователями информационной системы правил сохранности личных ключей и атрибутов доступа к ресурсам информационной системы, хранения персонального устройства идентификации (при наличии), магнитных носителей информации и документов, содержащих конфиденциальную информацию и персональные данные, опечатывание узлов и блоков информационной системы (при необходимости).
- Организовать осуществление мониторинга (просмотр, анализ) результатов регистрации событий безопасности.
- Обеспечить защиту конфиденциальной информации и персональных данных при подключении информационной системы к информационно - телекоммуникационным сетям (в т.ч. «Интернет»), контролировать работу пользователей в информационно - телекоммуникационных сетях и обеспечивать защиту информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа информационной системы через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа).

- Своевременно анализировать информацию, регистрируемую средствами защиты, с целью выявления возможных нарушений.
- Контролировать установку и использование элементов информационной системы, поставленных на балансовый учет в Администрации, предназначенных для работы в информационной системе и использования машинных носителей информации, поставленных на учет в соответствии с установленным порядком.
- Не допускать к работе на элементах информационной системы посторонних лиц.
- Осуществлять периодические контрольные проверки ПЭВМ и тестирование правильности функционирования средств защиты информационной системы.
- Оказывать помощь Пользователям информационной системы в части применения средств защиты и консультировать по вопросам введенного режима защиты.
- Докладывать руководству о состоянии защиты информационной системы, о нештатных ситуациях на объектах информационной системы и допущенных пользователями нарушениях установленных требований по защите информации.
- В случае отказа работоспособности технических средств и программного обеспечения информационной системы, в том числе средств защиты, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.
- Принимать меры по реагированию, в случае возникновения нештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3.2. Администратору безопасности информации **запрещается**:
- Использовать в личных целях конфиденциальную информацию и персональные данные, ставшие известными ему вследствие выполнения трудовых обязанностей.
- Копировать документированную конфиденциальную информацию и персональные данные на машинные носители, а также фотографировать защищаемую информацию, для последующей передачи третьим лицам.
- Подключать к ПЭВМ и оборудованию, подключенному к информационной системе, личные машинные носители информации и мобильные устройства.
- Отключать (блокировать) средства защиты информации во время обработки информации в информационной системе.
- Обрабатывать на ПЭВМ информацию и выполнять работы, не предусмотренные функциональными обязанностями.
- Сообщать (или передавать) посторонним лицам ключи и атрибуты доступа к ресурсам информационной системы.
- Оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации (при наличии), магнитные носители и распечатки, содержащие конфиденциальную информацию и персональные данные.

IV. Права Администратора безопасности информации

4.1. Администратор безопасности информации имеет **право**:
- Устанавливать и изменять правила пользования информацией в информационной системе.

- Знакомиться с документами, определяющими его права и обязанности по занимаемой должности (возложенных обязанностях), критерии оценки качества исполнения должностных (возложенных) обязанностей.
- Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с исполнением обязанностей в соответствии с настоящей инструкцией и функционированию информационной системы.
- Требовать от руководства обеспечения организационно - технических условий, необходимых для исполнения обязанностей в соответствии с настоящей инструкцией.
- Отключать элементы системы защиты информации при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей в установленном порядке.
- Требовать от Пользователей информационной системы соблюдения установленных правил и требований работы в информационной системе и использования машинных носителей информации.

V. Ответственность Администратора безопасности информации

5.1. Администратор безопасности информации несет ответственность:
- За нарушение функционирования средств защиты информации в информационной системе вследствие ненадлежащего исполнения своих обязанностей.
- За несвоевременное уведомление руководства о случаях нарушения правил пользования ресурсами информационной системы и случаях несанкционированного доступа к информации, обрабатываемой в информационной системе.

5.2. Администратор безопасности информации привлекается к ответственности:
- За ненадлежащее исполнение или неисполнение своих должностных (возложенных) обязанностей, предусмотренных настоящей инструкцией - в пределах, установленных действующим трудовым законодательством Российской Федерации.
- За разглашение информации, охраняемой законодательством Российской Федерации.
- За правонарушения, совершенные в процессе своей деятельности - в пределах, установленных действующим административным, уголовным и гражданским законодательством Российской Федерации.
- За причинение материального ущерба - в пределах, установленных действующим законодательством Российской Федерации.

Приложение № 4
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Инструкция
Администратора информационной системы

I. Общие положения

1.1. Администратор информационной системы относится к категории специалистов.

1.2. Администратором информационной системы назначается лицо, имеющее профильное профессиональное образование, опыт технического обслуживания и ремонта персональных компьютеров и оргтехники, знающее основы построения локальных сетей (протоколы TCP/IP, сетевое оборудование, принципы построения локальных вычислительных сетей).

1.3. Администратор информационной системы должен **знать**:

- Технические характеристики, назначение, режимы работы, конструктивные особенности, правила технической эксплуатации оборудования, входящего в состав информационной системы: оргтехники, серверов и персональных компьютеров.
- Аппаратное и программное обеспечение, применяемое в информационной системе.
- Принципы ремонта персональных компьютеров и оргтехники.
- Языки и методы программирования.
- Основы информационной безопасности, способы защиты информации от несанкционированного доступа, повреждения или умышленного искажения, уничтожения.
- Порядок оформления технической документации.
- Правила внутреннего трудового распорядка.
- Основы трудового законодательства.
- Правила и нормы охраны труда, техники безопасности и противопожарной защиты.

1.4. Администратор информационной системы приступает к исполнению обязанностей и освобождается от исполнения обязанностей, предусмотренных настоящей инструкцией, на основании распоряжения руководителя Администрации Южского муниципального района, по представлению сотрудника (руководителя) подразделения, осуществляющего кадровый учет.

1.5. Администратор информационной системы подчиняется непосредственному руководителю в соответствии с занимаемой должностью.

II. Обязанности Администратора информационной системы

2.1. Администратор информационной системы **обязан**:

- Обеспечивать бесперебойную работоспособность средств вычислительной техники информационной системы, проводить организационно-технические мероприятия по обслуживанию.

- Устанавливать на серверы и рабочие станции, прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации.
- Выполнять своевременное обновление программного обеспечения элементов информационной системы и системы защиты информации.
- Осуществлять конфигурацию программного обеспечения на рабочей станции.
- Поддерживать в работоспособном состоянии программное обеспечение рабочей станции информационной системы.
- Проводить антивирусный контроль.
- Формировать идентификаторы, по которым однозначно идентифицируются пользователи информационной системы.
- Своевременно осуществлять управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей (при необходимости) в информационной системе.
- Обеспечивать запрет запуска без команды пользователя в информационной системе программного обеспечения (программного кода), используемого для взаимодействия со съемным носителем информации.
- Осуществлять техническую и программную поддержку пользователей, консультировать пользователей по вопросам работы программ, составлять инструкции по работе с программным обеспечением и доводить их до сведения пользователей.
- Обеспечивать защиту информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа информационной системы через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа) (в случае необходимости использования).
- Устанавливать права доступа и контролировать использование сетевых ресурсов (при их наличии).
- Обеспечивать своевременное копирование, архивирование и резервирование данных.
- Принимать меры по восстановлению работоспособности информационной системы при сбоях или выходе из строя.
- Выявлять ошибки пользователей и программного обеспечения и принимать меры по их исправлению.
- Проводить мониторинг системы, разрабатывать предложения по развитию инфраструктуры информационной системы.
- Обеспечивать сетевую безопасность (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия (при наличии).
- Осуществлять антивирусную защиту информационной системы.
- Контролировать синхронизацию системного времени.
- Осуществлять мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.
- Осуществлять контроль за монтажом оборудования, входящего в состав информационной системы, специалистами сторонних организаций.

- Сообщать Администратору безопасности информации о случаях нарушения правил пользования информационной системой и принятых мерах.
- Участвовать совместно с Администратором безопасности информации в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации.

Администратору информационной системы **запрещается**:
- использовать в личных целях конфиденциальную информацию и персональные данные, ставшие известными ему вследствие выполнения трудовых обязанностей;
- копировать конфиденциальную информацию и персональные данные на машинные носители без разрешения, а также фотографировать защищаемую информацию, для последующей передачи третьим лицам;
- самостоятельно, без согласования с Администратором безопасности информации устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к папкам на ПЭВМ;
- подключать к ПЭВМ и оборудованию, подключенному к информационной системе, личные машинные носители информации и мобильные устройства;
- отключать (блокировать) средства защиты информации без согласования с Администратором безопасности информации;
- обрабатывать на ПЭВМ информацию и выполнять работы, не предусмотренные функциональными обязанностями;
- сообщать (или передавать) посторонним лицам ключи и атрибуты доступа к ресурсам информационной системы;
- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации (при наличии), магнитные носители и распечатки, содержащие конфиденциальную информацию и персональные данные;
- привлекать посторонних лиц для производства ремонта или настройки ПЭВМ и информационной системы, без согласования с Администратором безопасности информации.

III. Права Администратора информационной системы

3.1. Администратор информационной системы имеет **право**:
- Устанавливать и изменять правила пользования информацией в информационной системе.
- Знакомиться с документами, определяющими его права и обязанности по занимаемой должности (возложенных обязанностях), критерии оценки качества исполнения должностных (возложенных) обязанностей.
- Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с исполнением обязанностей в соответствии с настоящей инструкцией и функционированию информационной системы.
- Требовать от руководства обеспечения организационно - технических условий, необходимых для исполнения обязанностей в соответствии с настоящей инструкцией.

- Отключать элементы информационной системы при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей, после согласования и заблаговременного предупреждения пользователей и Администратора безопасности информации.
- Отключать элементы системы защиты информации при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей, только после согласования с Администратором безопасности информации.
- Требовать от пользователей информационной системы соблюдения установленных правил и требований работы в информационной системе.

IV. Ответственность Администратора информационной системы

4.1. Администратор информационной системы несет ответственность:
- За нарушение функционирования информационной системы, вследствие ненадлежащего исполнения своих обязанностей.
- За несвоевременное управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей в информационной системе.
- За несвоевременное уведомление руководства о случаях нарушения правил пользования ресурсами информационной системы и случаев несанкционированного доступа к информации, обрабатываемой в информационной системе.

4.2. Администратор информационной системы привлекается к ответственности:
- За ненадлежащее исполнение или неисполнение своих должностных (возложенных) обязанностей, предусмотренных настоящей инструкцией - в пределах, установленных действующим трудовым законодательством Российской Федерации.
- За разглашение информации, охраняемой законодательством Российской Федерации.
- За правонарушения, совершенные в процессе своей деятельности - в пределах, установленных действующим административным, уголовным и гражданским законодательством Российской Федерации.
- За причинение материального ущерба - в пределах, установленных действующим законодательством Российской Федерации.

Приложение № 5
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Инструкция
Пользователя информационной системы

I. Общие положения

1.1. Пользователь информационной системы относится к категории специалистов, участвующих в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, базам данных и средствам защиты.

1.2. Пользователь информационной системы должен иметь образование, или специальную подготовку, позволяющие самостоятельно и свободно обращаться с персональным компьютером, оргтехникой и пользоваться необходимым программным обеспечением.

1.3. Пользователь информационной системы должен **знать**:

- Технические характеристики, назначение, режимы работы, правила технической эксплуатации оборудования, входящего в состав информационной системы: персонального компьютера и оргтехники.
- Правила пользования материальными и машинными носителями, содержащими конфиденциальную информацию и персональные данные.
- Правила работы в информационной системе, основные требования и способы защиты информации от несанкционированного доступа, повреждения или умышленного искажения, уничтожения.
- Правила и порядок работы с обезличенной информацией.
- Правила внутреннего трудового распорядка.
- Основы трудового законодательства.
- Правила и нормы охраны труда, техники безопасности и противопожарной защиты.

1.4. Пользователь информационной системы допускается к работе в информационной системе в соответствии с утвержденным Перечнем лиц, доступ которых к конфиденциальной информации и персональным данным, обрабатываемым в информационной системе, необходим для выполнения им трудовых обязанностей.

1.5. Пользователь информационной системы подчиняется непосредственному руководителю структурного подразделения в соответствии с занимаемой должностью.

II. Обязанности Пользователя информационной системы

2.1. Пользователь информационной системы **обязан**:

- На выделенном, для работы персональном компьютере (ПЭВМ), в информационной системе выполнять только трудовые обязанности в соответствии с занимаемой должностью.
- Перед началом работы на ПЭВМ проверить свои рабочие папки на жестком магнитном диске, учтенные, установленным порядком машинные носители информации, на отсутствие вирусов с помощью штатных средств антивирусной защиты, убедиться в исправности ПЭВМ.
- При сообщениях тестовых программ о появлении вирусов немедленно прекратить работу, доложить Администратору информационной системы и своему непосредственному начальнику.
- При обработке конфиденциальной информации и персональных данных использовать только машинные носители информации, зарегистрированные установленным порядком.
- При необходимости использования машинных носителей, поступивших из других подразделений, учреждений, предприятий и организаций, прежде всего, провести проверку этих носителей на отсутствие вирусов.
- Выполнять указания и требования Администратора информационной системы и Администратора безопасности информации.
- Представлять для контроля ПЭВМ руководителю подразделения, Администратору информационной системы и Администратору безопасности информации.
- Сохранять в тайне полученные от Администратора безопасности информации или от Администратора информационной системы пароль и учетные данные, не сообщать их другим лицам и не хранить их в виде записей в доступных местах.
- Вводить пароль и другие учетные данные, убедившись, что клавиатура находится вне поля зрения других лиц.
- При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Завершение сеанса> или нажать комбинацию клавиш Win+L.
- Размещать устройства вывода (отображения) информации (экран монитора автоматизированного рабочего места и другие средства визуального отображения защищаемой информации, печатающие устройства (принтеры, плоттеры и иные устройства), аудиоустройства, многофункциональные устройства), так чтобы исключить несанкционированный просмотр защищаемой информации.
- Учет, размножение, обращение печатных материалов, содержащих сведения конфиденциального характера и персональные данные, проводить в соответствии с требованиями Инструкции по делопроизводству.
- При обнаружении различных неисправностей в работе компьютерной техники или информационной системы, недокументированных свойств в программном обеспечении, нарушений целостности пломб (наклеек, печатей), несоответствии номеров на аппаратных средствах сообщить Администратору информационной системы, Администратору безопасности информации и руководителю структурного подразделения.

- Принимать меры по реагированию, в случае возникновения нештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах, возложенных на него функций.
- Своевременно выявлять попытки посторонних лиц получить сведения о защищаемой информации и персональных данных.
- Немедленно принимать меры по предупреждению разглашения защищаемой конфиденциальной информации и персональных данных, а также возможной их утечки при выявлении фактов утраты или недостачи удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

2.2. Пользователю информационной системы **запрещается**:
- использовать в личных целях конфиденциальную информацию и персональные данные, ставшие известными вследствие выполнения трудовых обязанностей;
- копировать конфиденциальную информацию и персональные данные на машинные носители без разрешения руководителя подразделения, а также фотографировать защищаемую информацию;
- самостоятельно устанавливать, тиражировать, или модифицировать программное и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к папкам на ПЭВМ;
- подключать к ПЭВМ и оборудованию, подключенному к информационной системе, личные машинные носители информации и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- обрабатывать на ПЭВМ информацию и выполнять работы, не предусмотренные функциональными обязанностями и перечнем прав пользователя по доступу к информационной системе;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам информационной системы;
- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации (при наличии), машинные носители и распечатки, содержащие конфиденциальную информацию и персональные данные;
- привлекать посторонних лиц для производства ремонта или настройки ПЭВМ, без согласования с Администратором информационной системы и с Администратором безопасности информации.

III. Права Пользователя информационной системы

3.1. Пользователь информационной системы имеет **право**:
- Знакомиться с документами, определяющими правила и порядок работы в информационной системе.
- Вносить на рассмотрение непосредственного руководителя структурного подразделения, Администратора информационной системы и Администратора безопасности информации предложения по совершенствованию работы, связанной с исполнением обязанностей в соответствии с настоящей инструкцией и функционированию информационной системы.

- Требовать от непосредственного руководителя структурного подразделения, Администратора информационной системы и Администратора безопасности информации, обеспечение организационно - технических условий, необходимых для исполнения обязанностей в соответствии с настоящей инструкцией.

IV. Ответственность Пользователя информационной системы

4.1. Пользователь информационной системы несет ответственность:

- За разглашение информации конфиденциального характера и персональных данных, нарушение порядка обращения с документами и машинными носителями информации, содержащими такую информацию, а также за нарушение режима защиты, обработки и порядка использования этой информации.
- За нарушение функционирования информационной системы и ПЭВМ, оборудования, входящего в состав информационной системы, вследствие ненадлежащего исполнения своих обязанностей.
- За несвоевременное уведомление непосредственного руководителя подразделения, Администратора информационной системы и Администратора безопасности информации о случаях нарушения правил пользования ресурсами информационной системы и случаев несанкционированного доступа к информации, обрабатываемой в информационной системе.

4.2. Пользователь информационной системы привлекается к ответственности:

- За ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей инструкцией - в пределах, установленных действующим законодательством Российской Федерации.
- За разглашение информации, охраняемой законодательством Российской Федерации.
- За правонарушения, совершенные в процессе своей деятельности - в пределах, установленных действующим административным, уголовным и гражданским законодательством Российской Федерации.
- За причинение материального ущерба - в пределах, установленных действующим законодательством Российской Федерации.

Приложение № 6
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Инструкция
по обеспечению безопасности конфиденциальной информации и персональных данных при возникновении нештатных ситуаций при эксплуатации информационной системы

I. Общие положения

1.1. Настоящая инструкция определяет действия работников Администрации Южского муниципального района (далее Администрация) в случае возникновения нештатных ситуаций в процессах обработки персональных данных в информационной системе.

1.2. Положения инструкции обязательны для исполнения всеми должностными лицами Администрации в части выполнения вмененных им обязанностей.

1.3. Общими требованиями ко всем работникам Администрации, в случае возникновения нештатной ситуации являются:

- работник, обнаруживший нештатную ситуацию, немедленно ставит в известность своего непосредственного руководителя и Администратора безопасности информации;
- Администратор безопасности информации обязан проводить анализ ситуации и, в случае невозможности исправить положение, ставит в известность руководителя Администрации.

Кроме этого, Администратор безопасности информации для локализации (блокирования) проявлений угроз информационной безопасности может привлекать пользователей информационной системы Администрации, а также Администратора информационной системы;

- по факту возникновения нештатной ситуации и выяснению причин ее проявления проводится служебное расследование.

II. Действия пользователей информационной системы при возникновении нештатных ситуаций

2.1. Сбой программного обеспечения

2.1.1. Администратор безопасности информации совместно с Администратором информационной системы выясняют причину сбоя программного обеспечения. Если привести систему в работоспособное состояние своими силами (в том числе после консультации с разработчиками программного обеспечения) не удалось, копия акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику программного обеспечения для устранения причин, приведших к сбою. О произошедшем инциденте Администратор безопасности информации сообщает руководителю Администрации для принятия решения.

2.2. Отключение электропитания технических средств информационной системы

2.2.1. Администратор безопасности информации совместно с Администратором информационной системы проводят анализ на наличие потерь и (или) разрушения данных и программного обеспечения, а также проверяют работоспособность оборудования. В случае необходимости производится восстановление программного обеспечения и данных из последней резервной копии с составлением акта. О произошедшем инциденте Администратор безопасности информации сообщает руководителю Администрации для принятия решения.

2.3. Выход из строя технических средств информационной системы

2.3.1. Администратор информационной системы совместно с Администратором безопасности информации выполняют мероприятия по немедленному вводу в действие резервной рабочей станции для обеспечения непрерывной работы информационной системы.

2.3.2. О выходе из строя рабочей станции Администратор информационной системы, ответственный за эксплуатацию рабочей станции, сообщает руководителю Администрации.

2.3.3. При необходимости производятся работы по восстановлению программного обеспечения и данных из резервных копий с составлением акта. О произошедшем инциденте Администратор безопасности информации сообщает руководителю Администрации для принятия решения.

2.4. Потеря данных

2.4.1. При обнаружении потери данных Администратор информационной системы проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность программного обеспечения, целостность и работоспособность оборудования).

2.4.2. При необходимости Администратором информационной системы производится восстановление программного обеспечения и данных из резервных копий с составлением акта. О произошедшем инциденте Администратор информационной системы сообщает Администратору безопасности информации. Администратор безопасности информации сообщает руководителю Администрации для принятия решения.

2.5. Обнаружение вредоносной программы в программной среде средств автоматизации информационной системы

2.5.1. При обнаружении вредоносной программы (ВП) производится её локализация с целью предотвращения её дальнейшего распространения. Администратором информационной системы и Администратором безопасности информации проводится анализ состояния рабочей станции.

2.5.2. В результате анализа может быть предпринята попытка сохранения данных, так как после перезагрузки рабочей станции данные могут быть потеряны. После успешной ликвидации ВП сохранённые данные подвергаются повторной проверке на наличие ВП. Кроме того, при обнаружении ВП следует руководствоваться инструкцией по эксплуатации применяемого антивирусного программного обеспечения.

2.5.3. После ликвидации ВП, проводится внеочередная проверка на всех средствах информационной системы и машинных носителях информации, с применением обновлённых антивирусных баз. При необходимости производится восстановление программного обеспечения и данных из резервных копий с составлением акта.

2.5.4. По факту появления ВП в локальной вычислительной сети проводится служебное расследование. Решение о необходимости проведения служебного расследования принимается руководителем Администрации.

2.6. Утечка информации

2.6.1. При обнаружении утечки информации ставится в известность Администратор безопасности информации и начальник структурного подразделения. По факту инициируется процедура служебного расследования. Если утечка информации произошла по техническим причинам, проводится анализ защищённости процессов информационной системы и, если необходимо, принимаются меры по устранению каналов утечки и предотвращению их возникновения.

2.7. Взлом операционной системы средств автоматизации информационной системы (несанкционированное получение доступа к ресурсам операционной системы)

2.7.1. При обнаружении взлома рабочей станции ставится в известность руководитель Администрации.

2.7.2. По возможности производится временное отключение рабочей станции. Возможен временный переход на резервную рабочую станцию.

2.7.3. Администратором информационной системы проверяется целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения. Администратором информационной системы проводится анализ состояния файлов - скриптов и журналов, производится смена всех паролей, которые имели отношение к данной рабочей станции.

2.7.4. В случае необходимости Администратором информационной системы производится восстановление программного обеспечения и восстановление данных из эталонного архива и резервных копий с составлением акта.

2.7.5. По результатам анализа ситуации проверяется вероятность проникновения несанкционированных программ в рабочую станцию.

2.8. Попытка несанкционированного доступа (НСД)

2.8.1. При попытке НСД, Администратором информационной системы и Администратором безопасности информации проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости (есть реальная угроза НСД), принимаются меры по предотвращению НСД.

2.8.2. Проводится внеплановая смена паролей. В случае появления обновлений программного обеспечения, устраняющих уязвимости системы безопасности, Администратором информационной системы устанавливаются такие обновления.

2.8.3. По факту попытки НСД проводится служебное расследование. Решение о необходимости проведения служебного расследования принимается руководителем Администрации.

2.8.4. В случае установления в ходе служебного расследования факта, осуществления попытки НСД со стороны внешних по отношению к информационной системе субъектов, лицами, уполномоченными на проведение такого расследования, принимаются меры по фиксации и документированию факта инцидента и готовятся материалы для передачи в компетентные органы дознания для проведения предварительного расследования, установления субъекта-нарушителя, определения наличия состава преступления и принятия решения о возбуждении уголовного дела.

2.9. Компрометация ключевой информации (паролей доступа)

2.9.1. При компрометации ключевой информации (пароля доступа) Администратором безопасности информации проводится смена пароля, анализируется ситуация на наличие последствий компрометации и принимаются необходимые меры по минимизации возможного (или нанесённого) ущерба.

2.9.2. О произошедшем инциденте Администратор безопасности информации сообщает руководителю Администрации для принятия решения.

2.10. Физическое повреждение или хищение оборудования технических средств информационной системы

2.10.1. Работником, обнаружившим физическое повреждение элементов информационной системы, ставится в известность: непосредственный руководитель, Администратор безопасности информации и Администратор информационной системы.

2.10.2. Администратором информационной системы совместно с Администратором безопасности информации проводится анализ с целью оценки возможности утечки или повреждения информации. Определяется причина повреждения элементов информационной системы и возможные угрозы информационной безопасности.

2.10.3. О факте повреждения элементов информационной системы Администратор безопасности информации докладывает руководителю Администрации.

2.10.4. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование.

2.10.5. Администратором информационной системы проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.10.6. При необходимости Администратором информационной системы проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.11. Невыполнение установленных правил информационной безопасности (правил работы в информационной системе), использование информационной системы с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации

2.11.1. Работником, обнаружившим невыполнение установленных правил информационной безопасности, использование информационной системы с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации, ставится в известность: непосредственный руководитель и Администратор безопасности информации.

2.11.2. Администратором безопасности информации проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента.

2.11.3. Об обнаруженном факте Администратор безопасности информации докладывает руководителю Администрации.

2.11.4. При необходимости по решению руководителя Администрации по фактам выявленных нарушений проводится служебное расследование.

2.12. Ошибки пользователей

2.12.1. В случае возникновения сбоя, связанного с ошибками пользователей, руководитель структурного подразделения Администрации, в котором произошёл инцидент, ставит в известность Администратора безопасности информации и Администратора информационной системы.

2.12.2. Администратором безопасности информации совместно с Администратором информационной системы проводятся анализ с целью оценки возможности утечки или повреждения информации.

Определяются возможные угрозы информационной безопасности в результате инцидента и необходимость восстановления программного обеспечения и данных.

2.12.3. При необходимости Администратором информационной системы проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.12.4. В случае нанесения Администрации значительного ущерба вследствие ошибок пользователей, проводится служебное расследование.

2.13. Отказ в обслуживании

2.13.1. Пользователем, обнаружившим отказ в обслуживании, ставится в известность; непосредственный руководитель, Администратор безопасности информации и Администратор информационной системы.

2.13.2. Администратором информационной системы и Администратором безопасности информации проводится анализ с целью определения причин, вызвавших отказ в обслуживании.

2.13.3. Администратором информационной системы проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.13.4. При необходимости, Администратором информационной системы проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.13.5. О причинах инцидента и принятых мерах Администратор информационной системы информирует Администратора безопасности информации и руководителя Администрации.

2.14. Несанкционированные изменения состава программных и аппаратных средств (конфигурации) информационной системы

2.14.1. В случае обнаружения несанкционированного изменения состава программных и аппаратных средств (конфигурации) информационной системы Администратором безопасности информации проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента.

2.14.2. Администратором информационной системы проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта, а также (при необходимости) проверка на наличие компьютерных ВП.

2.14.3. Об инциденте Администратор безопасности информации докладывает руководителю Администрации.

2.15. Техногенные и природные проявления нештатных ситуаций

2.15.1. При стихийном бедствии, пожаре или наводнении, грозящем уничтожению или повреждению информации (данных), работнику, обнаружившему факт возникновения нештатной ситуации:

- немедленно оповестить других работников и принять все меры для самостоятельной оперативной защиты помещения;
- немедленно позвонить в соответствующие службы помощи (пожарная охрана, служба спасения и т.д.);
- немедленно сообщить своему непосредственному руководителю и Администратору безопасности информации.

2.15.2. После оперативной ликвидации причин, вызвавших пожар или наводнение, назначается внутренняя комиссия по устранению последствий инцидента.

2.15.3. Комиссия определяет ущерб (состав и объем уничтоженных оборудования и информации) и причины, по которым произошло происшествие, а также выявляет виновных.

Источники угроз

Технологические угрозы	
1	Пожар в здании
2	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
3	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
4	Химический выброс в атмосферу
Внешние угрозы	
5	Массовые беспорядки
6	Сбои общественного транспорта
7	Эпидемия
8	Массовое отравление персонала
Стихийные бедствия	
9	Удар молнии
10	Сильный снегопад
11	Сильные морозы
12	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
13	Затопление водой в период паводка
14	Наводнение, вызванное проливным дождем
15	Торнадо
16	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
Телеком и ИТ угрозы	
17	Сбой системы кондиционирования
18	Сбой ИТ – систем
Угроза, связанная с человеческим фактором	
19	Ошибка персонала, имеющего доступ к серверу (рабочей станции)
20	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
Угрозы, связанные с внешними поставщиками	
21	Отключение электроэнергии
22	Сбой в работе интернет-провайдера
23	Физический разрыв внешних каналов связи

Приложение № 7
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Инструкция
по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационной системы Администрации Южского муниципального района

I Общие положения

С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику Администрации Южского муниципального района (далее Администрация), также – Учреждение), допущенному к работе с конкретной подсистемой информационной системы Учреждения, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в информационной системе.

В случае необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе в информационной системе одного и того же имени пользователя запрещено.

II Правила по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационной системы

Процедура регистрации (создания учетной записи пользователя) для сотрудника Учреждения и предоставления (или изменения, прекращения) ему прав доступа к ресурсам информационной системы инициируется заявкой руководителя подразделения, в котором работает данный сотрудник.

Форма заявки:

_____

_____

(должность, ФИО Администратора безопасности информации)

(резолюция руководителя _____
(Администрации)

ЗАЯВКА
на внесение изменений в списки пользователей информационной системы и наделение пользователей полномочиями доступа к ресурсам системы

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

_____
(ненужное зачеркнуть)

_____
(должность с указанием подразделения)

_____
(фамилия имя и отчество сотрудника)

предоставив ему полномочия, необходимые (лишив его полномочий, необходимых)
(ненужное зачеркнуть)
для решения задач:

_____
(список задач)

_____
_____
_____
_____
_____

на рабочей станции:

_____
(условное наименование АРМ подразделения согласно формуляра)

_____
_____

Начальник

_____
(наименование заказывающего подразделения)

«___» _____ 20__ г. _____ _____
(подпись) *(фамилия)*

Обратная сторона заявки

Присвоено имя _____ и предоставлены полномочия, необходимые для решения следующих задач на АРМ:

Наименование АРМ (в соответствии с формуляром АРМ)	Наименование задачи (по перечню задач)

Администратор информационной системы

_____
(подпись, фамилия)
«___» _____ 20__ г.

Администратор безопасности информации
(должность)

_____
(подпись, фамилия)
«___» _____ 20__ г.

Имя, личные ключевые дискеты (при наличии) и начальные значения паролей получил, о порядке смены пароля при первом входе в систему проинструктирован.

Пользователь

_____
(подпись, фамилия)

«___» _____ 20__ года

В заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя информационной системы, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам информационной системы ранее зарегистрированного пользователя);
- должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;
- имя пользователя (учетной записи) данного сотрудника;
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач на рабочей станции).

Наименования задач должны указываться в соответствии с выполняемыми обязанностями (функциями), решаемыми задачами, наименования АРМ - в соответствии с формулярами терминальных рабочих станций.

Заявку визирует руководитель Администрации, утверждая тем самым необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных задач ресурсам информационной системы.

Затем Администратор безопасности информации подписывает задание Администратору информационной системы на внесение необходимых изменений в списки пользователей соответствующих подсистем.

ЗАДАНИЕ
на внесение изменений в списки пользователей информационной системы

Администратору информационной системы

_____
(фамилии и инициалы исполнителей)
_____

_____
Произвести изменения в списках пользователей
баз данных

_____
_____
(ФИО, должность Администратора безопасности информации)

«___» _____ 20__ г.

Администратор безопасности информации в соответствии с формулярами задач и Инструкцией Администратора безопасности информации производит необходимые операции по созданию нового пользователя, присвоению ему начального значения пароля и прав доступа к ресурсам указанных в заявке рабочей станции, включению его в соответствующие задачам системные группы пользователей и другие необходимые операции.

На основании заявки и задания Администратор информационной системы, в соответствии с формулярами задач, которые хранятся в архиве эталонных дистрибутивов программ, и документацией на средства защиты сетевых операционных систем, производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и заявленных прав доступа к ресурсам информационной системы, включению его в соответствующие задачам группы пользователей и другие необходимые действия. Учетные записи всех пользователей должны быть «привязаны» к рабочей станции.

После внесения изменений в списки пользователей Администратор безопасности информации совместно с Администратором информационной системы должен обеспечить соответствующие категориям защиты рабочей станции настройки и проверить правильность настроек программного обеспечения.

По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания за подписями исполнителей - Администратора безопасности информации и Администратора информационной системы.

Сотруднику, зарегистрированному в качестве нового пользователя системы, сообщается соответствующее имя пользователя, начальное значение пароля, которое он обязан сменить при первом же входе в систему (при первом подключении к информационной системе).

Исполненная заявка передается в подразделение и хранится у Администратора безопасности информации.

Они могут впоследствии использоваться:

- для восстановления учётных записей и полномочий пользователей после аварий в информационной системе;
- для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам системы при разборе конфликтных ситуаций;
- для проверки сотрудниками правильности настройки средств разграничения доступа к ресурсам системы.

В информационной системе для управления доступом субъектов доступа к объектам доступа должны быть реализованы установленные в Учреждении методы управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа.

Методы управления доступом реализуются в зависимости от особенностей функционирования информационной системы, с учетом угроз безопасности информации и должны включать один или комбинацию следующих методов:

- дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа;
- ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности);
- мандатный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе сопоставления классификационных меток каждого субъекта доступа и каждого объекта доступа, отражающих классификационные уровни субъектов доступа и объектов доступа,

являющиеся комбинациями иерархических и не иерархических категорий.

Типы доступа должны включать операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению пользователем (группе пользователей) или запускаемому от его имени процессу при доступе к объектам доступа.

Правила разграничения доступа реализуются на основе утвержденных списков доступа или матриц доступа и должны обеспечивать управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа.

В информационной системе должно быть обеспечено разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями (функциями), фиксирование в организационно-распорядительных документах по защите информации (документирование) полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей).

Администратор безопасности информации при назначении прав и привилегий пользователям и запускаемым от их имени процессам, исходит из минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями.

III Ответственность

За нарушение требований настоящей инструкции и других документов, регламентирующих порядок и правила работы в информационной системе, виновные лица привлекаются к дисциплинарной ответственности.

Приложение № 8
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Инструкция
по организации парольной защиты

I. Общие положения

1.1. Данная Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей на объекте информатизации автоматизированной системе Администрации Южского муниципального района (далее Администрация), предназначенных для обработки информации ограниченного распространения, а также контроль за действиями пользователей при работе с паролями.

II. Порядок работы по обеспечению парольной защиты

2.1. Организационное и техническое обеспечение процессов генерации, создания, присвоения, использования, смены и прекращения, уничтожения идентификаторов пользователей и устройств во всех подсистемах автоматизированной системы и контроль за действиями пользователей при работе с паролями возлагается на Администратора безопасности информации.

Администратор безопасности информации отвечает за формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство, присвоение идентификатора пользователю и (или) устройству, предотвращение повторного использования идентификатора пользователя и (или) устройства в течение установленного в Администрации периода времени, блокирование идентификатора пользователя после установленного времени неиспользования.

2.2. Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

- длина пароля должна быть не менее шести символов;
- в числе символов пароля обязательно должны присутствовать символы из следующих категорий: строчные буквы латинского алфавита, прописные буквы латинского алфавита, десятичные цифры (алфавит пароля не менее 60 символов);
- символы паролей должны вводиться в режиме латинской раскладки клавиатуры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ADMIN, SECRET, USER и т.п.);
- использование трех и более подряд идущих на клавиатуре символов, набранных в одном регистре, недопустимо;

- использование двух и более подряд одинаковых символов недопустимо;
- смена паролей не более чем через 120 дней;
- при смене пароля новое значение должно отличаться от предыдущего минимум в 6-ти символах;
- новый пароль не должен совпадать с одним из 10-ти предыдущих паролей;
- пользователь обязан сохранять в тайне свой личный пароль
- максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток;
- блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за разглашение парольной информации.

2.3. Полная плановая смена паролей пользователей должна проводиться регулярно.

2.4. При смене пароля Администратором безопасности информации производится тестирование функций средств защиты информации от несанкционированного доступа путем ввода с клавиатуры заведомо ложного пароля, при наличии считывателя – предъявления стороннего идентификатора.

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

2.6. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий Администратора безопасности информации (увольнение, переход на другую работу внутри Администрации и другие обстоятельства).

2.7. В информационной системе должна осуществляться защита аутентификационной информации в процессе её ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

Защита обратной связи «система - субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации.

Вводимые символы пароля могут отображаться условными знаками «*», «□» или иными знаками.

2.8. В информационной системе должна осуществляться идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа.

2.9. Администратор безопасности информации устанавливает и реализует следующие функции управления учетными записями пользователей:

- определение типа учетной записи (внутреннего пользователя, внешнего пользователя;

системная, приложения, гостевая (анонимная), временная и (или) иные типы записей);

- объединение учетных записей в группы (при необходимости);
- верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;
- заведение, активация, блокирование и уничтожение учетных записей пользователей;
- пересмотр и, при необходимости, корректировка учетных записей пользователей с периодичностью, установленной в Учреждении;
- порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов;
- оповещение Администратора информационной системы, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;
- уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;
- предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе.

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

2.10. В случае компрометации (утеря, передача парольной информации) личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п. 2.4 или п. 2.5 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

2.11. Хранение сотрудником (исполнителем) значений своих паролей на любом носителе не допускается.

2.12. Повседневный контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на руководителей подразделений, периодический контроль на Администратора безопасности информации, и лица, ответственного за организацию обработки персональных данных в Администрации.

Приложение № 9
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Инструкция
по организации резервного копирования

I. Общие положения

1.1. Настоящая Инструкция устанавливает основные требования к организации резервного копирования (восстановления) программ и данных, хранящихся в информационной системе Администрации Южского муниципального района (далее Администрация), а также к резервированию аппаратных средств.

1.2. Настоящая Инструкция разработана с целью:

- определения категории информации, подлежащей обязательному резервному копированию;
- определения процедуры резервирования данных для последующего восстановления работоспособности информационных систем при полной или частичной потере информации, вызванной сбоями или отказами аппаратного, или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);
- определения порядка восстановления информации в случае возникновения такой необходимости;
- упорядочения работы и определения ответственности должностных лиц, связанной с резервным копированием и восстановлением информации.

1.3. Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности информационной системы в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

1.4. Резервному копированию подлежит информация следующих основных категорий:

- персональная информация пользователей (личные каталоги) и групповая информация (общие каталоги подразделений);
- информация, обрабатываемая пользователями в информационной системе, а также информация, необходимая для восстановления работоспособности информационной системы, в т.ч. систем управления базами данных (СУБД) общего пользования и справочно-информационные системы общего использования;
- рабочие копии установочных компонентов программного обеспечения общего назначения и специализированного программного обеспечения информационной системы, СУБД;

- информация, необходимая для восстановления систем управления базами данных информационной системы;
- регистрационная информация системы информационной безопасности информационной системы;
- другая информация информационной системы, по мнению пользователей и Администратора безопасности информации, являющаяся критичной для работоспособности информационной системы.

1.5. Резервное копирование автоматизированных систем производится на основании следующих данных:

- состав и объем копируемых данных, необходимая периодичность проведения резервного копирования по форме:

Перечень резервируемой информации

№ п/п	Резервируемые ресурсы	Оценочный объем данных, Гб	Адрес хранения информации	Срок хранения резервной копии	Примечание*
1	2	3	4	5	6
1					
2					

* Описание резервируемой информации

- максимальный срок хранения резервных копий;
- требований к надежности и защищенности хранения резервных копий;
- требований к резервируемым аппаратным средствам информационной системы (при необходимости, в случае предъявления высоких требований к обеспечению доступности данных, обрабатываемых в информационной системе и значительного ущерба Администрации при нарушении заданных характеристик безопасности информации).

1.6. Машинным носителям информации, содержащим резервную копию, присваивается гриф конфиденциальности по наивысшему грифу содержащихся на них сведений.

1.7. Резервные копии хранятся вне пределов помещения, в котором установлена рабочая станция, доступ к резервным копиям ограничен. К носителям информации, содержащим резервные копии, а также к резервируемым программным и аппаратным средствам допускаются только работники Администрации, указанные в Списке лиц, имеющих доступ к резервируемым программным и аппаратным средствам информационной системы.

Список лиц, имеющих доступ к резервируемым программным и аппаратным средствам информационной системы

№ п/п	Выполняемая роль	ФИО ответственного работника
1	2	3
1	Первоначальная настройка системы резервного копирования (создание медиа-сетов, расписаний, selection lists, оповещений). Запуск в эксплуатацию системы	

№ п/п	Выполняемая роль	ФИО ответственного работника
1	2	3
	резервного копирования	
2	Внесение существенных изменений в настройку системы резервного копирования	
3	Анализ логов резервного копирования, отслеживание необходимости изменений настроек резервного копирования, обеспечение ротации носителей	
4	Ротация носителей, проверка корректности резервной копии, обеспечения хранения резервной копии вне помещения на случай катастрофы	

Список лиц формируется на основании письменной заявки руководителя подразделения, согласованной с Администратором безопасности информации. Изменение прав доступа к резервируемым техническим средствам, массивам и носителям информации производится на основании заявки руководителя подразделения, согласованной с Администратором безопасности информации.

О выявленных попытках несанкционированного доступа к резервируемой информации и аппаратным средствам, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается руководителю Администрации в течение рабочего дня после обнаружения указанного события.

II. Общие требования к резервному копированию

2.1. В настоящей Инструкции резервного копирования описываются действия при выполнении следующих мероприятий:

- резервное копирование с указанием конкретных резервируемых данных и аппаратных средств (в случае необходимости);
- контроль резервного копирования:
- хранение резервных копий;
- полное или частичное восстановление данных.

2.2. Архивное копирование резервируемой информации производится при помощи специализированных программно-аппаратных систем резервного копирования, программный и аппаратный состав которых обеспечивает выполнение требования к резервному копированию, приведенные в п. 1.5. Система резервного копирования обеспечивает производительность, достаточную для сохранения информации, указанной в п. 1.4, в установленные сроки и с заданной периодичностью.

2.3. Требования к техническому обеспечению систем резервного копирования:

- это комплекс взаимосвязанных технических средств, обеспечивающих процессы сбора, передачи, обработки и хранения информации, основывающийся на единой технологической платформе;
- имеет возможность расширения (замены) состава технических средств, входящих в комплекс, для улучшения их эксплуатационно-технических характеристик по мере возрастания объемов обрабатываемой информации:
- обеспечивает выполнение функций, перечисленных в п. 2.1;

- средства вычислительной техники отвечают действующим на момент сертификации российским и международным стандартам и рекомендациям.

2.4. Требования к программному обеспечению систем резервного копирования:

- лицензионное системное программное обеспечение и программное обеспечение резервного копирования;
- программное обеспечение резервного копирования обеспечивает простоту процесса инсталляции, конфигурирования и сопровождения.

2.5. Сопровождение системы резервного копирования возлагается на Администратора информационной системы, который обязан следить за работоспособностью программных и аппаратных средств, осуществляющих архивное копирование, в соответствии с инструкцией по эксплуатации.

2.6. Предварительный учет машинных носителей архивных копий производится в отдельном журнале учета машинных носителей для архивного копирования, который находится у Администратора безопасности информации.

Журнал учета машинных носителей для архивного копирования информации

№ п/п	Носитель (маркировка)	Кому выдан (ФИО работника, должность, подразделение)	Получен (дата, подпись)	Возвращен (дата, подпись)	Уничтожен (причина, ФИО работника, должность, подразделение, дата, подпись)
1	2	3	4	5	6
1					
2					
3					

Все машинные носители с архивными копиями маркируются, на них указывается предназначение носителя.

В случае неотделимости носителей архивной информации от системы резервного копирования допускается их не маркировать и учитывать всю систему как одно целое.

2.7. Хранение отдельных машинных носителей архивных копий организуется в отдельном от используемых данных помещении. Физический доступ к архивным копиям строго ограничен.

Контроль за физическим доступом возлагается на Администратора безопасности информации.

2.8. Доступ к носителям архивных копий имеют только Администратор безопасности информации и Администратор информационной системы, которые несут персональную ответственность за сохранность архивных копий и невозможность ознакомления с ними лиц, не имеющих на то права.

2.9. Машинные носители для архивных копий изымаются для работы только работником, непосредственно осуществляющим резервное копирование, под роспись в журнале учета машинных носителей архивных копий. Передача машинных носителей с архивными копиями кому бы то ни было, без документального оформления не допускается.

2.10. Уничтожение отделяемых машинных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательной записью в журнале их учета.

III. Ответственность за состояние резервного копирования

3.1. Ответственность за периодичность и полноту резервного копирования, а также состояние системы резервного копирования возлагается на Администратора информационной системы, осуществляющего резервное копирование.

3.2. Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением настоящей Инструкции, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на Администратора безопасности информации.

3.3. В случае обнаружения попыток несанкционированного доступа к носителям архивной информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается руководителю Администрации в течение рабочего дня после обнаружения указанного события.

IV. Периодичность резервного копирования

4.1. Резервное копирование специализированного программного обеспечения производится при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.

4.2. Резервное копирование открытой информации делается не позднее чем через сутки после её изменения, но не реже одного раза в месяц.

4.3. Информация, содержащаяся в постоянно изменяемых базах данных Администрации, сохраняется в соответствии со следующим графиком:

- ежедневно проводится копирование изменённой и дополненной информации. Носители с ежедневной информацией должны храниться в течение недели;
- еженедельно проводится резервное копирование всей базы данных. Носители с еженедельными копиями хранятся в течение месяца;
- ежемесячно производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится постоянно.

V. Контроль результатов резервного копирования

5.1. Контроль результатов всех процедур резервного копирования осуществляется Администратором безопасности информации и Администратором информационной системы, в срок до 16 часов рабочего дня, следующего за установленной датой выполнения этих процедур. В случае обнаружения ошибки лицо, ответственное за контроль результатов, сообщает руководителю Администрации до 17 часов текущего рабочего дня.

5.2. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, осуществляется ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем, располагающих необходимыми объемами дискового пространства для её хранения.

VI. Ротация носителей резервной копии

6.1. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации информационной системы в случае отказа любого из устройств резервного копирования.

6.2. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются Администратором информационной системы. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек. Информация ограниченного доступа с носителей, которые перестают использоваться в системе резервного копирования, уничтожается.

VII. Восстановление информации из резервных копий

7.1. В случае необходимости, восстановление данных из резервных копий производится Администратором информационной системы.

7.2. Восстановление данных из резервных копий происходит в случае её исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок пользователей и аппаратных сбоев.

7.3. Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

7.4. Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

7.5. Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.

7.6. При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

Приложение № 10
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы Администрации Южского муниципального района

I. Общие положения

Настоящей инструкцией регламентируется взаимодействие подразделений Администрации Южского муниципального района (далее Администрация, также - Учреждение) по обеспечению безопасности информации при проведении модификаций программного обеспечения, технического обслуживания средств вычислительной техники и при возникновении нештатных ситуаций в работе информационной системы.

Все изменения конфигурации технических и программных средств защищенных рабочих станций и серверов информационной системы Администрации должны производиться только на основании заявок начальников структурных подразделений либо заявки Администратора безопасности информации, согласованных с руководителем Администрации.

Право внесения изменений в конфигурацию аппаратно-программных средств защищенных рабочих станций и серверов информационной системы предоставляется:

- в отношении системных и прикладных программных средств, а также в отношении аппаратных средств - Администратору информационной системы;
- в отношении программно-аппаратных средств телекоммуникации - Администратору информационной системы;
- в отношении программно-аппаратных средств защиты - Администратору безопасности информации.

Изменение конфигурации аппаратно-программных средств защищенных рабочих станций и серверов кем-либо, кроме перечисленных уполномоченных сотрудников, запрещено.

Право внесения изменений в конфигурацию аппаратно-программных средств АРМ и серверов информационной системы предоставляется Администратору безопасности информации или Администратору информационной системы (на основании служебных записок).

Процедура внесения изменений в конфигурацию аппаратных и программных средств защищенного АРМ/сервера информационной системы инициируется заявкой начальника подразделения

.

Формы заявок:

_____ *(указывается должность Администратора безопасности информации)*

(резолюция руководителя
(_____ *(*Администрации*)*
« __» _____ 20 _ года

ЗАЯВКА
на внесение изменений в состав аппаратно-программных средств информационной системы

Прошу произвести следующие изменения конфигурации аппаратно - программных средств автоматизированной подсистемы
_____ -
(наименование подразделения)
развернуть новую рабочую станцию и установить на (обновить на / снять с) нее _____ компоненты, необходимые для решения следующих задач:
_____
_____
(наименование задач согласно перечню)
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Начальник _____
(наименование подразделения заказчика)

«___» _____ 20__ г. _____ _____
(подпись) *(фамилия и инициалы)*

_____ *(указывается должность Администратора безопасности информации)*

(резолюция руководителя
(_____ *(*Администрации)
« __» _____ 20 _ года

ЗАЯВКА
на внесение изменений в состав аппаратно-программных средств ИС

В связи с необходимостью

_____
(обоснование причины внесения изменений)

_____

_____

прошу допустить установленным порядком сотрудников:

_____
_____
(фамилии исполнителей)

_____

для выполнения необходимых работ в

_____
(наименование подразделения)

по установке рабочей станции (обновлению/снятию с АРМ _____ компонентов), необходимых для решения следующих задач:

_____
_____
(наименование задач согласно перечню)

_____
_____
_____
_____
_____
_____
_____
_____
_____

_____

Начальник отдела

«___» _____ 20__ г. _____ _____
(подпись) *(фамилия и инициалы)*

Обратная сторона заявки

Отметка о выполнении
(о внесении изменений в состав аппаратно-программных средств АС)

Рабочей группой в составе:

_____

_____

(фамилии исполнителей)

указанные в заявке изменения внесены (не внесены по следующей причине):

_____

(краткое пояснение причины)

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Изменения в формуляр АРМ (ссылка на данную заявку) внесены.

От отдела _____

_____

(подпись, фамилия)

Администратор информационной системы

_____

(подпись, фамилия)

«_____» _____ 20__ года

От отдела _____

_____

(подпись, фамилия)

Администратор безопасности информации

_____

(подпись, фамилия)

«_____» _____ 20__ года

Заявка, в которой требуется произвести изменения конфигурации АРМ/сервера, оформляется на имя Администратора безопасности информации. Служебная необходимость проведения указанных в заявке изменений подтверждается подписью руководителя Администрации.

Заявка Администратора информационной системы, который отвечает за плановое проведение изменений (обновлений версий) программного обеспечения и его компонентов, оформляется на имя Администратора безопасности информации.

В заявках могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств АРМ и серверов:

- установка в подразделении новой ПЭВМ (развертывание нового АРМ) /сервера;
- замена ПЭВМ (АРМ)/сервера;
- изъятие ПЭВМ (АРМ)/сервера;
- добавление устройства (узла, блока) в состав АРМ/сервера;
- замена устройства (узла, блока) в составе АРМ/сервера;
- изъятие устройства (узла, блока) из состава АРМ/сервера;
- установка (развертывание) на АРМ/сервере программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи на данном АРМ/сервере);
- обновление (замена) на конкретном АРМ/сервере программных средств, необходимых для решения определенной задачи (обновление версий, используемых для решения определенной задачи программ);
- удаление с АРМ/сервера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на АРМ/сервере).

В заявке указываются условное наименование АРМ/сервера в соответствии с формуляром. В случае развертывания нового АРМ/сервера его наименование в заявке указывать не требуется (оно устанавливается позднее при заполнении формуляра нового АРМ/сервера). Наименования задач указываются в соответствии с формулярами задач или перечнем задач архива эталонных дистрибутивов (АЭД), которые можно решать с использованием информационной системы.

Заключение о технической возможности осуществления затребованных изменений выдается Администратором информационной системы (на основании формуляров задач и формуляра, соответствующего АРМ/сервера).

Заключение о возможности совмещения решения новых задач (обработки информации) на указанном в заявке АРМ/сервере, в соответствии с требованиями по безопасности и на основе проведенного анализа потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных, выдается Администратором безопасности информации, которому заявка передается на согласование (одновременно с этим производится определение новых категорий защищенности указанного АРМ/сервера).

После чего заявка передается для непосредственного исполнения работ по внесению изменений в конфигурацию АРМ/сервера информационной системы.

Руководитель подразделения допускает уполномоченных сотрудников к внесению изменений в состав аппаратных средств и программного обеспечения только по предъявлении последними, утвержденной заявки на осуществление данных изменений.

Установка, изменение (обновление) и удаление системных и прикладных программных средств, производится уполномоченными сотрудниками.

Установка, снятие, и внесение необходимых изменений в настройки средств защиты информации от несанкционированного доступа (НСД) и средств контроля целостности файлов на АРМ/сервере, осуществляется организацией, имеющий лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

Работы производятся в присутствии Администратора безопасности информации и пользователя АРМ.

Подготовка модификаций программного обеспечения защищенных рабочих станций и серверов, тестирование, стендовые испытания и передача исходных текстов, документации и дистрибутивных носителей программ в архив эталонных дистрибутивов и другие необходимые действия производятся Администратором безопасности информации и Администратором информационной системы, согласно утвержденным инструкциям.

Установка или обновление подсистем информационной системы Учреждения должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

Установка (инсталляция) в информационной системе программного обеспечения (вида, типа, класса программного обеспечения) и (или) его компонентов осуществляется с учетом перечня программного обеспечения и (или) его компонентов, разрешенных руководителем Администрации к установке, и (или) перечнем программного обеспечения и (или) его компонентов, запрещенных к установке.

Указанные перечни программного обеспечения и (или) его компонентов разрабатываются в Учреждении для информационной системы в целом или для всех её устройств в отдельности.

Установка (инсталляция) в информационной системе программного обеспечения и (или) его компонентов должна осуществляться только от имени Администратора информационной системы.

Администратор информационной системы осуществляет периодический контроль установленного (инсталлированного) в информационной системе программного обеспечения на предмет соответствия его перечню программного обеспечения, разрешенному к установке в информационной системе, а также на предмет отсутствия программного обеспечения, запрещенного к установке.

После проведения модификации программного обеспечения и его компонентов на рабочей станции или сервере Администратор информационной системы проводит антивирусный контроль.

Установка и обновление общего программного обеспечения и его компонентов (системного, тестового и т.п.) на рабочей станции/сервере производится с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных

установленным порядком, а прикладного программного обеспечения и его компонентов – с эталонных копий программных средств, полученных из АЭД (при реализации сетевого архива эталонных дистрибутивов программ – из него). При необходимости (в случае установки части компонент на дисках) к работам привлекается Администратор информационной системы.

Все добавляемые программные и аппаратные компоненты должны быть предварительно, установленным порядком, проверены на работоспособность, а также отсутствие опасных функций.

После установки (обновления) программного обеспечения и его компонентов Администратор информационной системы должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с её (его) формуляром и совместно с Администратором безопасности информации и Пользователем АРМ, должен проверить работоспособность программного обеспечения и его компонентов и правильность настройки средств защиты.

После завершения работ по внесению изменений в состав аппаратных средств защищенного АРМ/сервера, его системный блок должен закрываться Администратором информационной системы – на ключ (при наличии штатных механических замков) и опечатываться (пломбироваться, защищаться специальной наклейкой) Администратором безопасности информации.

Уполномоченные сотрудники (Администратор информационной системы, Администратор безопасности информации) должны произвести запись в соответствующий журнал о факте вскрытия и опечатывания ПЭВМ/сервера, выполнения профилактических работ, установки и модификации аппаратных и программных средств АРМ/сервера, сделать отметку о выполнении (на обратной стороне заявки) и передать исполненную заявку для хранения вместе с формуляром рабочей станции/сервера.

Формат записей о фактах вскрытия и опечатывания ПЭВМ/сервера, выполнения профилактических работ, установки и модификации аппаратных и программных средств АРМ и серверов:

№ п/п	**Дата**	**Краткое описание выполненной работы (нештатной ситуации)**	**ФИО исполнителей и их подписи**	**ФИО ответственного пользователя АРМ, подпись**	**Подпись Администратора безопасности информации**	**Примечание (ссылка на заявку)**
1	**2**	**3**	**4**	**5**	**6**	**7**

При изъятии рабочей станции/сервера из подразделения, их передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как Администратор безопасности информации и Администратор информационной системы снимут с данной ПЭВМ/сервера средства защиты и предпримут необходимые меры для затирания

защищаемой информации, которая хранилась на ЖМД АРМ /сервера. Факт уничтожения данных, находившихся на ЖМД АРМ/сервера, оформляется актом за подписью Администратора безопасности информации и Администратора информационной системы.

Форма Акта:

АКТ
о затирании остаточной информации, хранившейся на диске компьютера

Все файлы, содержащие, подлежащую защите информацию, находившиеся на ЖМД №_____, передаваемого _____
(с какой целью)

_____
(Кому: должность, Ф.И.О.)

_____
—
системного блока ПЭВМ марки _____ серийный №_____
уничтожены (затерты) посредством программы _____.

Администратор безопасности информации

_____
(Ф.И.О.)

_____ _____
(подпись) *(дата)*

Администратор информационной системы

_____
(Ф.И.О.)

_____ _____
(подпись) *(дата)*

Доступ новых пользователей к решению задач с использованием вновь развернутого программного обеспечения и его компонентов (либо изменение их полномочий доступа) осуществляется согласно «Инструкции по внесению изменений в списки пользователей системы и наделению пользователей полномочиями доступа к ресурсам информационной системы Администрации.

Оригиналы заявок (документов), на основании которых производились изменения в составе технических или программных средств АРМ/ сервера, с отметками о внесении изменений в состав аппаратно-программных средств должны храниться вместе с оригиналом формуляра АРМ/сервера (у Администратора безопасности информации). Они могут использоваться:

- для восстановления конфигурации АРМ/сервера после аварий;

- для контроля правомерности установки на АРМ/сервер средств, для решения соответствующих задач при разборе конфликтных ситуаций;
- для проверки правильности установки и настройки средств защиты АРМ/сервера.

II. Экстренная модификация (обстоятельства форс-мажор)

В исключительных случаях (сбой программного обеспечения и его компонентов, не позволяющий продолжить работу), требующих безотлагательного изменения программного обеспечения и его компонентов, допускается корректировка программ непосредственно на АРМ/сервер. В данной ситуации Администратор информационной системы ставит в известность руководителя Администрации и Администратора безопасности информации о необходимости такого изменения. Факт внесения изменений в программное обеспечение и его компонентов фиксируется актом за подписью Администратора безопасности информации. В акте указывается причина модификации, перечисляются файлы, подвергшиеся изменению, и указывается лицо, проводившее изменения. При необходимости проводится изменение программного обеспечения и его компонентов загрузочного раздела АРМ. Если это необходимо, Администратор информационной системы вносит необходимые корректировки в настройки системы контроля целостности программного обеспечения и его компонентов рабочей станции. Факт модификации программного обеспечения, его компонентов и корректировки настроек системы защиты фиксируется в соответствующем журнале.

III. Порядок технического обслуживания и ремонта технических средств

Техническое обслуживание и ремонтные работы на технических средствах АРМ и серверов должны осуществляться только уполномоченными сотрудниками, назначенными ответственными за их обслуживание (сопровождение). Их вызов осуществляется сотрудниками подразделения, эксплуатирующего АРМ/сервер, при возникновении нештатных ситуаций.

К нештатным ситуациям относятся:

- выход из строя или неустойчивое функционирование узлов ПЭВМ или периферийных устройств (например, дисковода, принтера) АРМ/сервера;
- выход из строя системы электроснабжения АРМ/сервера.

Техническое обслуживание и регламентные работы могут проводиться в плановом порядке.

В этом случае работы проводятся на основании заявок, согласованных с руководителем Администрации.

Ответственность за соблюдение требований по обеспечению безопасности информации при проведении технического обслуживания и ремонтных работ на ПЭВМ возлагается на Администратора безопасности информации, Администратора информационной системы и руководителя подразделения.

Уполномоченные сотрудники имеют право доступа к АРМ и серверам для разбора нештатных ситуаций при обнаружении сбоев в их работе только для тестирования рабочей станции/сервера с использованием, установленных на АРМ тестовых средств.

О факте выполнения данных работ Администратор безопасности информации делает отметку в соответствующем журнале с указанием признаков проявления ситуации и содержания выполненных работ по ее устранению.

IV. Порядок проверки работоспособности системы защиты после установки (обновления) программных средств информационной системы и внесения изменений в списки пользователей

После установки (обновления) программных средств АРМ и серверов или внесения изменений в списки пользователей системы Администратор безопасности информации обязан проверить работоспособность АРМ/сервера и правильность настройки средств защиты, установленных на рабочей станции.

При установке нового (обновлении существующего) программного средства Администратор безопасности информации обязан:

- установить права доступа пользователей системы к файлам программного средства таким образом, как это указано в формуляре на программное средство (задачу);
- подсчитать контрольные суммы файлов программных средств (при наличии указаний в формуляре);
- если для пользователя, использующего установленное программное средство, установлен режим замкнутой программной среды, необходимо добавить в список разрешенных ему для запуска программ исполняемые модули данного пакета.

После осуществления данных действий необходимо проверить корректность функционирования системы защиты, для чего требуется произвести следующие действия:

- для каждого пользователя АРМ, для которого установлен режим замкнутой программной среды, требуется проверить работоспособность установленного программного средства и сохранение режима замкнутой программной среды;
- в режиме обычного пользователя необходимо проверить возможность удаления вновь установленных (обновленных) файлов.

Приложение № 11
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Инструкция по обеспечению безопасности персональных данных при их обработке в информационной системе Администрации Южского муниципального района

I. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с требованиями ст. 19 Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных», на основании Федерального закона РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановления Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных, Приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», внутренних документов, определяющих политику Администрации Южского муниципального района (далее Администрация) в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

1.2. Для обеспечения безопасности персональных данных необходимо исключить несанкционированный, в том числе случайный, доступ к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

1.3. В целях обеспечения безопасности персональных данных создается система защиты персональных данных (СЗПДн), которая должна обеспечивать конфиденциальность, целостность и доступность персональных данных при их обработке в информационной системе персональных данных (ИСПДн) во всех структурных элементах, на технологических участках обработки и во всех режимах функционирования информационной системы.

1.4. СЗПДн включает в себя организационные и технические меры, средства защиты информации, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных, а также используемые в ИСПДн информационные технологии.

1.5. Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационной системе, подлежат учету с использованием индексов или условных наименований и регистрационных номеров.

1.6. Помещение, в котором размещены объекты информатизации, содержащие ИСПДн, должны соответствовать требованиям по обеспечению их сохранности, пожарной безопасности, а также защиты от несанкционированного проникновения посторонних лиц.

1.7. Ответственность за безопасность персональных данных возлагается на лиц, допущенных к их обработке.

2. Организация работ по обеспечению безопасности персональных данных при их обработке с использованием средств автоматизации

2.1. Обеспечение безопасности перед началом обработки персональных данных:

2.1.1. К обработке персональных данных допускаются сотрудники, которые ознакомились с документами, определяющими политику Администрации, в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений, прошедшие или которые прошли обучение.

2.2.2. Перед началом обработки персональных данных необходимо обеспечить:

- соответствие средств защиты персональных данных классу информационной системы;
- отсутствие посторонних лиц в помещении, в котором ведется работа с персональными данными;
- сохранность и целостность носителей персональных данных;
- отсутствие возможности несанкционированного доступа к персональным данным;
- исправное состояние технических средств автоматизированной обработки и защиты персональных данных;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.2. Обеспечение безопасности персональных данных во время обработки:

2.2.1. Во время обработки персональных данных необходимо обеспечить:

- недопущения воздействия на технические средства автоматизированной обработки персональных данных, способного нарушить их функционирование;
- недопущение нахождения в помещении, в котором ведется работа с персональными данными, посторонних лиц;
- постоянный контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- недопущение несанкционированного доступа к персональным данным;
- работоспособность средств защиты информации, функционирующих при отсутствии лиц, допущенных к обработке персональных данных;
- конфиденциальность персональных данных.

2.3. Обеспечение безопасности персональных данных в экстремальных ситуациях:

2.3.1. При модификации или уничтожении персональных данных, вследствие несанкционированного доступа к ним необходимо обеспечить возможность их незамедлительного восстановления.

2.3.2. При нарушении порядка предоставления персональных данных пользователям информационной системы необходимо приостановить их предоставление.

2.3.3. При обнаружении несанкционированного доступа к персональным данным необходимо немедленно прервать этот доступ.

2.3.4. В случае несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению

конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных необходимо произвести разбирательство и составление заключений по данным фактам, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

2.3.5. Обо всех экстремальных ситуациях необходимо немедленно поставить в известность руководителя Администрации и произвести разбирательство.

2.4. Обеспечение безопасности персональных данных при завершении их обработки

2.4.1. После завершения сеанса обработки персональных данных необходимо обеспечить:

- корректное закрытие программ и приложений;
- сохранность и целостность всех носителей персональных данных;
- выключение средств автоматизации.

III. Контроль обеспечения безопасности персональных данных

3.1. Целью контроля является соблюдение пользователями ИСПДн требований по обеспечению безопасности персональных данных при их обработке.

3.2. Задачами контроля являются:

- установление фактического положения дел в Администрации по обеспечению безопасности персональных данных при их обработке в ИСПДн;
- выявление проблемных вопросов в организации обеспечения безопасности персональных данных;
- обеспечение соблюдения законодательства Российской Федерации в области персональных данных;
- выработка мер по оказанию методической и практической помощи;
- повышение ответственности пользователей за выполнение возложенных задач, соблюдение законности в их деятельности.

3.3. Оценка достаточности принятых мер по обеспечению безопасности персональных данных при их обработке в информационной системе проводится не реже одного раза в три года.

4. Заключительные положения

4.1. Проверка и пересмотр настоящей инструкции осуществляются в следующих случаях:

- при изменении законодательства Российской Федерации в области персональных данных и пересмотре отраслевых требований обеспечения безопасности персональных данных;
- при внедрении новой техники и (или) технологий;
- по результатам анализа материалов расследования нарушений требований законодательства по обеспечению безопасности персональных данных;
- при появлении новых актуальных угроз безопасности персональных данных;
- изменением уровня защищенности персональных данных при их обработке в информационной системе персональных данных в зависимости от угроз безопасности этих данных;
- по требованию представителей контролирующих (надзорных) органов.

4.2. Ответственность за своевременную корректировку настоящей инструкции возлагается на лицо, назначенное ответственным за организацию обработки персональных данных в Администрации.

Приложение № 12
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Инструкция
по проведению антивирусного контроля

I. Общие положения

1.1. Настоящая Инструкция определяет требования к организации антивирусной защиты информационной системы Администрации Южского муниципального района (далее Администрация).

1.2. Настоящая Инструкция предназначена для уполномоченных работников Администрации: Администратора информационной системы, Администратора безопасности информации и пользователей, осуществляющих обработку конфиденциальной информации и персональных данных в информационной системе Администрации.

1.3. Действие настоящей Инструкции распространяется на пользователей информационной системы Администрации.

1.4. В целях обеспечения защиты от деструктивных воздействий компьютерных вредоносных программ производится антивирусный контроль. Обязательному антивирусному контролю подлежит любая информация, поступающая на средства вычислительной техники, в том числе получаемая на внешних носителях из сторонних организаций.

1.5. Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на ресурсы информационной системы.

Вредоносная программа способна выполнять ряд функций, в том числе:

- скрывать признаки своего присутствия в программной среде рабочей станции;
- обладать способностью к самодублированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать произвольным образом) код программ в оперативной памяти;
- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- искажать произвольным образом, блокировать и/или подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

1.6. Основными задачами системы обеспечения антивирусной защиты являются:

- исключение или существенное затруднение противоправных действий в отношении информационной системы, содержащей защищаемую информацию;
- обеспечение условий для устойчивой бесперебойной работы АРМ.

1.7. Объектом защиты от воздействия вредоносных программ являются АРМ, оборудование, входящее в состав оборудования, подключенного к АРМ и машинные носители информации.

1.8. Обеспечение антивирусной защиты включает:

- регулярные профилактические работы;
- анализ ситуации проявления вредоносных программ и причины их появления;
- уничтожение вредоносных программ на АРМ;
- принятие мер по предотвращению причин появления вредоносных программ.

1.9. Для выполнения требований по антивирусной защите информационной системы используется специализированное программное обеспечение (ПО), обеспечивающее надежную ежедневную автоматическую антивирусную защиту и контроль чистоты информационных массивов данных от вредоносных программ.

1.10. Организация работ по антивирусной защите и ответственность за сопровождение системы антивирусной защиты возлагается на Администратора информационной системы.

1.11. Ответственность за контроль установленного порядка антивирусной защиты возлагается на Администратора безопасности информации.

1.12. Периодический контроль состояния антивирусной защиты информационной системы возлагается на Администратора информационной системы и Администратора безопасности информации.

1.13. Лица, на которых возлагается ответственность по антивирусной защите, имеют полноправный доступ к АРМ и другому оборудованию информационной системы.

1.14. Все процессы производятся в автоматическом режиме без участия пользователей и без помех для работы основного и специального ПО.

Процесс плановой полной проверки файловой системы рабочей станции пользователей и информационной системы проводится во время наименьшей нагрузки оборудования пользовательскими задачами.

1.15. Лицо, ответственное за ежедневное сопровождение антивирусной защиты, обладает необходимыми практическими навыками и теоретическими знаниями по данному вопросу. В основные обязанности по антивирусной защите входит:

- проведение периодического анализа и оценки ситуации по обеспечению антивирусной безопасности для контроля степени защищенности информационной системы и выработки предложений по изменению и улучшению состояния дел;
- проверка соблюдения порядка обновления средств и баз данных антивирусной защиты;
- осуществление контроля за состоянием средств антивирусной защиты на рабочей станции;
- осуществление контроля за соблюдением пользователями требований по обеспечению антивирусной защиты;
- передача еженедельного отчета по состоянию антивирусной защиты Администратору безопасности информации.

Администратор безопасности информации осуществляет следующие действия:

- контроль и анализ еженедельных отчетов по состоянию антивирусной защиты;
- проведение служебных расследований по фактам обнаружения вредоносных программ, повлекших неустойчивую работу и (или) разрушение технологического оборудования и информационных массивов информационной системы;

- организацию мероприятий по улучшению антивирусной защиты в Администрации.

1.16. Устанавливаемое (изменяемое) ПО в информационной системе предварительно проверяется Администратором информационной системы на отсутствие вредоносных программ.

Непосредственно после установки (изменения) ПО Администратор безопасности информации и (или) Администратор информационной системы выполняет антивирусную проверку на рабочей станции информационной системы.

1.17. При возникновении подозрения на наличие вредоносных программ (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) Администратор безопасности информации и (или) Администратор информационной системы проводит внеочередной антивирусный контроль рабочей станции.

1.18. Для пользователей рабочей станции запрещена возможность изменения настроек и параметров защиты антивирусных средств, эти действия производит Администратор безопасности информации или Администратор информационной системы вручную.

1.19. По факту появления и проникновения вредоносных программ, повлекших неустойчивую работу и (или) вывод из строя технологического оборудования и информационных массивов, проводится служебное расследование на инциденты информационной безопасности.

1.20. Результаты расследования причин появления и последствий воздействия вредоносных программ на рабочую станцию докладываются руководителю Администрации с предложениями по принятию мер, предотвращающими в будущем повторение подобных фактов.

II. Требования к антивирусному программному обеспечению

2.1. Применение только лицензионного антивирусного ПО.

2.2. Возможность обнаружения как можно большего числа известных вредоносных программ, в том числе вирусов, деструктивного кода (макро-вирусы, объектов ActiveX, апплетов языка Java и т.п.), а также максимальная готовность быстрого реагирования на появление новых видов вирусных угроз.

2.3. Исчерпывающий список защищаемых точек (автоматизированные рабочие места и т.д.) возможного проникновения вредоносных программ.

2.4. Обеспечение обновлений, консультаций и других форм сопровождения эксплуатации поставщиком антивирусного ПО.

2.5. Соответствие системных требований антивирусного ПО платформам, характеристикам и комплектации применяемой вычислительной техники.

2.6. Надежность и работоспособность антивирусного ПО в любом из предусмотренных режимов работы, по возможности, в русскоязычной среде.

2.7. Наличие документации, необходимой для практического применения и освоения антивирусного ПО, на русском языке.

III. Мероприятия по штатному управлению средствами антивирусного контроля

3.1. В штатном режиме работы системы антивирусной защиты Администратор безопасности информации и (или) Администратор информационной системы выполняет:

- установку средств антивирусной защиты на рабочую станцию, добавляемые в средства защиты информационной системы, в порядке, описанном в эксплуатационной документации;

- необходимые обновления версий средств антивирусной защиты на объекте антивирусной защиты;
- контроль над выполнением задач постоянной защиты;
- контроль актуальности версий антивирусных баз и модулей сканирования ПО;
- непрерывный мониторинг информационного обмена в средствах защиты ИСПДн с целью выявления проявлений программно-математических воздействий;
- обработку сведений, поступающих от средств антивирусной защиты;
- формирование сводных отчётов о работе средств антивирусной защиты, инцидентах и проч.;
- обработку отчётов о состоянии логических сетей;
- формирование отчётов о работе средств антивирусной защиты логической сети.

3.2. Процесс управления системой антивирусной защиты включает в себя следующие действия Администратора безопасности информации и (или) Администратора информационной системы:

- внесение изменений в политику антивирусной защиты;
- управление средствами антивирусной защиты, входящими в состав системы антивирусной защиты;
- мониторинг событий, информация о которых поступает от средств антивирусной защиты с объекта защиты.

3.3. В обязанности Администратора безопасности информации и (или) Администратора информационной системы входит проведение мероприятий, обеспечивающих возможность анализа результатов работы средств системы антивирусной защиты:

- разработка отчётов о работе средств антивирусной защиты;
- разработка сводных отчётов о работе средств антивирусной защиты, инцидентах и пр. за месяц.

В отчётах о состоянии системы антивирусной защиты отражается следующая информация:

- количество обнаруженных вредоносных программ за данный период;
- наиболее активные обнаруженные вредоносные программы;
- объекты, где наблюдается наибольшая частота обнаружения вредоносных программ;
- список зараженных объектов.

IV. Мероприятия по нештатному управлению средствами антивирусного контроля

4.1. В случае заражения рабочей станции вредоносными программами Администратор безопасности информации выполняет следующие действия:

- обновляет антивирусную базу объекта антивирусной защиты;
- проверяет состояние объекта антивирусной защиты, наличие заражения рабочей станции в случае обнаружения пораженных узлов;
- оперативно принимает меры по предотвращению распространения заражения вредоносными программами оборудования и машинных носителей информации и при необходимости отключает их от зараженной рабочей станции;
- по завершении мероприятий по устранению последствий заражения восстанавливает работоспособность рабочей станции и передаёт её пользователю.

4.2. Все или часть вышеперечисленных мероприятий может быть делегирована Администратору информационной системы.

V. Уничтожение вредоносных программ

5.1. Уничтожение вредоносных программ выполняется Администратором безопасности информации и (или) Администратором информационной системы.

5.2. Если вредоносная программа поразила какие-либо программы, то уничтожение вредоносной программы выполняется путем уничтожения программы на жестком диске, либо на ином машинном носителе. После уничтожения зараженной программы восстанавливают программу, используя её резервную копию.

5.3. Если вредоносная программа поразила файлы, то вредоносная программа уничтожается, либо путем стирания этих файлов, либо путем использования специального «лечащего» режима антивирусного ПО. Использование «лечащего» режима не даёт полной гарантии восстановления файла, поэтому после «лечения» необходима проверка восстановления данного файла. «Лечащие» программы используются лишь в тех случаях, когда отсутствует резервная копия зараженной программы или файла с данными, либо восстановление уничтоженного файла с помощью резервной копии очень трудоёмко.

5.4. В любом случае после уничтожения вредоносных программ и восстановления зараженных программ и файлов с данными ещё раз выполняется проверка наличия вредоносных программ, используя антивирусную программу с установленными последними обновлениями.

Перед повторной проверкой производится перезагрузка рабочей станции через выключение и последующее включение.

Если повторная проверка не выявила вредоносных программ, то можно быть уверенным в их отсутствии.

VI. Ответственность пользователей

6.1. Организация мероприятий по централизованной антивирусной защите информационной системы возлагается на Администратора безопасности информации.

6.2. Администратор безопасности информации несет ответственность за формирование политики антивирусной защиты, организацию своевременной инсталляции средств антивирусной защиты информации и централизованное обновление баз данных вирусных описаний на комплексе программно-технических средств информационной системы.

6.3. Выполнение технических мероприятий по централизованной антивирусной защите в информационной системе производится непосредственно Администратором безопасности информации или делегируется Администратору информационной системы.

6.4. Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации и требований настоящей Инструкции в части защиты информационной системы несут пользователи информационной системы.

Приложение № 13
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Положение
о разрешительной системе доступа к информационным ресурсам информационной системы Администрации Южского муниципального района

I. Общие положения

1.1. Настоящее «Положение о разрешительной системе доступа к информационным ресурсам информационной системы персональных данных» (далее - Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и нормативными правовыми документами ФСТЭК России по вопросам обеспечения безопасности персональных данных, разработанными в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 № 1119.

1.2. Разрешительная система доступа к информационным ресурсам информационной системы представляет собой совокупность процедур оформления прав субъектов на доступ к информационным ресурсам (ИР) Администрации Южского муниципального района (далее Администрация, также - Учреждение), прав и обязанностей ответственных лиц, осуществляющих реализацию этих процедур.

1.3. Действие настоящего Положения распространяется на администраторов и пользователей информационной системы.

1.4. Объектами доступа являются:

- ИР, обрабатываемые в информационной системе Учреждения (в том числе содержащие персональные данные), в виде баз данных, библиотек, архивов и на отдельных машинных носителях информации;
- технологическая информация системы защиты информации.

1.5. Субъектами доступа являются:

- Администратор безопасности информации;
- Администратор информационной системы;
- уполномоченные работники Учреждения – пользователи информационной системы.

1.6. Субъекты доступа несут персональную ответственность за соблюдение ими установленного порядка обеспечения защиты ИР информационной системы.

1.7. Ответственными лицами, осуществляющими реализацию процедур оформления и прав субъектов на доступ к ИР, являются:

- руководитель Администрации;

- должностное лицо (работник), ответственный за защиту информации и за обеспечение безопасности персональных данных в информационной системе – Администратор безопасности информации;
- руководители структурных подразделений;
- Администратор информационной системы.

II. Порядок формирования информационных ресурсов информационной системы

2.1. Порядок формирования и использования информационных ресурсов информационной системы определяется Администрации, которое является обладателем информационных ресурсов информационной системы.

2.2. Подлежащие защите информационные ресурсы информационной системы включаются в «Перечень конфиденциальной информации, обрабатываемой в информационной системе» и в «Перечень персональных данных, обрабатываемых в информационной системе», утверждаемые руководителем Администрации.

III. Допуск к информационным ресурсам информационной системы

3.1. Наделение пользователей полномочиями доступа к информационным ресурсам информационной системы:

3.1.1. Лица, доступ которых к конфиденциальной информации и персональным данным, обрабатываемым в информационной системе, необходим для выполнения трудовых обязанностей, допускаются к ним на основании списков, утверждаемых руководителем Администрации.

3.1.2. Необходимость доступа работника к ИР информационной системы определяет начальник структурного подразделения Учреждения на основании трудовых обязанностей работника. Допуск работника к информации, содержащей конфиденциальную информацию и персональные данные, осуществляется в объеме, необходимом для выполнения ими должностных (трудовых) обязанностей. Права доступа работников к защищаемой информации определяются в «Списке должностей работников с указанием методов управления доступом, типа доступа и правил доступа» (далее – Список), утвержденном руководителем Администрации.

3.1.3. Основанием для предоставления (изменения, либо прекращения (отзыва)) прав доступа пользователям информационной системы является заполненная в установленном порядке письменная заявка, подписанная начальником структурного подразделения и согласованная с Администратором безопасности информации и руководителем Администрации.

3.1.4. Согласованная заявка является разрешением на допуск и основанием для регистрации пользователя в информационной системе Администратором информационной системы.

Оформленная заявка поступает к Администратору безопасности информации, который её визирует и направляет Администратору информационной системы, осуществляющему администрирование указанных в заявке прав доступа к информационной системе.

После получения заявки Администратор информационной системы в соответствии с документацией на средства защиты производит необходимые действия по созданию (изменению, удалению) учетной записи пользователя, присвоению ему начального значения пароля и заявленных прав доступа к ресурсам информационной системы, включению его в соответствующие группы пользователей и другие необходимые действия. Для всех пользователей

информационных систем устанавливается режим принудительного запроса смены пароля не реже, чем это необходимо в соответствии с «Инструкцией по организации парольной защиты».

Уникальное имя (учетная запись пользователя), под которым он регистрируется и осуществляет работу в информационной системе, присваивается каждому пользователю для обеспечения персональной ответственности за свои действия. В случае необходимости пользователю информационной системы могут быть сопоставлены несколько уникальных имен (учетных записей).

Использование несколькими работниками при работе в информационной системе одного и того же имени пользователя («группового имени») запрещается.

3.1.5. При изменении должностных обязанностей пользователя, связанных с переводом в другое подразделение, переводом на другую должность и т.п., учетная запись пользователя на основании заявки начальника соответствующего структурного подразделения подлежит изменению (корректировке), при этом старые полномочия аннулируются.

3.1.6. При необходимости уполномоченный работник (администратор) в соответствии с назначаемыми правами доступа осуществляет настройку телекоммуникационных средств информационной системы в части контроля доступа пользователей.

3.1.7. Администратор информационной системы проводит регистрацию прав доступа к ресурсам указанных в заявке рабочей станции (автоматизированного рабочего места (АРМ)) с отметкой изменений в «Списке должностей работников с указанием методов управления доступом, типа доступа и правил доступа» и другие необходимые операции.

3.1.8. После внесения изменений в Список, Администратор безопасности информации производит настройку (при их наличии) специализированных средств защиты рабочей станции.

3.1.9. По результатам изменений в правах доступа Администратор безопасности информации и Администратор информационной системы делают отметку об исполнении задания на бланке Заявки.

3.1.10. Все изменения в правах доступа выполняются администраторами не позднее трех суток с момента получения заявки на внесение изменений.

3.1.11. Работнику, зарегистрированному в качестве нового пользователя системы, под роспись доводится имя соответствующего ему пользователя и начальное значение пароля, которое он обязан сменить при первом же входе в систему (при первом подключении к информационной системе).

3.1.12. Оригиналы исполненных заявок хранятся у Администратора безопасности информации и могут впоследствии использоваться в следующих случаях:

- для восстановления полномочий пользователей после сбоев в информационной системе;
- для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам информационной системы при разборе конфликтных ситуаций;
- для проверки правильности настройки средств разграничения доступа к ресурсам информационной системы.

3.1.13. Блокирование учётных записей на время отпуска пользователей информационной системы осуществляется Администратором информационной системы по заявке начальника соответствующего структурного подразделения. Учётная запись пользователя информационной

системы может быть временно разблокирована, либо изменены права доступа по заявке начальника структурного подразделения, в котором работает пользователь.

3.2. Отзыв прав доступа:

3.2.1. При увольнении пользователей информационной системы и/или лишения их прав доступа к ресурсам информационной системы начальник структурного подразделения, в котором работает увольняемый работник, подает заявку на имя Администратора безопасности информационной системы. Администратор безопасности информации визирует Заявку, утверждая тем самым лишение прав пользователя на доступ к информационным ресурсам информационной системы.

3.2.2. После визирования Заявка на бумажном носителе или в электронном виде поступает к Администратору информационной системы.

3.2.3. Администратор информационной системы удаляет учетные записи из всех указанных в заявке списков доступа.

Администратор безопасности информации:

- проводит смену (удаление) действующих настроек прав доступа на соответствующих средствах защиты в соответствии с изменившимися полномочиями;
- производит необходимые отметки в Списке;
- совместно с непосредственным руководителем работника анализирует целостность данных, к которым имел доступ работник.

Удаление или сохранение содержимого личных папок пользователя согласовывается с начальником структурного подразделения и Администратором безопасности информации.

Администратор безопасности информации совместно с Администратором информационной системы анализируют автоматизированное рабочее место уволенного работника на наличие закладок, вирусов, после чего все данные на жестком диске уничтожаются и операционная система (ОС) на рабочем месте переинсталлируется.

По результатам изменений в правах доступа Администратор безопасности информации и Администратор информационной системы делают отметку об исполнении задания на бланке Заявки.

Все изменения в правах доступа, связанные с увольнением пользователя информационной системы, выполняются администраторами не позднее трех суток с момента получения заявки на внесение изменений.

3.3. Порядок и периодичность проверки прав пользователей:

Проверка прав пользователей проводится Администратором безопасности информации с периодичностью не реже одного раза в три месяца путем сравнения прав согласно утвержденного «Списка должностей работников с указанием методов управления доступом, типа доступа и правил доступа» с правами пользователей по доступу к информационным ресурсам информационной системы.

IV. Допуск к информационным ресурсам информационной системы сторонних организаций

4.1. Допуск к информационным ресурсам сторонних организаций, деятельность которых не связана с исполнением функций информационной системы, регламентируется законодательством Российской Федерации, приказами и распоряжениями министерств и служб, законодательно наделенных полномочиями на получение такой информации, а также настоящим Положением.

4.2. Доступ к информационным ресурсам информационной системы сторонних организаций осуществляется на основании письменных мотивированных запросов.

В письменном запросе указывается:

- основание (с приведением ссылки на нормативный акт), в соответствии с которым предоставляется информация;
- для каких целей необходима информация;
- конкретное наименование предоставляемой информации и её объём;
- способ доступа (предоставления).

4.3. Основанием для доступа (предоставления) информации служит резолюция руководителя Администрации на соответствующем документе (запросе).

V. Допуск к информационным ресурсам информационной системы сторонних организаций, выполняющих работы на договорной основе

5.1. К организациям, выполняющим работы на договорной основе, могут относиться:

- организации, осуществляющие монтаж и настройку информационной системы, сопровождение программно-прикладного обеспечения и технических средств;
- организации, оказывающие услуги в области защиты информации (проведение обследований, монтаж и настройка средств защиты информации, контроль эффективности системы защиты информации, аттестация объектов информатизации и т.п.);
- другие организации, оказывающие услуги по информационно-техническому обеспечению и т.п.

5.2. Порядок допуска определяется в договоре на выполнение работ (оказание услуг) в соответствии с требованиями Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд». Обязательным условием договора является заключение соглашения об обеспечении безопасности конфиденциальной информации и персональных данных и их конфиденциальности.

5.3. Решением о допуске является подписанный в установленном порядке «Договор на выполнение работ или оказание услуг».

5.4. Доступ к информационным ресурсам информационной системы сторонних организаций осуществляется на основании:

- письменных запросов;
- письменных соглашений (договоров) сторон об обмене информацией.

5.5. В письменном запросе (договоре) указывается:

- основание (ссылка на нормативный акт, договор), в соответствии с которым предоставляется информация;
- для каких целей необходима информация;
- конкретное наименование предоставляемой информации и её объём;
- способ доступа (предоставления).

5.6. Основанием для доступа (предоставления) информации служит резолюция руководителя Администрации на соответствующем документе (запросе).

5.7. При наличии официального соглашения со сторонней организацией о допуске (предоставлении) к информации доступ к ней осуществляется в порядке, указанном в подписанном соглашении (договоре).

5.8. Запрещается передача электронных копий баз данных любым сторонним организациям, за исключением санкционированных случаев передачи электронных файлов, выгружаемых из баз данных в рамках осуществления полномочий (функций) Администрации.

5.9. В договор на оказание услуг включается условие о неразглашении сведений, составляющих конфиденциальную информацию и персональные данные, а также иной защищаемой информации, ставшей известной в ходе выполнения работ, если для их выполнения предусмотрено использование таких сведений.

VI. Контроль функционирования разрешительной системы допуска к информационным ресурсам информационной системы

6.1. Контроль функционирования разрешительной системы допуска к информационным ресурсам организуется в соответствии с:

- планом основных мероприятий по защите информации на текущий год;
- функциональными обязанностями должностных лиц;
- распоряжениями руководителя Администрации.

6.2. Контроль функционирования разрешительной системы допуска к информационным ресурсам осуществляется ответственными должностными лицами.

Организация контроля возлагается на уполномоченных лиц, назначенных распоряжением руководителя Администрации.

Приложение № 14
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Перечень
должностей работников, доступ которых к конфиденциальной информации и персональным данным, обрабатываемым в информационной системе Администрации Южского муниципального района, и к техническим средствам необходим для выполнения ими трудовых обязанностей

№ п/п	Структурное подразделение и наименование должности	Номер (название) помещения
1	2	3
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		
26.		
27.		
28.		

Приложение № 15
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Перечень
должностей работников, имеющих физический доступ к машинным носителям информации в информационной системе Администрации Южского муниципального района, для выполнения ими трудовых обязанностей

№ п/п	Структурное подразделение и наименование должности	Номер (название) помещения
1	2	3
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		
26.		
27.		
28.		
29.		

Приложение № 16
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Список
должностей работников с указанием методов управления доступом, типа доступа и правил доступа к ресурсам информационной системы Администрации Южского муниципального района

№ пп	Структурное подразделение и наименование должности	Метод управления доступом	Тип доступа	Правила доступа (разрешенные действия)
1	2	3	4	5
1.		Мандатный	чтение, запись, систематизация, передача, накопление, хранение, уточнение, обезличивание, блокирование, уничтожение	Доступ к персональным данным: сотрудников
2.		Мандатный	чтение, запись, систематизация, передача, накопление, хранение, уточнение, обезличивание, блокирование, уничтожение	Доступ к персональным данным: сотрудников, их родственников, физических лиц, состоящих в договорных и иных гражданско-правовых отношениях
3.		Мандатный	чтение, запись, систематизация, передача, накопление, хранение, уточнение, обезличивание, блокирование, уничтожение	Доступ к персональным данным: сотрудников
4.				
5.				
6.				
7.				

Приложение № 17
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Положение
об использовании мобильных устройств и носителей информации в Администрации Южского муниципального района

I.Общие положения

1.1. Настоящее «Положение об использовании мобильных устройств и носителей информации в информационной системе» (далее - Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и нормативными правовыми документами ФСТЭК России по вопросам обеспечения безопасности персональных данных, разработанными в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 № 1119.

1.2. Положение об использовании мобильных устройств и носителей информации в информационной системе устанавливает порядок использования мобильных устройств и носителей информации, предоставляемых Администрации Южского муниципального района (далее Администрация) для использования в ИС Администрации.

1.3. Действие настоящего Положения распространяется на администраторов и пользователей информационной системы.

1.4. Субъекты доступа несут персональную ответственность за соблюдение ими установленного порядка использования мобильных устройств и носителей информации в информационной системе.

1.5. Ответственными лицами, осуществляющими реализацию процедур использования мобильных устройств и носителей информации в информационной системе, являются:

- руководитель Администрации;
- должностное лицо (работник), ответственное за защиту информации и за обеспечение безопасности персональных данных в информационной системе – Администратор безопасности информации;
- руководители структурных подразделений;
- Администратор информационной системы.

II. Порядок использования мобильных устройств и носителей информации

2.1. Под использованием мобильных устройств и носителей информации в ИС Администрации понимается их подключение к инфраструктуре ИС с целью обработки,

приема/передачи информации между ИС и мобильными устройствами, а также носителями информации.

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

2.3. На предоставленных Администрации мобильных устройствах допускается использование коммерческого ПО, входящего в Реестр разрешенного к использованию ПО и указанного в Приложении №20 «Перечень программного обеспечения …» к Распоряжению.

2.4. К предоставленным мобильным устройствам и носителям информации предъявляются те же требования информационной безопасности, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения информационной безопасности определяется администраторами).

2.5. Мобильные устройства и носители информации предоставляются работникам Администрации по инициативе Руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у работника Администрации производственной необходимости.

2.6. Процесс предоставления работнику Администрации мобильных устройств и носителей информации состоит из следующих этапов:

2.6.1. Подготовка заявки (Приложение А) в утвержденной форме, осуществляется Руководителем структурного подразделения на имя Руководителя Администрации.

2.6.2. Согласование подготовленной заявки (для получения заключения о возможности предоставления работнику Администрации заявленного мобильного устройства и/или носителя информации) с Администратором безопасности.

2.6.3. Передача оригинала заявки Администратору безопасности для учета предоставленного мобильного устройства и/или носителя информации и внесения изменений в «Список работников Администрации, имеющих право работы с мобильными устройствами вне территории Администрации, а также выполнения технических настроек по регистрации мобильного устройства в ИС и/или предоставлению права использования носителей информации на АРМах Администрации (в случае согласования заявки с Руководителем Администрации.

2.7. Внос на территорию Администрации предоставленных мобильных устройств работниками Администрации, а также вынос их за его пределы производится только на основании «Списка работников Администрации, имеющих право работы с мобильными устройствами вне территории Администрации (Приложение Б), который ведется Администратором безопасности на основании утвержденных заявок и передается в службу безопасности.

2.8. Внос на территорию Администрации предоставленных мобильных устройств работниками подрядных и сторонних организаций, а также вынос их за его пределы производится на основании заполненной по форме заявки (Приложение В) на внос/вынос мобильного устройства, подписанной Руководителем структурного подразделения.

2.9. При использовании предоставленных работникам Администрации мобильных устройств и носителей информации необходимо:

2.9.1. Соблюдать требования настоящего Положения.

2.9.2. Использовать мобильные устройства и носители информации исключительно для выполнения своих служебных обязанностей.

2.9.3. Ставить в известность администраторов ИС о любых фактах нарушения требований настоящего Положения.

2.9.4. Бережно относится к мобильным устройствам и носителям информации.

2.9.5. Эксплуатировать и транспортировать мобильные устройства и носители информации в соответствии с требованиями производителей.

2.9.6. Обеспечивать физическую безопасность мобильных устройств и носителей информации всеми разумными способами.

2.9.7. Извещать администраторов ИС о фактах утраты (кражи) мобильных устройств и носителей информации.

2.10. При использовании предоставленных работникам Администрации мобильных устройств и носителей информации запрещено:

2.10.1. Использовать мобильные устройства и носители информации в личных целях.

2.10.2. Передавать мобильные устройства и носители информации другим лицам (за исключением администраторов ИС).

2.10.3. Оставлять мобильные устройства и носители информации без присмотра, если не предприняты действия по обеспечению их физической безопасности.

2.11. Любое взаимодействие (обработка, прием/передача информации) инициированное работником Администрации между ИС и неучтенными (личными) мобильными устройствами, а также носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с администраторами ИС заранее). Администрация оставляет за собой право блокировать или ограничивать использование таких устройств и носителей информации.

2.12. Информация об использовании работниками Администрации мобильных устройств и носителей информации в ИС протоколируется и, при необходимости, может быть предоставлена Руководителям структурных подразделений, а также Администрации.

2.13. При подозрении работника Администрации в несанкционированном и/или нецелевом использовании мобильных устройств и носителей информации инициализируется служебная проверка, проводимая комиссией, состав которой определяется Руководителем Администрации.

2.14. По факту выясненных обстоятельств составляется акт расследования инцидента и передается Руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Администрации и действующему законодательству. Акт расследования инцидента и сведения о принятых мерах подлежат передаче Администратору безопасности.

2.15. Информация, хранящаяся на предоставляемых Администрации мобильных устройствах и носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

2.16. В случае увольнения или перевода работника в другое структурное подразделение Администрации, предоставленные ему мобильные устройства и носители информации изымаются.

III. Контроль использования мобильных устройств и носителей информации в информационной системе

3.1. Контроль использования мобильных устройств и носителей информации в информационной системе организуется в соответствии с:

- планом основных мероприятий по защите информации на текущий год;
- функциональными обязанностями должностных лиц;
- распоряжениями руководителя Администрации.

3.2. Контроль использования мобильных устройств и носителей информации в информационной системе осуществляется ответственными должностными лицами.

Организация контроля возлагается на уполномоченных лиц, назначенных распоряжениями руководителя Администрации.

Приложение А. Заявка на предоставление работнику Администрации мобильного устройства/носителя информации.

ЗАЯВКА

на предоставление работнику _____

(Администрации Южского муниципального района)

мобильного устройства

Руководителю _____

(Администрации Южского муниципального района)

«___»_____ 20___ года

В связи с возникшей производственной необходимостью, прошу предоставить следующему работнику:

_____

(ФИО)

_____

(должность)

_____

(структурное подразделение)

_____

(номер служебного телефона)

_____

(наименование мобильного устройства)

_____

(перечень задач, решаемых с использованием мобильного устройства)

_____

_____

Руководитель: _____

(наименование структурного подразделения)

«___» _____ 20___ г. _____ _____

(подпись) *(фамилия и инициалы)*

Согласовано:

ЗАЯВКА

на предоставление работнику _____ _____

(Администрации Южского муниципального района)

носителя информации

Руководителю _____

(Администрации Южского муниципального района)

«___»_____ 20___ года

В связи с возникшей производственной необходимостью, прошу предоставить следующему работнику:

_____

(ФИО)

_____

(должность)

_____

(структурное подразделение)

_____

(номер служебного телефона)

_____

(наименование мобильного устройства)

_____

(перечень задач, решаемых с использованием носителя информации)

_____

_____

Руководитель: _____

(наименование структурного подразделения)

«___» _____ 20___ г. _____ _____

(подпись) *(фамилия и инициалы)*

Согласовано:

Приложение Б. Список работников, имеющих право работы с мобильными устройствами вне территории Администрации

СПИСОК

работников_____ *(Администрации Южского муниципального района)*, имеющих право работы с мобильными устройствами вне территории _____

(Администрации Южского муниципального района)

№ п/п	ФИО	Должность	Структурное подразделение	Наименование мобильного устройства	Инвентарный номер мобильного устройства
1	2	3	4	5	6

Руководитель отдела ИТ:

«___» _____ 20___ г. _____ _____

(подпись) *(фамилия и инициалы)*

Согласовано:

Приложение В. Заявка на внос/вынос мобильного устройства за пределы Администрации

ЗАЯВКА
на внос/вынос мобильного устройства за пределы _____
(Администрации Южского муниципального района)

Руководителю _____
(Администрации Южского муниципального района)

«___»_____ 20___ года

В связи с возникшей производственной необходимостью, прошу разрешить внос/вынос за пределы _____ *(Администрации Южского муниципального района)* следующего мобильного устройства:

_____

(наименование мобильного устройства)

_____

(инвентарный номер мобильного устройства)

_____

(ФИО ответственного за мобильное устройство работника)

_____

(должность ответственного за мобильное устройство работника)

_____

(структурное подразделение ответственного за мобильное устройство работника)

_____

(номер служебного телефона ответственного за мобильное устройство работника)

_____

(цель вноса/выноса мобильного устройства)

_____

(период нахождения мобильного устройства на территории)

_____

Руководитель: _____

(наименование структурного подразделения)

«___» _____ 20___ г. _____ _____

(подпись) *(фамилия и инициалы)*

Согласовано:

Приложение № 18
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Перечень
конфиденциальной информации, обрабатываемой в информационной системе Администрации Южского муниципального района

№ п/п	Категория сведений	Основания для отнесения к сведениям конфиденциального характера
1	2	3
1.	Персональные данные сотрудников Администрации Южского муниципального района: - ФИО; - место, год и дата рождения; - адрес по прописке; - паспортные данные (серия, номер паспорта, кем и когда выдан); - информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающих образование: наименование, номер, дата выдачи, специальность); - информация о трудовой деятельности до приема на работу; - информация о трудовом стаже (место работы, должность, период работы, причины увольнения); - адрес проживания (реальный); - телефонный номер (домашний, рабочий, мобильный); - семейное положение и состав семьи (муж/жена, дети); - информация о знании иностранных языков; - форма допуска; - оклад; - данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные	Пункт 1 «Перечня сведений конфиденциального характера», утверждённого Указом Президента РФ от 06.03.1997 № 188 (Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях)

№ п/п	Категория сведений	Основания для отнесения к сведениям конфиденциального характера
1	2	3
	социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты); - сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета); - ИНН; - СНИЛС; - страховой полис; - данные об аттестации работников; - данные о повышении квалификации; - данные о наградах, медалях, поощрениях, почетных званиях; - информация о приеме на работу, перемещении по должности, увольнении; - информация об отпусках; - информация о командировках; - информация о негосударственном пенсионном обеспечении.	
2.	Персональные данные субъектов, персональные данные которых обрабатываются Администрации Южского муниципального района в связи с исполнением своих обязанностей: - ФИО; - дата рождения; - контактный телефон; - адрес прописки; - адрес фактического проживания; - паспортные данные; - сведения о гражданстве, социальном положении субъекта; - биометрические данные; - страховой полис; - сведения о факте обращения субъекта за медицинской помощью; - сведения о состоянии здоровья субъекта и диагнозе; - иные сведения, имеющие отношение к деятельности Администрации Южского муниципального района.	Пункт 1 «Перечня сведений конфиденциального характера», утверждённого Указом Президента РФ от 06.03.1997 № 188 (Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях) Пункт 4 Перечня сведений конфиденциального характера, утверждённого Указом Президента РФ от 06.03.1997 № 188 (Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами)
3.	Информация о частной жизни гражданина	Статья 9 Федерального закона

№ п/п	Категория сведений	Основания для отнесения к сведениям конфиденциального характера
1	2	3
	(физического лица), в том числе информации, составляющей личную или семейную тайну	Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Опубликован 29.07.2006. Принят Государственной Думой 08.07.2006. Одобрен Советом Федерации 14.07.2006
4.	Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).	Пункт 3 «Перечня сведений конфиденциального характера», утвержденного Указом Президента РФ от 06.03.1997 № 188
5.	Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами	Пункт 4 Перечня сведений конфиденциального характера, утверждённого Указом Президента РФ от 06.03.1997 № 188
	Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определённых видов деятельности (профессиональная тайна), в случаях, когда на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации. Информация, составляющая профессиональную тайну, защищаемая в соответствии с федеральными законами и (или) по решению суда	Статья 9 Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Опубликован 29.07.2006. Принят Государственной Думой 08.07.2006. Одобрен Советом Федерации 14.07.2006
6.	Информация, доступ к которой ограничен федеральными законами	Статья 9 Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Опубликован 29.07.2006. Принят Государственной Думой 08.07.2006. Одобрен Советом Федерации 14.07.2006
7.	Содержание регистров бухгалтерского учёта и внутренней бухгалтерской отчётности	Статья 10 Федерального закона «О бухгалтерском учёте», принятого Государственной Думой 23.02.1996, одобренного Советом Федерации 20.03.1996
8.	Сведения о порядке и состоянии защиты конфиденциальной информации.	Пункт 3 «Перечня сведений конфиденциального характера», утвержденного Указом Президента РФ от 06.03.1997 № 188 Федеральный закон Российской
9.	Сведения о защищаемых информационных ресурсах в локальных сетях организации.	
10.	Сведения об охране организации, пропускном	

№ п/п	Категория сведений	Основания для отнесения к сведениям конфиденциального характера
1	2	3
	и внутриобъектовом режиме, системе сигнализации, о наличии средств контроля и управления доступом.	Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Опубликован 29.07.2006. Принят Государственной Думой 08.07.2006. Одобрен Советом Федерации 14.07.2006

Приложение № 19
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Правила
обработки персональных данных в информационной системе Администрации Южского муниципального района

I. Общие положения

1.1. Настоящие Правила обработки персональных данных в Администрации Южского муниципального района (далее - Правила) определяют цели, содержание и порядок обработки персональных данных, меры, направленные на защиту персональных данных, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных в Администрации Южского муниципального района.

1.2. Правила определяют деятельность Администрации Южского муниципального района, как оператора, осуществляющего обработку персональных данных, в отношении обработки и защиты персональных данных.

1.3. Обработка персональных данных в Администрации Южского муниципального района осуществляется с соблюдением принципов и условий, предусмотренных законодательством Российской Федерации в области персональных данных и настоящими Правилами.

II. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных

2.1. Для выявления и предотвращения нарушений, предусмотренных законодательством Российской Федерации в области персональных данных, в Администрации Южского муниципального района используются следующие процедуры:

- осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;
- оценка вреда, который может быть причинен субъектам персональных данных;
- ознакомление работников Администрации Южского муниципального района, непосредственно осуществляющих обработку персональных данных, с законодательством Российской Федерации в области персональных данных, в том числе с требованиями к защите персональных данных и с настоящими Правилами, и (или) их обучение;
- осуществление обработки персональных данных в соответствии с принципами и условиями обработки персональных данных, установленными законодательством Российской Федерации в области персональных данных;

- недопущение объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обеспечение при обработке персональных данных точности персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных;
- ограничение обработки персональных данных достижением конкретных, заранее определенных и законных целей;
- соответствие содержания и объема обрабатываемых персональных данных заявленным целям обработки.

III. Цели обработки персональных данных

3.1. Обработка персональных данных в Администрации Южского муниципального района осуществляется в целях:

- рассмотрение возможности заключения трудового соглашения/договора с субъектом персональных данных;
- начисления заработной платы работникам _ Администрации Южского муниципального района
- регулирование трудовых (гражданско-правовых) отношений субъекта с Администрацией Южского муниципального района (обеспечение соблюдения законов и иных нормативных правовых актов, содействие работникам в трудоустройстве, обучении и продвижении по службе, обеспечение личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества);
- предоставления отчетности государственным надзорным органам в соответствии с требованиями действующего законодательства Российской Федерации;
- обеспечения пропускного режима на Администрации Южского муниципального района;
- передача Администрации Южского муниципального района персональных данных или поручение их обработки третьим лицам в соответствии с действующим законодательством;
- осуществления статистических или иных исследовательских целей;
- обеспечения доступа неограниченного круга лиц к общедоступным персональным данным, который предоставлен субъектом персональных данных либо по просьбе субъекта персональных данных;
- выполнения возложенных на Администрацию Южского муниципального района функций, полномочий и обязанностей.

3.2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей.

3.3. Обработка персональных данных, несовместимых с целями сбора персональных данных не допускается.

3.4. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным в п. 3.1. Правил целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

IV. Условия и порядок обработки персональных данных работников Администрации Южского муниципального района

4.1. Персональные данные работников Администрации Южского муниципального района, граждан, претендующих на замещение должностей в Администрации Южского муниципального района, обрабатываются в целях осуществления кадровой работы, в том числе содействия работникам Администрации Южского муниципального района в трудоустройстве, формирования кадрового резерва, обучения и должностного роста, учета результатов исполнения должностных обязанностей, обеспечения личной безопасности работников Администрации Южского муниципального района, включая членов их семей, обеспечения работникам Администрации Южского муниципального района установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, а также в целях противодействия коррупции.

4.2. В Администрации Южского муниципального района обрабатываются следующие категории персональных данных работников Администрации Южского муниципального района:

- фамилия, имя, отчество, дата и место рождения, гражданство;
- прежние фамилия, имя, отчество, дата, место рождения (в случае изменения);
- владение иностранными языками и языками народов Российской Федерации;
- образование (когда и какие образовательные организации окончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому);
- выполняемая работа с начала трудовой деятельности (в том числе военная служба, работа по совместительству, предпринимательская деятельность);
- классный чин муниципальной службы (кем и когда присвоены);
- государственные награды, иные награды и знаки отличия (кем награжден и когда);
- степень родства, фамилии, имена, отчества, даты рождения близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены);
- места рождения, места работы и домашние адреса близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены);
- фамилии, имена, отчества, даты рождения, места рождения, места работы и домашние адреса бывших мужей (жен);
- пребывание за границей (когда, где, с какой целью);
- близкие родственники (отец, мать, братья, сестры и дети), а также муж (жена), в том числе бывшие, постоянно проживающие за границей и (или) оформляющие документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество, с какого времени проживают за границей);
- адрес регистрации и фактического проживания, дата регистрации по месту жительства;
- вид, серия, номер документа, удостоверяющего личность на территории Российской Федерации, наименование органа, выдавшего его, дата выдачи;

- паспорт, удостоверяющий личность гражданина Российской Федерации за пределами Российской Федерации (серия, номер, кем и когда выдан);
- номер контактного телефона или сведения о других способах связи;
- отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);
- идентификационный номер налогоплательщика;
- номер страхового свидетельства обязательного пенсионного страхования;
- реквизиты полиса обязательного медицинского страхования;
- реквизиты свидетельств государственной регистрации актов гражданского состояния;
- наличие (отсутствие) судимости;
- допуск к государственной тайне, оформленный за период работы, службы, учебы (форма, номер и дата);
- наличие (отсутствие) заболевания, препятствующего трудоустройству и осуществлению трудовой деятельности, подтвержденного заключением медицинского учреждения;
- наличие (отсутствие) медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, подтвержденное заключением медицинского учреждения;
- сведения о доходах, расходах, имуществе и обязательствах имущественного характера, а также о доходах, расходах, имуществе, обязательствах имущественного характера супруга (супруги) и несовершеннолетних детей;
- номер индивидуального лицевого счета, дата его открытия, номер банковской карты;
- иные персональные данные, необходимые для достижения целей, указанных в п. 4.1. Правил.

4.3. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных работников Администрации Южского муниципального района, осуществляется путем:

- получения оригиналов необходимых документов (заявление, трудовая книжка, иные документы, предоставляемые в кадровые подразделения);
- копирования оригиналов документов;
- внесения сведений в учетные формы;
- формирования персональных данных в ходе кадровой работы;
- внесения персональных данных в информационные системы (при наличии);
- получения персональных данных непосредственно от работников Администрации Южского муниципального района, граждан, претендующих на замещение должностей в Администрации Южского муниципального района.

4.4. Запрещается получать, обрабатывать и приобщать к личному делу работника Администрации Южского муниципального района персональные данные, не предусмотренные п. 4.2. Правил, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни.

V. Условия и порядок обработки персональных данных субъектов в связи с предоставлением государственных услуг и исполнением государственных функций

5.1. В Администрации Южского муниципального района обработка персональных данных субъектов персональных данных может осуществляться в целях предоставления государственных услуг и исполнения государственных функций.

5.2. Персональные данные субъектов персональных данных, обратившихся в Администрации Южского муниципального района лично, а также направивших индивидуальные или коллективные письменные обращения (запросы) или обращения (запросы) в форме электронного документа, обрабатываются в целях рассмотрения указанных обращений (запросов) с последующим уведомлением о результатах рассмотрения.

5.3. Обработка персональных данных, необходимых в связи с предоставлением государственных услуг и исполнением государственных функций, осуществляется без согласия субъектов персональных данных в соответствии с п. 4, п. 5 части 1 статьи 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»:

- обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, в том числе в случае реализации оператором своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

5.4. Обработка персональных данных, необходимых в связи с предоставлением государственных услуг и исполнением государственных функций, осуществляется уполномоченными работниками либо структурными подразделениями Администрации Южского муниципального района, предоставляющими соответствующие государственные услуги и (или) исполняющими государственные функции, и включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

5.5. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов, обратившихся в Администрации Южского

муниципального района для получения государственной услуги или в целях исполнения государственной функции, осуществляется путем:

- получения оригиналов необходимых документов (заявление);
- заверения копий документов;
- внесения сведений в учетные формы (на бумажных и электронных носителях).

5.6. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от субъекта персональных данных.

5.7. При сборе персональных данных уполномоченный Администрации Южского муниципального района, осуществляющий получение персональных данных непосредственно от субъектов персональных данных, обратившихся за предоставлением государственной услуги или в связи с исполнением государственной функции, обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить персональные данные.

5.8. Передача (распространение, предоставление) и использование персональных данных заявителей (субъектов персональных данных) Администрации Южского муниципального района осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

VI. Порядок обработки персональных данных субъектов персональных данных в информационных системах

6.1. Обеспечение безопасности при обработке персональных данных, содержащихся в информационных системах Администрации Южского муниципального района осуществляется в соответствии с постановлением Правительства Российской Федерации от «01» ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

6.2. Уполномоченному работнику, имеющему право осуществлять обработку персональных данных в информационных системах Администрации Южского муниципального района предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется в соответствии с функциями, предусмотренными должностными регламентами работников Администрации Южского муниципального района.

6.3. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных Администрации Южского муниципального района;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах, необходимых для выполнения требований к защите персональных данных,

исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

- применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учет машинных носителей персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационных системах, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.

6.4. В случае выявления нарушений порядка обработки персональных данных уполномоченными работниками Администрации Южского муниципального района незамедлительно принимаются меры по установлению причин нарушений и их устранению.

VII. Сроки обработки и хранения персональных данных

7.1. Сроки обработки и хранения персональных данных работников Администрации Южского муниципального района, граждан, претендующих на замещение должностей в Администрации Южского муниципального района, определяются в соответствии с законодательством Российской Федерации.

С учетом положений законодательства Российской Федерации устанавливаются следующие сроки обработки и хранения персональных данных:

- персональные данные, содержащиеся в приказах по личному составу работников Администрации Южского муниципального района (о приеме, о переводе, об увольнении, об установлении надбавок), подлежат хранению в соответствующих структурных подразделениях в течение 75 лет в порядке, предусмотренном законодательством Российской Федерации (на основании Приказа № 558 от 25.08.2010г. «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций с указанием сроков хранения»);
- персональные данные, содержащиеся в личных делах работников Администрации Южского муниципального района, а также личных карточках работников Администрации Южского муниципального района, хранятся в соответствующих структурных подразделениях в течение 75 лет в порядке, предусмотренном законодательством Российской Федерации;

- персональные данные, содержащиеся в приказах о поощрениях, материальной помощи работникам Администрации Южского муниципального района, подлежат хранению в течение 75 лет в порядке, предусмотренном законодательством Российской Федерации;
- персональные данные, содержащиеся в распоряжениях о предоставлении отпусков, о краткосрочных внутрироссийских и зарубежных командировках, о дисциплинарных взысканиях работников Администрации Южского муниципального района, подлежат хранению в соответствующих структурных подразделениях в течение 5 лет;
- персональные данные, содержащиеся в документах граждан, претендующих на замещение должностей в Администрации Южского муниципального района, не допущенных к участию в конкурсе, и кандидатов, участвовавших в конкурсе, хранятся в соответствующих структурных подразделениях Администрации Южского муниципального района в течение 3 лет со дня завершения конкурса, после чего подлежат уничтожению.
- сроки обработки и хранения персональных данных, предоставляемых субъектами персональных данных в Администрации Южского муниципального района в связи с получением государственных услуг и исполнением государственных функций, определяются нормативными правовыми актами, регламентирующими порядок их сбора и обработки.

7.3. Персональные данные граждан, обратившихся в Администрации Южского муниципального района лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, хранятся в течение 5 лет.

7.4. Персональные данные, предоставляемые субъектами персональных данных на бумажном носителе в связи с предоставлением Администрации Южского муниципального района государственных/муниципальных услуг и исполнением государственных/муниципальных функций, хранятся на бумажных носителях в структурных подразделениях Администрации Южского муниципального района, к полномочиям которых относится обработка персональных данных в связи с предоставлением государственной услуги или исполнением государственной функции, в соответствии с положениями о соответствующих структурных подразделениях.

7.5. Если сроки хранения персональных данных не установлены законодательством Российской Федерации, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных, то обработка и хранение персональных данных осуществляются не дольше, чем этого требуют цели их обработки и хранения.

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

7.7. Уполномоченные должностные лица Администрации Южского муниципального района обеспечивают раздельное хранение персональных данных на разных

материальных носителях, обработка которых осуществляется в различных целях, определенных Правилами.
7.8. Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляют руководители соответствующих структурных подразделений Администрации Южского муниципального района.
7.9. Срок хранения персональных данных, внесенных в информационные системы Администрации Южского муниципального района, должен соответствовать сроку хранения бумажных оригиналов.

VIII. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

8.1. Структурным подразделением Администрации Южского муниципального района, ответственным за документооборот, осуществляется систематический контроль и выделение документов, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению.
8.2. Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается на заседании комиссии по уничтожению материальных носителей информации, содержащих персональные данные Администрации Южского муниципального района (далее - Комиссия), состав которой утверждается распоряжением Администрации Южского муниципального района
По итогам заседания составляется протокол и акт об уничтожении документов с указанием уничтожаемых дел и их количества, проверяется их комплектность, акт подписывается председателем и членами Комиссии Администрации Южского муниципального района и утверждается руководителем Администрации Южского муниципального района.
8.3. Должностное лицо Администрации Южского муниципального района, ответственное за архивную деятельность, организует работу по уничтожению документов, содержащих персональные данные.
8.4. Уничтожение по окончании срока обработки персональных данных на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.
8.5. По итогам уничтожения дел (на бумажном и (или) электронном носителях) в акт об уничтожении документов вносится соответствующая запись.

Приложение к Правилам
обработки персональных данных
в Администрации Южского муниципального района

Перечень
персональных данных, обрабатываемых в информационной системе Администрации Южского муниципального района

№ п/п	Категории субъектов персональных данных	Персональные данные
1	2	3
1.	Работники	Фамилия, имя, отчество (при наличии последнего)
2.	Члены семей работников	Фамилия, имя, отчество (при наличии последнего)
3.	Персональные данные субъектов, персональные данные которых обрабатываются Администрацией Южского муниципального района в связи с исполнением своих обязанностей	Фамилия, имя, отчество (при наличии последнего)
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		

Приложение № 20
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Перечень
программного обеспечения и (или) его компонентов, разрешенных к установке («белый список»), перечень программного обеспечения и (или) его компонентов, запрещенных к установке («черный список»), и перечень программного обеспечения и (или) его компонентов, разрешенного к загрузке при старте операционной системы

№ п/п	Программное обеспечение и (или) его компоненты, разрешенное к установке («белый список»)	Программное обеспечение и (или) его компоненты, запрещенное к установке («черный список»)	Программное обеспечение и (или) его компоненты, разрешенное к загрузке при старте операционной системы
1	2	3	4
1.	Операционные: Microsoft Windows XP, Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows Server 2008 R2 Server 2003, Linux (Embedded, DEPO ThinOS)	Программное обеспечение и его компоненты, отсутствующие в «белом списке»	Программное обеспечение и его компоненты, разрешенные к загрузке при старте операционной системы
2.	Офисные системы: Microsoft Office 2010/2013/2016…, LibreOffice		
3.	Антивирусное ПО: Антивирус Касперского, Dr. Web		
4.	Архиваторы: 7-zip,		
5.	Чтение PDF: Adobe Reader, Foxit Reader		
6.	Распознавание текстов: CuneiForm, ABBYY FineReader		
7.	Приложения: 1С: Бухгалтерия/, СБИС, 1С: Предприятие, ПУ 6, Консультант +, Сотрудники предприятия, СЭДО, TotalComander		

Использование программного обеспечения, не включенного в данный список, запрещено. Для установки программного обеспечения, выходящего за рамки данного списка необходимо письменное разрешение Администратора безопасности информации.

При обнаружении неутвержденного программного обеспечения на рабочих станциях сотрудников, уполномоченные лица имеют право инициировать служебное расследование.

Приложение № 21
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Перечень
событий безопасности в информационной системе Администрации Южского муниципального района

№ п/п	События безопасности	Состав и содержание информации о событиях безопасности, подлежащих регистрации
1	2	3
1.	Вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы	Дата и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа
2.	Подключение машинных носителей информации и вывод информации на носители информации	Дата и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации
3.	Запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации	Дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).
4.	Попытки доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа	Дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер))
5.	Попытки удаленного доступа	Дата и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе

Приложение № 22
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Типовая форма

Журнал
антивирусных проверок информационной системы

_____ *(Администрации Южского муниципального района)*

_____
(дата начала ведения журнала)

_____
(наименование юридического лица)

_____
(адрес (место нахождения) постоянно действующего исполнительного органа юридического лица)

_____
(государственный регистрационный номер записи о государственной регистрации юридического лица)

Ответственное лицо: _____
_____
(фамилия, имя, отчество (в случае, если имеется), должность лица (лиц), ответственного за ведение журнала)

_____
(фамилия, имя, отчество (в случае, если имеется) руководителя юридического лица)

Подпись: _____
М.П.

Инструкция по заполнению
Журнала антивирусных проверок информационной системы
Администрации Южского муниципального района

Журнал антивирусных проверок информационной системы (далее - Журнал) информационной системы Администрации Южского муниципального района (далее - Администрация) содержит информацию о проведении антивирусных проверок на элементах (технических средствах), используемых в информационной системе Администрации в том числе на машинных носителях информации.

В Журнал заносится следующая информация:

- порядковый номер выполнения работ;
- дата выполнения работы;
- наименование работ и проверяемых информационных ресурсов;
- результаты проверки;
- принятые меры;
- расписка исполнителя работ.

Журнал подлежит уничтожению, установленным порядком, после полного заполнения.

Журнал должен быть прошит, пронумерован и удостоверен печатью.

ОБРАЗЕЦ. Журнал антивирусных проверок информационной системы _____ *(указать название ИС)*
Администрации Южского муниципального района

№ п/п	Дата выполнения работы	Наименование работ и проверяемых информационных ресурсов	Результаты проверки	Принятые меры	Подпись исполнителя работ
1	2	3	4	5	6
1.		Обновление антивирусной базы, сканирование дисков	Вирусов не обнаружено		
2.		Антивирусная проверка технических средств информационной системы,	Вирусов не обнаружено	Лечение проведено антивирусными средствами.	
3.		Обновление антивирусной базы. Антивирусная проверка средств информационной системы.	Обнаружен вирус «Flame».	Вирус удален. О заражении доложено администратору безопасности информационной системы	
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18.					
19.					
20.					

Приложение № 23
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Типовая форма

Журнал
учета машинных носителей конфиденциальной информации и персональных данных информационной системы Администрации Южского муниципального района

_____ *(указать название информационной системы)*
Администрации Южского муниципального района

_____

(дата начала ведения журнала)

_____

(наименование юридического лица)

_____

(адрес (место нахождения) постоянно действующего исполнительного органа юридического лица)

_____

(государственный регистрационный номер записи о государственной регистрации юридического лица)

Ответственное лицо: _____

_____

(фамилия, имя, отчество (в случае, если имеется), должность лица (лиц), ответственного за ведение журнала)

_____

(фамилия, имя, отчество (в случае, если имеется) руководителя юридического лица)

Подпись: _____

М.П.

Инструкция по заполнению
Журнала учета машинных носителей конфиденциальной информации и персональных данных информационной системы Администрации Южского муниципального района

Журнал учета машинных носителей конфиденциальной информации и персональных данных информационной системы Администрации Южского муниципального района (далее – Журнал), содержит перечень носителей, используемых при обработке конфиденциальной информации (персональных данных).

В Журнал заносится следующая информация:

- порядковый номер записи;
- регистрационный номер носителя;
- тип носителя и объем;
- гриф конфиденциальности К/ПДн (конфиденциальная информация/персональные данные);
- отметка о получении носителя пользователем (указывается дата получения, подпись и фамилия пользователя);
- отметка о приеме носителя (указывается дата приема, подпись и фамилия лица, получившего носитель от пользователя);
- состав информации на носителе (конфиденциальная информация/персональные данные);
- отметка об отправке носителя (с указанием даты и номера сопроводительного письма) или уничтожении носителя (информации) (с указанием даты и номера акта)

Журнал подлежит уничтожению, установленным порядком, после полного заполнения.

Журнал должен быть прошит, пронумерован и удостоверен печатью.

Журнал учета машинных носителей конфиденциальной информации и персональных данных информационной системы _____ *(указать название информационной системы)*

Администрации Южского муниципального района

№ п/п	Регистра-ционный номер носителя	Тип носителя и объем	Гриф конфиденц-иальности (К / ПДн)	Отметка о получении носителя			Отметка о приеме носителя			Состав информации на носителе	Отметка об отправке (с указанием даты и номера сопроводительного письма) уничтожении (с указанием даты и номера акта)
				Дата	Подпись	Фамилия	Дата	Подпись	Фамилия		
1	2	3	4	5	6	7	8	9	10	11	12

Приложение № 24
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Типовая форма

Журнал
учета средств защиты информации, технической и эксплуатационной документации информационной системы Администрации Южского муниципального района

_____ *(указать название информационной системы)*
Администрации Южского муниципального района

_____
(дата начала ведения журнала)

_____
(наименование юридического лица)

_____
(адрес (место нахождения) постоянно действующего исполнительного органа юридического лица)

_____
(государственный регистрационный номер записи о государственной регистрации юридического лица)

Ответственное лицо: _____
_____
(фамилия, имя, отчество (в случае, если имеется), должность лица (лиц), ответственного за ведение журнала)

_____
(фамилия, имя, отчество (в случае, если имеется) руководителя юридического лица)

Подпись: _____
М.П.

Инструкция по заполнению
Журнала учета средств защиты информации информационной системы, технической и эксплуатационной документации информационной системы Администрации Южского муниципального района

Журнал учета средств защиты информации, технической и эксплуатационной документации информационной системы Администрации Южского муниципального района (далее – Журнал), содержит информацию об используемых средствах защиты информации (СЗИ), технической и эксплуатационной документации к ним.

В Журнал заносится следующая информация:

- наименование СЗИ, технической и эксплуатационной документации, ключевых документов;
- регистрационные номера СЗИ, технической и эксплуатационной документации, ключевых документов, номера серий ключевых документов;
- номера экземпляров ключевых документов;
- отметка о получении (указывается от кого получены, с указанием даты и номера сопроводительного письма, акта приема);
- отметка о выдаче (указывается АРМ, на который установлено СЗИ, фамилия пользователя, дата получения (установки) СЗИ, подпись);
- отметка о подключении (установке) СЗИ (указывается фамилия лица, производившего подключение (установку) СЗИ, дата подключения (установки) и подпись лица, производившего подключение (установку), номера аппаратных средств, в которые установлено или к которым подключено СЗИ);
- отметка об изъятии СЗИ из аппаратных средств, уничтожении ключевых документов (дата изъятия (уничтожения), фамилия исполнителя, производившего изъятие СЗИ, номер акта и подпись, при уничтожении – подпись).

Журнал подлежит уничтожению, установленным порядком, после полного заполнения.

Журнал должен быть прошит, пронумерован и удостоверен печатью.

№ п/п	Наименование средства защиты информации, эксплуатационной и технической документации к нему, ключевых документов	Регистрационные номера СЗИ, эксплуатационной и технической документации к нему, номера серий ключевых документов	Номера экземпляров ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получено	Дата и номер сопроводительного письма	Ф.И.О. пользователя СЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СЗИ			Отметка об изъятии СЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. ответственного лица, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключено средство защиты информации	Дата изъятия (уничтожения)	Ф.И.О. ответственного лица, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение № 25
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Типовая форма

Журнал
учета ремонтно-восстановительных работ на основных технических средствах информационной системы Администрации Южского муниципального района

_____ *(указать название информационной системы)*
Администрации Южского муниципального района

_____
(дата начала ведения журнала)

_____
(наименование юридического лица)

_____
(адрес (место нахождения) постоянно действующего исполнительного органа юридического лица)

_____
(государственный регистрационный номер записи о государственной регистрации юридического лица)

Ответственное лицо: _____
_____
(фамилия, имя, отчество (в случае, если имеется), должность лица (лиц), ответственного за ведение журнала)

_____
(фамилия, имя, отчество (в случае, если имеется) руководителя юридического лица)

Подпись: _____
М.П.

Инструкция по заполнению
Журнала учета ремонтно-восстановительных работ на основных технических средствах информационной системы_____ *(указать название информационной системы)*
Администрации Южского муниципального района

Журнал учета ремонтно-восстановительных работ на основных технических средствах информационной системы_____ *(указать название информационной системы)* (далее – Журнал), содержит информацию о проведении ремонтно-восстановительных работ на технических средствах, используемых в информационной системе.

В Журнал заносится следующая информация:

- порядковый номер записи;
- наименование технического средства;
- инвентарный (заводской) номер технического средства;
- краткое описание ремонтных работ;
- фамилия специалиста, проводившего ремонтные работы и его подпись;
- отметка о приеме технического средства после ремонта (указывается дата приема, подпись);
- в примечании указывается дополнительная информация.

Журнал подлежит уничтожению, установленным порядком, после полного заполнения.

Журнал должен быть прошит, пронумерован и удостоверен печатью.

Журнал учета ремонтно-восстановительных работ на основных технических средствах информационной системы_____ *(указать название информационной системы)*

Администрации Южского муниципального района

№ п/п	Наименование технического средства	Инвентарный (заводской) номер тех. средства	Краткое описание ремонтных работ	Фамилия специалиста, проводившего ремонтные работы	Подпись специалиста, проводившего работы	Фамилия и подпись лица, принявшего тех. средство после ремонта	Дата получения	Примечание
1	2	3	4	5	6	7	8	9

Приложение № 26
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Типовая форма

Журнал
учета мероприятий по контролю режима защиты конфиденциальной информации и персональных данных и выполнения обязательных процедур в информационной системе Администрации Южского муниципального района

_____ *(указать название информационной системы)*
Администрации Южского муниципального района

_____
(дата начала ведения журнала)

_____
(наименование юридического лица)

_____
(адрес (место нахождения) постоянно действующего исполнительного органа юридического лица)

_____
(государственный регистрационный номер записи о государственной регистрации юридического лица)

Ответственное лицо: _____
_____
(фамилия, имя, отчество (в случае, если имеется), должность лица (лиц), ответственного за ведение журнала)

_____
(фамилия, имя, отчество (в случае, если имеется) руководителя юридического лица)

Подпись: _____
М.П.

Инструкция по заполнению
Журнала учета мероприятий по контролю режима защиты конфиденциальной информации (персональных данных) и выполнения обязательных процедур в информационной системе _____ *(указать название информационной системы)* **Администрации Южского муниципального района**

Журнал учета мероприятий по контролю режима защиты конфиденциальной информации (персональных данных) и выполнения обязательных процедур в информационной системе _____ *(указать название информационной системы)* (далее – Журнал), содержит информацию: о проведении мероприятий по контролю, соблюдения пользователями установленных порядка и правил обработки конфиденциальной информации (персональных данных) в информационной системе _____ *(указать название информационной системы)*, в том числе при использовании машинных носителей информации, о результатах проверки установленного программного обеспечения и его компонентов, о мероприятиях по очистке (стиранию) временных файлов, о проведении процедуры резервного копирования конфиденциальной информации (персональных данных).

В Журнале фиксируются:

- плановые (при наличии плана) и внеплановые мероприятия по контролю;
- результаты проверки установленного программного обеспечения и его компонентов;
- мероприятия по очистке (стиранию) временных файлов;
- сведения о проведении процедуры резервного копирования конфиденциальной информации (персональных данных).
- сведения об инцидентах безопасности, в т.ч. при возникновении нештатных ситуаций.

В Журнал заносится следующая информация:

- порядковый номер;
- дата проведения мероприятия;
- краткое содержание проводимого мероприятия, проверяемые вопросы;
- результаты мероприятия с указанием выявленных / не выявленных нарушений;
- фамилия и подпись лиц (а) проводивших (проводившего) мероприятие по контролю.

Журнал подлежит уничтожению, установленным порядком, после полного заполнения.

Журнал должен быть прошит, пронумерован и удостоверен печатью.

Журнал учета мероприятий по контролю режима защиты конфиденциальной информации (персональных данных) и выполнения обязательных процедур в информационной системе ________________ *(указать название информационной системы)*

Администрации Южского муниципального района

№ п/п	Дата	Мероприятие	Результаты	Фамилия, подпись
1	2	3	4	5

Приложение № 27
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Типовая форма

Журнал
учета учетных записей пользователей информационной системы Администрации Южского муниципального района

_____ *(указать название информационной системы)*
Администрации Южского муниципального района

_____
(дата начала ведения журнала)

_____
(наименование юридического лица)

_____
(адрес (место нахождения) постоянно действующего исполнительного органа юридического лица)

_____
(государственный регистрационный номер записи о государственной регистрации юридического лица)

Ответственное лицо: _____

_____
(фамилия, имя, отчество (в случае, если имеется), должность лица (лиц), ответственного за ведение журнала)

_____
(фамилия, имя, отчество (в случае, если имеется) руководителя юридического лица)

Подпись: _____

М.П.

Инструкция по заполнению
Журнала учета учетных записей пользователей информационной системы
_____ *(указать название информационной системы)*
Администрации Южского муниципального района

Журнал учета учетных записей пользователей информационной системы _____ *(указать название информационной системы)* (далее – Журнал), содержит информацию об идентификаторах, о присвоении их пользователям (в соответствии с утвержденным перечнем должностей), которым в зависимости от установленных прав доступа присвоены идентификаторы, о выдаче и блокировании идентификаторов.

В Журнал заносится следующая информация:

- порядковый номер;
- сформированный идентификатор;
- пользователь, которому присвоен соответствующий идентификатор;
- дата выдачи идентификатора пользователю;
- дата блокирования идентификатора.

Журнал подлежит уничтожению, установленным порядком, после полного заполнения.

Журнал должен быть прошит, пронумерован и удостоверен печатью.

Журнал учета учетных записей пользователей информационной системы

__________________ *(указать название информационной системы)*

Администрации Южского муниципального района

№ п/п	Идентификатор	Пользователь	Дата выдачи идентификатора	Дата блокирования идентификатора
1	2	3	4	5

Приложение № 28
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Типовая форма

Журнал
учета печатных документов информационной системы Администрации Южского муниципального района

_____ *(указать название информационной системы)*
Администрации Южского муниципального района

_____
(дата начала ведения журнала)

_____
(наименование юридического лица)

_____
(адрес (место нахождения) постоянно действующего исполнительного органа юридического лица)

_____
(государственный регистрационный номер записи о государственной регистрации юридического лица)

Ответственное лицо: _____
_____
(фамилия, имя, отчество (в случае, если имеется), должность лица (лиц), ответственного за ведение журнала)

_____
(фамилия, имя, отчество (в случае, если имеется) руководителя юридического лица)

Подпись: _____
М.П.

Инструкция по заполнению
Журнала учета печатных документов информационной системы _____
(указать название информационной системы) **Администрации Южского муниципального района**

Журнал учета печатных документов информационной системы _____ *(указать название информационной системы)* (далее – Журнал), содержит информацию о дате и времени выдачи (обращения к подсистеме вывода), спецификацию устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа, идентификатор субъекта доступа, запросившего документ, регистрацию запуска (завершения) программ и процессов (заданий, задач).

В Журнал заносится следующая информация:

- порядковый номер;
- дата и время начала печати;
- регистрационный номер устройства печати;
- регистрационный номер устройства печати;
- уровень конфиденциальности документа;
- фамилия и инициалы, лица, осуществляющего печать документа;
- дата и время окончания печати.

Журнал подлежит уничтожению, установленным порядком, после полного заполнения.

Журнал должен быть прошит, пронумерован и удостоверен печатью.

Журнал учета печатных документов информационной системы

___________________ *(указать название информационной системы)*

Администрации Южского муниципального района

№ п/п	Дата и время начала печати	Регистрационный номер устройства печати	Наименование документа	Уровень конфиденци-альности документа	Фамилия, инициалы	Дата и время окончания печати
1	2	3	4	5	6	7

Приложение № 29
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Типовая форма Акта об уничтожении персональных данных субъекта (ов) персональных данных (в случае достижения целей обработки)

РАЗРЕШАЮ УНИЧТОЖИТЬ

_____
_____
_____
(должность, ФИО руководителя)
«__» _____ 201__ г.

Акт об уничтожении бумажных носителей персональных данных

Комиссия в составе:

	Ф.И.О.	**Должность**
Председатель		
Члены комиссии		

провела отбор бумажных носителей персональных данных и установила, что, в соответствии с требованиями руководящих документов по защите информации, персональные данные, зафиксированные на них, подлежат гарантированному уничтожению:

№ п/п	**Дата окончания срока обработки зафиксированных на носителе персональных данных**	**Название бумажного носителя**

Всего подлежит уничтожению:

_____ носителей
(цифрами и прописью)

Перечисленные бумажные носители персональных данных уничтожены путем _____.
(разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

Председатель: _____ _____
(подпись) *(расшифровка подписи)*

Члены комиссии: _____ _____
(подпись) *(расшифровка подписи)*

_____ _____
(подпись) *(расшифровка подписи)*

_____ _____
(подпись) *(расшифровка подписи)*

РАЗРЕШАЮ УНИЧТОЖИТЬ

_____
_____
_____
(должность, ФИО руководителя)
«__» _____ 201__ г.

Акт об уничтожении машиночитаемых носителей и электронных файлов, содержащих персональные данные

Комиссия в составе:

	Ф.И.О.	**Должность**
Председатель		
Члены комиссии		

провела отбор съемных носителей персональных данных, файлов и папок, содержащихся в информационной системе персональных данных, и установила, что, в соответствии с требованиями руководящих документов по защите информации, персональные данные, зафиксированные на них, подлежат гарантированному уничтожению:

№ п/п	**Дата окончания срока обработки зафиксированных на носителе персональных данных**	**Учетный номер съемного носителя или наименование технического средства ИС, на котором уничтожаются файлы**	**Примечание**

Всего съемных носителей _____
(цифрами и прописью)

На съемных носителях уничтожены персональные данные путем стирания ее с помощью возможностей операционной системы _____.

Перечисленные съемные носители уничтожены путем_____
_____
(механического уничтожения, сжигания, разрезания, деформирования и т.п.).

Председатель: _____ _____
(подпись) *(расшифровка подписи)*

Члены комиссии: _____ _____
(подпись) *(расшифровка подписи)*

_____ _____
(подпись) *(расшифровка подписи)*

_____ _____
(подпись) *(расшифровка подписи)*

Приложение № 30
к распоряжению «О назначении ответственных лиц и об утверждении документов по защите конфиденциальной информации и персональных данных, обрабатываемых в информационных системах Администрации Южского муниципального района от 29.12.2017г. № 1092-р

Типовая форма

Журнал
учета мероприятий по контролю эффективности использования применяемых средств защиты информации информационной системы Администрации Южского муниципального района

_____ *(указать название информационной системы)*
Администрации Южского муниципального района

_____
(дата начала ведения журнала)

_____
(наименование юридического лица)

_____
(адрес (место нахождения) постоянно действующего исполнительного органа юридического лица)

_____
(государственный регистрационный номер записи о государственной регистрации юридического лица)

Ответственное лицо: _____
_____
(фамилия, имя, отчество (в случае, если имеется), должность лица (лиц), ответственного за ведение журнала)

_____
(фамилия, имя, отчество (в случае, если имеется) руководителя юридического лица)

Подпись: _____
М.П.

Инструкция по заполнению
Журнала учета мероприятий по контролю эффективности использования применяемых средств защиты информации информационной системы _____ *(указать название информационной системы)* **Администрации Южского муниципального района**

Журнал учета мероприятий по контролю эффективности использования применяемых средств защиты информации информационной системы _____ *(указать название информационной системы)* (далее – Журнал), содержит информацию: о проведении мероприятий по контролю эффективности применяемых средств защиты информации, о выявлении ненадлежащих режимов работы системы защиты, прогнозировании и превентивном реагировании на новые угрозы безопасности информации, о результатах проверки эффективности используемых средств защиты информации и их компонентов, об инцидентах безопасности, в т.ч. при возникновении нештатных ситуаций.

В Журнале фиксируются:

- плановые (при наличии плана) и внеплановые мероприятия по контролю;
- результаты проверки эффективности используемых средств защиты информации и их компонентов;
- мероприятия по выявлению ненадлежащих режимов работы системы защиты (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), прогнозирование и превентивное реагирование на новые угрозы безопасности информации.
- сведения об инцидентах безопасности, в т.ч. при возникновении нештатных ситуаций.

В Журнал заносится следующая информация:

- порядковый номер;
- дата проведения мероприятия;
- краткое содержание проводимого мероприятия, проверяемые вопросы;
- результаты мероприятия с указанием выявленных / не выявленных нарушений;
- фамилия и подпись лиц (а) проводивших (проводившего) мероприятие по контролю.

Журнал подлежит уничтожению, установленным порядком, после полного заполнения.

Журнал должен быть прошит, пронумерован и удостоверен печатью.

Журнал учета мероприятий по контролю эффективности использования применяемых средств защиты информации информационной системы

_____ *(указать название информационной системы)*

Администрации Южского муниципального района

№ п/п	Дата	Мероприятие	Результаты	Фамилия, подпись
1	2	3	4	5