АДМИНИСТРАЦИЯ ОКТЯБРЬСКОГО МУНИЦИПАЛЬНОГО РАЙОНА ПЕРМСКОГО КРАЯ

РАСПОРЯЖЕНИЕ

01.03.2018 № 62-266-01-06

Об утверждении должностной инструкции Администратора безопасности информационных систем Администрации Октябрьского муниципального района Пермского края

В соответствии с требованиями Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»:

1. Возложить на Сектор по информационному и техническому обеспечению Администрации Октябрьского муниципального района (далее - Сектор) функции Администратора безопасности информационных систем структурных подразделений Администрации Октябрьского муниципального района.
2. Утвердить прилагаемую должностную инструкцию Администратора безопасности информационных систем структурных подразделений Администрации Октябрьского муниципального района.
3. Определить, что все работники Сектора являются Администраторами безопасности информационных систем. Ведущий инженер данного сектора является ответственным Администратором безопасности.
4. Поручить Сектору разработать в 2-х недельный срок со дня подписания распоряжения:
   - Журнал антивирусных проверок;
   - Журнал учета логинов;
   - Журнал учета обращения субъектов персональных данных;
   - Журнал учета средств защиты информации (СЗИ).
5. Кадровому сектору Администрации Октябрьского муниципального района внести дополнения к основным должностным инструкциям работников Сектора в соответствии с настоящим распоряжением.
6. Контроль за исполнением настоящего распоряжения оставляю за собой.

Глава муниципального района-
глава Администрации Октябрьского
муниципального района Пермского края Г.В. Поезжаев

УТВЕРЖДЕНА:
распоряжением Администрации
Октябрьского муниципального района
Пермского края от 01.03.2018 № 62-266-01-06

Должностная инструкция
Администратора безопасности информационных систем структурных подразделений Администрации Октябрьского муниципального района

I. Общие положения

1.1. Настоящая инструкция определяет уровень квалификации, круг ответственности и должностные обязанности администратора безопасности информационных систем персональных данных в Администрации Октябрьского муниципального района Пермского края (далее - Администрация района).

1.2. Определения и сокращения

В настоящей инструкции приняты следующие сокращения:

АВЗ — антивирусная защита;
Администратор — администратор безопасности информационных систем персональных данных;
АРМ – автоматизированное рабочее место;
ИС — информационная система;
ЛВС — локальная вычислительная сеть;
НСД — несанкционированный доступ;
ОС — операционная система;
СЗИ – средства защиты информации;
СКЗИ — средства криптографической защиты информации;
ЭП – электронная подпись.

1.3. Настоящая инструкция разработана в соответствии с требованиями:

- Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных»;
- постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа ФСТЭК России от 18.02.2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
- ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения
- ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.

1.4. Инструкция определяет основные задачи, функции, обязанности, права и ответственности администратора безопасности информационных систем в Администрации района.

1.5. Администратор безопасности назначается распоряжением Администрации района, из сотрудников Аппарата Администрации района, выполняющим функции по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники ИС, в пределах своей зоны ответственности.

1.6. Закрепление функциональных обязанностей и разделение зон ответственности производится распорядительным документом по Администрации района.

1.7. В своей деятельности Администратор руководствуется требованиями действующих федеральных законов, общегосударственных, ведомственных, а также внутренних нормативных документов по вопросам защиты информации и обеспечивает их выполнение пользователями ИС.

1.8. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам защиты информации и не исключает обязательного выполнения их требований.

II. Состав нормативно-методического обеспечения

2.1. Администратор для обеспечения соответствия уровня своей квалификации должностным обязанностям должен владеть нормативно-методическим обеспечением, приведенным в таблице 1.

Таблица 1

№ п/п	Нормативно-методическое обеспечение
1	Федеральный закон РФ от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»
2	Федеральный закон от 27.07.2006г №152-ФЗ «О персональных данных»
3	Федеральный закон от 06.04.2011г №63-ФЗ «Об электронной подписи»
4	Федеральный закон от 04.05.2011г. №99-ФЗ «О лицензировании отдельных видов деятельности»
5	Указ Президента Российской Федерации от 06.03.1997 г. №188 «Перечень сведений конфиденциального характера»
6	Указ Президента РФ от 12.05.2004 №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
7	Постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
8	Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных системах персональных данных»
9	Приказ ФСБ РФ от 27.12.2011 №796 "Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра"
10	Приказ ФСБ РФ от 09.02.2005 №66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)"
11	Приказ ФАПСИ №152 от 13.06.2001
12	Нормативные документы ФСТЭК России в части обеспечения защиты конфиденциальной информации
13	Нормативные документы ФСБ России в части использования СКЗИ при защите конфиденциальной информации
14	Организационно распорядительные документы Администрации района и вышестоящих органов

III. Состав специальных знаний Администратора

3.1. Администратор для обеспечения соответствия уровня своей квалификации должностным обязанностям должен владеть специальными знаниями, приведенными в таблице 2.

Таблица 2

№п/п	Специальные знания
1	Операционные системы семейства Windows на уровне администратора безопасности ОС
2	Сетевые технологии на уровне администратора безопасности ЛВС и администратора безопасности информационных сервисов
3	Средства криптографической защиты информации на уровне администратора
4	Средства защиты информации от НСД на уровне администратора
5	Системы АВЗ на уровне администратора
6	Средства ЭП

3.2. В своей деятельности Администратор руководствуется:

- действующим законодательством РФ;
- руководящими документами регуляторов в области защиты информации;
- Организационно распорядительными документами Администрации района и вышестоящих органов;
- заданиями главы муниципального района - главы администрации Октябрьского муниципального района, либо ответственным лицом за организацию обработки персональных данных в Администрации района.

3.3. На время отсутствия Администратора его замещение возлагается на должностное лицо, назначаемое распоряжением Администрации района.

IV. Состав должностных обязанностей Администратора

4.1. В сферу ответственности Администратора входит исполнение следующих обязанностей, приведенных в таблице 3.

Таблица 3

№п/п	Должностная обязанность
1.	Выполнять мероприятия по соблюдению требований информационной безопасности в подразделениях Администрации района
2.	Участвовать в составе рабочих групп при проведении контрольно-ревизионных мероприятий по соблюдению требований информационной безопасности в подразделениях Администрации района
3.	Обеспечивать организацию мероприятий по разработке и актуализации нормативных документов по ИБ Администрации района
4.	Отслеживать изменения в законодательной базе по вопросам обеспечения информационной безопасности с подготовкой докладных записок руководителю направления/подразделения
5.	Разрабатывать и актуализировать внутренние требования, методик, инструкций и регламентов по обеспечению ИБ в подразделениях Администрации района с учетом реальных режимов эксплуатации ИС для последующего их согласования и включения в нормативную базу по ИБ Администрации района

№п/п	Должностная обязанность
6.	Осуществлять мероприятия по созданию и модернизации систем ИБ Администрации района
7.	Организовывать и участвовать в расследованиях инцидентов информационной безопасности Администрации района
8.	Организовывать и участвовать в мероприятиях по оценке защищенности конфиденциальной информации, обрабатываемой в ИС
9.	Оказывать практическую помощь по вопросам информационной безопасности работникам Администрации района, не являющихся техническими работниками
10.	Организовывать и обеспечивать сохранность зафиксированной на бумажных и электронных носителях конфиденциальной информации
11.	Вести учет (по вопросам обеспечения безопасности информации) и знать перечень установленных в подразделениях Администрации района СЗИ и перечень задач, решаемых с их использованием
12.	Вести журнал учета средств защиты информации, эксплуатационной и технической документации к ним
13.	Вести журнал учета машинных носителей персональных данных
14.	Осуществлять непосредственное управление режимами работы и административную поддержку функционирования (настройку и сопровождение) применяемых на автоматизированных рабочих местах специальных программных и программно-аппаратных СЗИ
15.	Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных АРМ и серверов, осуществлять проверку работоспособности системы защиты после установки (обновления) программных средств ИС
16.	Периодически проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки (выборочное тестирование)
17.	Контролировать соответствие технического паспорта ИС фактическому составу (комплектности) ИС и вести учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения в ИС)
18.	Периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищенных АРМ
19.	Вести журнал учета нештатных ситуаций, фактов вскрытия и опечатывания АРМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств ИС
20.	Проводить периодический инструктаж сотрудников (пользователей ИС) по правилам работы с используемыми средствами и системами зашиты информации
21.	Участвовать в разработке и знать перечень защищаемых информационных ресурсов

4.2. Администратор разрабатывает для ИС решения по:

– определению информационных связей между сегментами сети и требований к их изоляции;

– определению списка устройств, логических дисков, каталогов общего пользования, с указанием состава допущенных к ним пользователей и режимов допуска;

– осуществлению контроля над использованием разделяемых ресурсов;

– разработке порядка выхода пользователей в сети связи общего пользования и использованию встроенных СЗИ в сервисных программах;

– определению режимов использования СЗИ: защита паролей, защита в протоколах передачи данных, шифрование файлов, подключение алгоритмов криптографической защиты;

– разработке политики аудита: определению состава регистрируемых событий и списка лиц, имеющих допуск к журналам аудита;

– осуществлению учета и периодического контроля над составом и полномочиями пользователей ИС;

– контролю и требованию соблюдения установленных правил по организации парольной защиты в ИС Администрации района;

– осуществлению оперативного контроля над работой пользователей защищенных АРМ, анализа содержимого журналов событий операционных систем, систем управления базами данных, пакетов прикладных программ и СЗИ всех АРМ и реагированию на возникающие внештатные ситуации;

– обеспечению строгого выполнения требований по обеспечению безопасности информации при организации технического обслуживания АРМ и отправке их в ремонт (контролировать стирание информации на съемных носителях);

– организации учета, хранения, приема и выдачи персональных идентификаторов ответственным исполнителям, осуществление контроля над правильностью их использования;

– осуществлению периодического контроля над порядком учета, создания, хранения и использования резервных и архивных копий массивов данных;

– своевременному и точному отражению изменений в организационно-распорядительных и нормативных документах по управлению СЗИ, установленных в ИС по указанию руководства;

– контролю обеспечения защиты конфиденциальной информации при взаимодействии пользователей с информационными сетями связи общего пользования.

4.3. Администратор наделен функцией контролировать эффективность защиты информации, в том числе:

– проводить работу по выявлению возможности вмешательства в процесс функционирования ИС и осуществления НСД к информации и техническим средствам АРМ;

– докладывать ответственному по обеспечению безопасности о выявленных угрозах безопасности информации, обрабатываемой в ИС, об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ;

– участвовать в расследовании причин возникновения нарушений и внештатных ситуаций в ИС.

4.4. Администратору запрещается:

– используя служебное положение, создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к информации и предоставлять его другим с целью ознакомления, модификации, копирования, уничтожения, блокирования доступа к информации;

– использовать ставшие доступными в ходе исполнения обязанностей идентификационные данные пользователей (имя, пароль, ключи и т. п.) для маскирования своих действий;

– самостоятельно (без согласования с подразделением автоматизации) вносить изменения в настройки серверной части ИС;

– использовать в своих и в чьих-либо личных интересах ресурсы ИС, предоставлять такую возможность другим;

– выключать средства защиты информации без письменной санкции руководства;

– передавать третьим лицам тем или иным способом сетевые адреса, имена, пароли,

информацию о привилегиях пользователей, конфигурационные настройки;

– производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы ИС, блокированию доступа, потере информации без санкции руководства и предупреждения пользователей;

– нарушать правила эксплуатации оборудования ИС;

– корректировать, удалять, подменять журналы аудита.

V. Права и ответственность администратора

5.1. Администратор имеет право:

– получать доступ к программным и аппаратным средствам ИС, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах ИС и АРМ пользователей;

– требовать от пользователей ИС выполнения инструкций по обеспечению безопасности и защите информации в ИС;

– участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИС;

– осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности;

– производить анализ защищенности ИС путем применения специального программного обеспечения, осуществления попыток взлома системы защиты ИС. Такие работы должны проводиться в часы наименьшей информационной нагрузки с обязательным уведомлением сотрудников подразделений автоматизации и обеспечение безопасности информации;

– вносить свои предложения по совершенствованию мер защиты в ИС.

VI. Ответственность

6.1. Администратор несет ответственность за:

- реализацию принятой в Администрации района локальной документации по информационной безопасности;
- программно - технические средства защиты информации, средства вычислительной техники, информационно - вычислительные комплексы, сети и ИС обработки информации, закрепленные за ним распорядительным документом Администрации района, а также за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями;
- разглашение сведений, конфиденциального характера, ставших известными ему по роду работы;
- качество и последствия проводимых им работ по контролю действий пользователей при работе в ИС;
- неисполнение или ненадлежащее исполнение своих обязанностей, предусмотренных настоящей инструкцией;
- несоблюдение действующего законодательства и внутренних документов Администрации района по информационной безопасности и защите персональных данных;
- разглашение служебной и иной конфиденциальной информации, ставшей ему известной в процессе исполнения служебных обязанностей;
- несоблюдение правил и норм охраны труда, техники безопасности и противопожарной защиты.