Приложение 12

к распоряжению администрации Бобровского муниципального района Воронежской области

от 01.11.2013 г. № 372-р

**Должностная инструкция**

**ответственного за обеспечение безопасности персональных данных - администратора безопасности информационных систем персональных данных администрации Бобровского муниципального района Воронежской области**

1. Общие положения

Настоящая Должностная инструкция определяет основные обязанности, права и ответственность ответственного за обеспечение безопасности персональных данных - администратора безопасности информационных систем персональных данных (далее - администратор безопасности) администрации Бобровского муниципального района Воронежской области (далее - администрация).

Администратор безопасности назначается распоряжением администрации.

Администратор безопасности в своей работе руководствуется настоящей Инструкцией и Положением по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в администрации Бобровского муниципального района Воронежской области.

Администратор безопасности является ответственным должностным лицом, уполномоченным на проведение работ по поддержанию достигнутого уровня защиты информационных систем персональных данных (далее - ИСПДн) и ее ресурсов на этапах промышленной эксплуатации и модернизации.

Администратор безопасности осуществляет методическое руководство администрации, системных администраторов и других лиц, допущенных к работе в ИСПДн, в вопросах обеспечения защиты персональных данных (далее - ПДн).

Требования администратора безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

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

2. Основные функции и должностные обязанности администратора безопасности

Администратор безопасности осуществляет следующие основные функции:

- разрабатывает перечень сведений конфиденциального характера;

- участвует в проведении классификации ИСПДн;

- распределяет ответственность по вопросам обработки и защиты ПДн;

- определяет допустимые сроки хранения ПДн по каждой категории ПДн;

- организует подачу уведомлений в уполномоченный орган по защите прав субъектов ПДн;

- заслушивает руководителей и начальников структурных подразделений о принимаемых мерах по состоянию и совершенствованию СЗПДн;

- организует работы по разработке, изменению и уточнению политик, регламентов, стандартов в части защиты ПДн;

- осуществляет организацию плановых и внеплановых проверочных мероприятий;

- организует выполнение требований по защите ПДн в администрации;

- проводит разработку и актуализацию правовых актов, регламентирующих защиту ПДн в администрации;

- проводит ознакомление работников с нормативными документами в области защиты ПДн;

- проводит оценку эффективности принятых мер и применяемых средств защиты ПДн;

- проводит занятия с работниками по изучению организационно-распорядительных документов по всему комплексу вопросов защиты ПДн;

- разрабатывает и актуализирует частные модели угроз безопасности ПДн и технические задания на СЗПДн;

- определяет необходимость обучения работников по вопросам обеспечения безопасности ПДн, а также определяет формы и программы обучения работников администрации в области защиты ПДн;

- контролирует выполнение работниками требований по защите ПДн;

- организует работы по сбору сведений об изменениях в составе и структуре ИСПДн;

- осуществляет контроль соответствия изменений в составе и архитектуре ИСПДн требованиям нормативных документов по защите ПДн, а также внутренних организационно-распорядительных документов администрации;

- контролирует исполнение требований по уничтожению ПДн;

- разрабатывает рекомендации по оптимизации существующих и новых информационных процессов обработки ПДн по критериям соответствия требованиям по защите ПДн и минимизации затрат на создание и эксплуатацию системы защиты ПДн;

- контролирует исполнение требований нормативных документов администрации в области обеспечения безопасности ПДн, структурными подразделениями и работниками;

- организует и осуществляет взаимодействие с регуляторами по вопросам защиты ПДн;

- участвует в аттестации (декларировании соответствия) ИСПДн администрации по требованиям безопасности информации;

- управляет проектами по внедрению систем и средств защиты ПДн;

- контролирует ввод в действие, эксплуатацию СЗПДн;

- проводит расследования инцидентов, связанных с нарушением безопасности ПДн, правил обработки ПДн, принимает меры по недопущению повторения нештатных ситуаций.

Администратор безопасности обязан:

- знать перечень и состав ИСПДн, перечень задач, решаемых их использованием;

- знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по обеспечению защиты ПДн;

- осуществлять установку, настройку и сопровождение средств защиты информации (далее - СЗИ);

- осуществлять учет применяемых СЗИ, эксплуатационной и технической документации к ним;

- обеспечивать обновление антивирусных программ;

- участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн;

- участвовать в приемке новых программных средств;

- обеспечить доступ к защищаемой информации пользователям ИСПДн согласно Разрешительной системы доступа к информационным ресурсам, программным и техническим средствам ИСПДн;

- уточнять в установленном порядке обязанности пользователей ИСПДн;

- проводить резервирование ПДн;

- вести учет носителей ПДн;

- выдавать пользователям личные пароли доступа к средствам ИСПДн;

- анализировать состояние защиты ИСПДн и ее отдельных подсистем;

- контролировать неизменность состояния СЗИ их параметров и режимов защиты;

- контролировать физическую сохранность средств и оборудования ИСПДн;

- контролировать исполнение пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и СЗИ;

- контролировать исполнение пользователями парольной защиты;

- контролировать работу пользователей в сетях общего пользования и международного обмена;

- своевременно анализировать журналы учета событий, с целью выявления возможных нарушений;

- не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач;

- осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования СЗИ ИСПДн;

- оказывать помощь пользователям ИСПДн в части применения СЗИ и консультировать по вопросам введенного режима защиты;

- периодически представлять руководству отчет о состоянии защиты ИСПДн, о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации;

- в случае отказа работоспособности СЗИ ИСПДн принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;

- принимать меры по реагированию, в случае возникновения нештатных и аварийных ситуаций, с целью ликвидации их последствий, участвовать в расследовании причин их возникновения.

3. Организация парольной защиты

Личные пароли доступа к средствам ИСПДн выдаются пользователям администратором безопасности или другим уполномоченным лицом.

Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

Правила формирования пароля:

- пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

- пароль должен состоять не менее чем из 8 символов;

- в пароле должны присутствовать символы трех категорий из числа следующих четырех:

прописные буквы английского алфавита от A до Z;

строчные буквы английского алфавита от a до z;

десятичные цифры (от 0 до 9);

символы, не принадлежащие алфавитно-цифровому набору (например, !, #, %);

- запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

- запрещается выбирать пароли, которые уже использовались ранее.

4. Права администратора безопасности

Администратор безопасности имеет право:

- отключать любые элементы СЗПДн при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей в установленном порядке;

- в установленном порядке изменять конфигурацию элементов ИСПДн и систем (подсистем) защиты персональных данных (далее - СЗПДн);

- требовать от работников соблюдения правил работы в ИСПДн, приведенных в должностных инструкциях;

- требовать от пользователей безусловного соблюдения установленной технологии обработки ПДн и выполнения требований локальных документов, регламентирующих вопросы обеспечения защиты ПДн;

- требовать прекращения обработки информации в случае нарушения установленной технологии обработки ПДн или нарушения функционирования СЗИ;

- вносить свои предложения по совершенствованию СЗПДн;

- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты ПДн в ИСПДн.

5. Ответственность администратора безопасности

Администратор безопасности несет ответственность:

- за ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей инструкцией, другими локальными организационно-распорядительными документами, в соответствии с действующим трудовым законодательством Российской Федерации;

- за правонарушения, совершенные в процессе своей деятельности в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации;

- за разглашение сведений конфиденциального характера и другой защищаемой информации в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации;

На администратора безопасности возлагается персональная ответственность за работоспособность и надлежащее функционирование СЗИ ИСПДн.