



Инструкция
системного администратора информационной системы персональных данных, ответственного за защиту информации и обеспечение безопасности, за организацию обработки персональных данных в информационных системах персональных данных в администрации муниципального образования «Бугровское сельское поселение» Всеволожского муниципального района Ленинградской области.

1. Общие положения

1.1. Системный администратор информационной системы персональных данных администрации муниципального образования «Бугровское сельское поселение» Всеволожского муниципального района Ленинградской области (ИСПДн) (далее - Администратор) назначается на основании распоряжения администрации.

1.2. Администратор подчиняется начальнику сектора по делопроизводству, кадрам, архиву, противодействию коррупции, социальной и молодежной политики, спорту.

1.3. Администратор в своей работе руководствуется настоящей инструкцией, положением по обеспечению безопасности персональных данных, руководящими и нормативными документами ФСТЭК России и регламентирующими документами администрации.

1.4. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн администрации и средств защиты при обработке персональных данных.

1.5. Администратор является должностным лицом, ответственным за реагирование на инциденты безопасности, приводящие к потере защищаемой информации в ИСПДн.

1.6. Администратор должен обладать навыками по методам частичного и полного восстановления работоспособности элементов ИСПДн.

2. Должностные обязанности

Администратор обязан:

2.1. Знать и выполнять требования, действующих нормативных и руководящих документов, а также внутренних инструкций, положений, распоряжений, регламентирующих вопросы обработки и обеспечения безопасности персональных данных в администрации.

Инструкция
системного администратора информационной системы персональных
данных, ответственного за защиту информации и обеспечение безопасности,
за организацию обработки персональных данных в информационных
системах персональных данных
в администрации муниципального образования «Бугровское сельское
поселение» Всеволожского муниципального района» Ленинградской
области.

1. Общие положения

1.1. Системный администратор информационной системы персональных данных администрации муниципального образования «Бугровское сельское поселение» Всеволожского муниципального района Ленинградской области (ИСПДн) (далее - Администратор) назначается на основании распоряжения администрации.

1.2. Администратор подчиняется начальнику сектора по делопроизводству, кадрам, архиву, противодействию коррупции, социальной и молодежной политики, спорту.

1.3. Администратор в своей работе руководствуется настоящей инструкцией, положением по обеспечению безопасности персональных данных, руководящими и нормативными документами ФСТЭК России и регламентирующими документами администрации.

1.4. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн администрации и средств защиты при обработке персональных данных.

1.5. Администратор является должностным лицом, ответственным за реагирование на инциденты безопасности, приводящие к потере защищаемой информации в ИСПДн.

1.6. Администратор должен обладать навыками по методам частичного и полного восстановления работоспособности элементов ИСПДн.

2. Должностные обязанности

Администратор обязан:

2.1. Знать и выполнять требования, действующих нормативных и руководящих документов, а также внутренних инструкций, положений, распоряжений, регламентирующих вопросы обработки и обеспечения безопасности персональных данных в администрации.

2.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);
- аппаратных средств;
- аппаратных и программных средств защиты.

2.3. Обеспечивать работоспособность элементов ИСПДн (АРМ и серверов) и элементов локальной вычислительной сети, задействованных в ИСПДн.

2.4. В целях предотвращения потери защищаемой информации осуществлять резервное копирование баз данных, содержащих персональные данные, а также технологической информации (конфигурационные файлы и др.); осуществлять учет резервных и архивных копий ПО и массивов данных.

2.5. Обеспечивать работоспособность антивирусных средств защиты и своевременность обновления антивирусных баз.

2.6 Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках, возложенных на него функций.

2.7. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.8. Проводить периодический контроль принятых мер по защите информации в пределах, возложенных на него функций.

2.9. Осуществлять прием и выдачу персональных паролей пользователей, а также осуществлять контроль за правильностью использования персонального пароля пользователем ИСПДн.

2.10. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.11. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения защищаемой информации.

2.12. Присутствовать при выполнении технического обслуживания элементов ИСПДн сторонними организациями или физическими лицами.

В кратчайшие сроки, не превышающие одного рабочего дня, принимать меры по восстановлению работоспособности ИСПДн, в случае возникновения внештатных и аварийных ситуаций.

2.13. Участвовать в организации работ по обеспечению защиты информации в ИСПДн;

- 2.14. Доводить до сведения пользователей, осуществляющих доступ к ИСПДн, требования нормативных актов и методических документов в области защиты информации;
- 2.15. Осуществлять контроль за соблюдением пользователями, осуществляющими доступ к ИСПДн, требований по защите информации в ИСПДн;
- 2.16. Осуществлять установку, настройку и сопровождение технических средств защиты;
- 2.17. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн;
- 2.18. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения;
- 2.19. Уточнять в установленном порядке обязанности пользователей ИСПДн по обработке информации ограниченного доступа;
- 2.20. Вести контроль над процессом осуществления резервного копирования объектов защиты;
- 2.21. Анализировать состояние защиты ИСПДн и ее отдельных подсистем;
- 2.22. Контролировать неизменность состояния средств защиты их параметров и режимов защиты;
- 2.23. Контролировать физическую сохранность средств защиты ИСПДн;
- 2.24. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты;
- 2.25. Организовать и контролировать исполнение пользователями парольной политики;
- 2.26. Своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений;
- 2.27. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач;
- 2.28. Не допускать к работе в ИСПДн посторонних лиц;
- 2.29. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн;
- 2.30. Оказывать помощь пользователям ИСПДн в части применения средств защиты и осуществлять консультативную помощь по вопросам информационной безопасности;
- 2.31. В случае потери работоспособности технических средств и программного обеспечения средств защиты ИСПДн принимать меры по их своевременному восстановлению и выявлению причин, приведших к потере работоспособности;

- 2.32. Принимать меры по реагированию, в случае возникновения нештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.
- 2.33. Взаимодействовать с регулирующими органами по вопросам обработки и обеспечения безопасности персональных данных;
- 2.34. Контролировать договоры с третьими лицами на предмет их соответствия требованиям организационно-распорядительных документов по обработке и обеспечению безопасности персональных данных;
- 2.35. Предоставлять необходимую информацию при проведении проверок регулирующими органами и при проведении контрольных мероприятий по обеспечению безопасности персональных данных;
- 2.36. Обеспечивать выполнение требований по обработке и обеспечению безопасности персональных данных в соответствии с «Положением о порядке обработки персональных данных в администрации муниципального образования «Бугровское сельское поселение» Всеволожского муниципального района Ленинградской области и иными нормативными документами в области обработки и защиты персональных данных;
- 2.37. Осуществлять непрерывный контроль действий, пользователей при обработке персональных данных, разъяснять и требовать от пользователей выполнения требований нормативных документов в области обработки и защиты персональных данных;
- 2.38. Участвовать в процессе разработки организационно-распорядительных документов, регламентирующих требования по обеспечению информационной безопасности персональных данных, обрабатываемых в ИСПДн;
- 2.39. Определять необходимость и направлять на обучение пользователей ИСПДн;
- 2.40. Предоставлять консультации пользователей ИСПДн по вопросам автоматизированной и неавтоматизированной обработки персональных данных в рамках своих компетенций;
- 2.41. Организовывать и контролировать своевременное предоставление пользователями ИСПДн доступа к персональным данным и средствам их обработки в объеме, необходимом для выполнения ими своих трудовых обязанностей;
- 2.42. Определять права доступа к персональным данным и автоматизированным средствам обработки персональных данных в рамках своих компетенций;
- 2.43. Обеспечивать выполнение плана периодических проверок условий обработки персональных данных в пределах своих функциональных обязанностей;
- 2.44. Участвовать в разработке плана периодических проверок условий обработки персональных данных.

1. Права Администратора

1.1. Администратор имеет право:

- запрашивать и получать необходимые материалы для организации и проведения работ по вопросам обеспечения защиты информации в ИСПДн;
- привлекать в установленном порядке пользователей для проведения работ по обеспечению защиты информации в ИСПДн;
- требовать от пользователей ИС выполнения инструкций по обеспечению безопасности и защите информации;
- доступа к любым программным и аппаратным ресурсам и любой информации на рабочих станциях пользователей (за исключением информации, закрытой с использованием средств криптозащиты) и средствам их защиты;
- участвовать в проведении служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;
- непосредственно обращаться к руководителям подразделений с требованием прекращения работы в ИСПДн при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности;
- выдвигать и рассматривать предложения о привлечении к проведению работ по обеспечению защиты информации в ИСПДн организаций, имеющих лицензии на право проведения работ в области защиты информации, вносить свои предложения по совершенствованию мер защиты информации в ИСПДн.

2. Ответственность

2.1. На Администратора возлагается персональная ответственность за работу программно-технических и криптографических средств защиты информации и за качество проводимых работ по обеспечению защиты информации на объектах информатизации в соответствии с функциональными обязанностями.

2.2. Администратор несет ответственность по действующему законодательству за разглашение информации ограниченного доступа, ставшей известной ему по роду работы.

2.3. Администратор несет ответственность за реализацию принятой в ИСПДн политики парольной защиты.

2.4. Администратор несет ответственность за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.