АДМИНИСТРАЦИЯ
ПРИСТЕНСКОГО РАЙОНА КУРСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

от 15 октября 2020 № 319-ра

О назначении администратора информационной безопасности в Администрации Пристенского района Курской области

С целью обеспечения исполнения требований Федерального закона Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» и организации работ по обеспечению безопасности персональных данных при их обработке в Администрации Пристенского района Курской области:

1. Назначить администратором информационной безопасности консультанта отдела юридического сопровождения, муниципальных услуг, защиты информации и ИКТ Администрации Пристенского района Курской области - Дронову Анну Александровну.

2. Назначить администратором информационной безопасности, замещающим администратора информационной безопасности на время отсутствия в период командировки, отсутствия ввиду служебной необходимости, отпуска или больничного консультанта отдела юридического сопровождения, муниципальных услуг, защиты информации и ИКТ Администрации Пристенского района Курской области - Надеину Кристину Александровну.

3. Утвердить прилагаемую инструкцию администратора безопасности информации.

4. Контроль за исполнением настоящего распоряжения возложить на заместителя главы администрации, управляющего делами Администрации Пристенского района Курской области - Миронову Н.М.

5. Распоряжение вступает в силу со дня его подписания.

Глава Пристенского района
Курской области **В.В. Петров**

С распоряжением ознакомлен(а): Дронова А.А. 15.10.2020
(подпись, расшифровка подписи, дата)

С распоряжением ознакомлен(а): Кафелина К.А. 15.10.2020
(подпись, расшифровка подписи, дата)

Утверждена
распоряжением Администрации
Пристенского района
Курской области
от 15 октября 2020 № 319-рг

ИНСТРУКЦИЯ
администратора безопасности информации

1. Общие положения

1.1. Администратор безопасности информации (далее – Администратор) назначается распоряжением Администрации Пристенского района Курской области (далее - Администрация).

1.2. Администратор подчиняется руководителю Администрации и ответственному за организацию обработки персональных данных.

1.3. Администратор в своей работе руководствуется настоящей инструкцией, принятыми локальными нормативными актами Администрации в области обработки персональных данных, руководящими и нормативными документами ФСТЭК России, ФСБ России, законодательством РФ в области защиты персональных данных.

1.4. Настоящая инструкция определяет задачи, функции, обязанности, права и ответственность лица, назначенного ответственным за обеспечение безопасности информации (персональных данных) в информационных системах (далее - ИС) Администрации.

1.5. Методическое руководство работой Администратора осуществляется ответственным за организацию обработки персональных данных.

2. Обязанности

Основными действиями Администратора при выполнении своих обязанностей являются:

2.1. Проведение инструктажа и консультации пользователей ИС по соблюдению установленного режима конфиденциальности при обработке конфиденциальной информации (персональных данных) в ИС.

2.2. Взаимодействие с органом по аттестации ИС (организация, имеющая лицензию ФСТЭК России на работы по аттестации информационных систем по безопасности информации) по вопросам обеспечения защиты информации и сопровождения системы защиты информации.

2.3. Управления учетными записями пользователей.

2.4. Выполнение, учет и контроль изменений, вносимых:

– в списки пользователей ИС;

– в перечень защищаемых информационных ресурсов ИС;

– в перечень съемных машинных носителей информации.

2.5. Организация и проведение периодического и внеочередного контроля работы пользователей.

2.6. Контроль выполнения пользователями ИС установленного режима конфиденциальности при обработке защищаемой информации, в том числе, соблюдения режима конфиденциальности при обращении с персональными идентификаторами, со съемными машинными носителями информации.

2.7. Участие в процедурах контроля операций по безопасному удалению личных файлов пользователя при прекращении полномочий учетной записи, форматированию персонального идентификатора (токена) при прекращении полномочий учетной записи и создание новой учетной записи, присвоение электронного идентификатора, пароля новой учетной записи в случае такой необходимости.

2.8. Организация и участие в служебных расследованиях для выяснения причин утечки или воздействия на обрабатываемую в ИС информацию, компрометации паролей (электронных идентификаторов) с целью выяснения величины нанесенного ущерба безопасности информации и выработки новых или совершенствования принятых технических и организационных мер по защите информации от реализации угрозы в будущем.

2.9. При возникновении необходимости, организация и участие в мероприятиях, связанных с событиями вскрытия, опечатывания, модификации состава, ремонта и т.д. технических средств ИС. Опечатывание корпусов технических средств ИС. Составление актов о вскрытии и опечатывании корпусов технических средств.

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

2.11. Информировать ответственного за организацию обработки персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИС.

2.12. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИС или средств защиты.

2.13. Обеспечивать контроль и строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. В случае, если ИС имеет действующий аттестат соответствия требованиям по безопасности информации, вышедшие из строя элементы и блоки средств вычислительной техники заменяются с согласования органа по аттестации, выдавшим аттестат соответствия.

2.14. Присутствовать при выполнении технического обслуживания элементов ИС, сторонними физическими лицами и организациями.

2.15. Принимать меры по реагированию в случае возникновения внештатных и аварийных ситуаций с целью ликвидации их последствий.

2.16. Не допускать к работе на рабочих станциях и серверах структурного подразделения посторонних лиц.

2.17. Осуществлять контроль монтажа оборудования структурного подразделения специалистами сторонних организаций.

2.18. Участвовать в мероприятиях по выбору средств защиты информации.

2.19. Обобщать результаты своей деятельности и готовить предложения по ее совершенствованию.

2.20. При изменении конфигурации автоматизированной системы вносить соответствующие изменения в паспорт АС, обрабатывающей информацию ограниченного доступа. В случае, если ИС имеет действующий аттестат соответствия требованиям по безопасности информации, изменения согласовываются с органом по аттестации, выдавшим аттестат соответствия.

2.21. Обеспечивать контроль и строгое выполнение требований по соблюдению установленного режима эксплуатации и обеспечения безопасности СКЗИ и криптографических ключей.

2.22. Участвовать в периодических мероприятиях по контролю за обеспечением уровня защищенности информации, содержащейся в информационной системе.

3. Права

Администратор имеет право:

3.1. Требовать от пользователей ИС выполнения принятых локальных нормативных актов в области обеспечения безопасности информации.

3.2. Участвовать в разработке мероприятий по совершенствованию системы защиты информации в ИС.

3.3. Обращаться к руководителю Организации и ответственному за организацию обработки персональных данных по вопросам связанных с выполнением обязанностей Администратора.

4. Действия при обнаружении попыток НСД

4.1. При возникновении нештатных ситуаций и/или инцидентов информационной безопасности Администратор руководствуется инструкцией о действиях лиц, допущенных к работе в информационных системах в случае возникновения нештатных ситуаций и иными организационно-распорядительными документами, утвержденными в Администрации.

4.2. К попыткам НСД относятся:

– сеансы работы с телекоммуникационными ресурсами информационной системы незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий, которых не входят операции доступа к определенным данным или манипулирования ими;

– действия третьего лица, пытающегося получить доступ (или получившего доступ) к информационным ресурсам информационной системы с использованием учетной записи администратора или другого пользователя информационной системы, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

4.3. При выявлении факта/попытки НСД Администратор обязан:

– прекратить доступ к информационным ресурсам со стороны выявленного участка НСД;

– доложить в случае необходимости ответственному за безопасность и руководителю Учреждения о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;

– известить начальника структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

– проанализировать характер НСД;

– по решению руководства осуществить действия по выяснению причин, приведших к НСД;

– предпринять меры по предотвращению подобных инцидентов в дальнейшем.

5. Действия по управлению идентификаторами (учетными записями) пользователей и устройств в информационных системах

5.1. К функциям по управлению идентификаторами пользователей и устройств в информационной системе относится:

– 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 оператором периода времени;

– блокирование идентификатора пользователя и (или) устройства.

Администратором должно быть исключено повторное использование идентификатора пользователя в течение не менее одного года;

Администратором должно быть обеспечено блокирование идентификатора пользователя через период времени неиспользования не

более 90 дней.

5.2. К функциям по управлению учетными записями пользователей относится:

– 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);

– верификация 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 не реже одного раза в год;

– предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами.

В информационных системах запрещается использование гостевых (анонимных) и временных учетных записей пользователей, а также более одной привилегированной учетной записи администратора.

Администратор должен оперативно вносить изменения в учетные записи пользователей в случаях изменения сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях.

Управление учетными записями пользователей информационных систем, имеющих аттестат соответствия требованиям безопасности информации, осуществляется в соответствии с техническим паспортом информационной системы и аттестационной документацией.

При необходимости внесения изменений в учетные записи пользователей (изменение, заведение, активация, блокирование, уничтожение), изменения согласовываются с органом по аттестации, выдавшим аттестат соответствия.

5.3. При реализации функций по управлению идентификаторами пользователей и устройств в информационной системе, управлению учетными записями пользователей Администратор руководствуется утвержденной в Администрации организационно-распорядительной документацией и эксплуатационной документацией на средства защиты информации (СЗИ), реализующие соответствующие функции.

В процессе работы администратору запрещается:

–Использовать для постоянного хранения и обработки конфиденциальной информации каталоги несъемных носителей, за исключением выделенных каталогов;

–Осуществлять попытки несанкционированного доступа к ресурсам операционной системы;

–В рамках выделенных ресурсов и полномочий доступа к ним обрабатывать информацию с уровнем конфиденциальности, выше заявленного при регистрации;

–Покидать помещение с незаблокированной учетной записью;

–Отключать установленные средства защиты информации;

–Использовать машинные носители без их предварительной проверки антивирусными средствами;

–Несанкционированно устанавливать программное обеспечение;

–Несанкционированно менять параметры конфигурации ранее установленных программных средств;

–Запрещается передавать в любом виде или сообщать идентификаторы и пароли для доступа другим лицам, в том числе и своим руководителям;

–Хранение пароля на любых твердых носителях, позволяющих другим лицам получить информацию о пароле;

–Использовать информацию, полученную в результате доступа к БД, в целях, не предусмотренных его функциональными обязанностями;

–Ответственность за сохранность и правильное использование информации, ставшей известной в процессе обработки конфиденциальной информации, несет администратор;

–Возможность получения технического доступа к конфиденциальной информации не дает права администратору обработки такой информации, если им не предоставлены права доступа к этой информации. Такие действия рассматриваются как попытки несанкционированного доступа;

–При выявлении инцидентов с доступом к конфиденциальной информации доступ администратора к ней может быть ограничен до окончания расследования инцидента, о чем Администратор уведомляется в кратчайшие сроки. По результатам служебного расследования нарушитель может быть лишен прав доступа к конфиденциальной информации, материалы расследования могут быть направлены в соответствующие службы для привлечения нарушителя к ответственности;

–Администратор несет ответственность за все действия, совершенные от имени его учетной записи, если не доказан факт несанкционированного использования этой учетной записи;

–При нарушениях Администратором правил, связанных с информационной безопасностью, он несет ответственность, установленную действующим законодательством.