АДМИНИСТРАЦИЯ
ПРИСТЕНСКОГО РАЙОНА КУРСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 04 июля 2022 № 387-па

О назначении ответственных за защиту информации и обеспечение защиты персональных данных при их обработке в информационной системе «ЗАГС» отдела ЗАГС Администрации Пристенского района Курской области

Во исполнение Федерального закона №152-ФЗ от 27 июля 2006 года «О персональных данных», постановления Правительства Российской Федерации № 1119 от 1 ноября 2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» Администрация Пристенского района Курской области ПОСТАНОВЛЯЕТ:

1. Назначить ответственным за защиту информации и обеспечение защиты персональных данных при их обработке в информационной системе «ЗАГС» отдела ЗАГС Администрации Пристенского района Курской области - консультанта отдела юридического сопровождения, муниципальных услуг, защиты инфомации и ИКТ – А.А.Дронову.

2. Возложить на консультанта отдела юридического сопровождения, муниципальных услуг, защиты информации и ИКТ Администрации Пристенского района Курской области – А.А. Дронову функциональные обязанности администратора безопасности информации информационной системы «ЗАГС» отдела ЗАГС Администрации Пристенского района Курской области. В случае отсутствия обязанности выполняет сотрудник, исполняющий обязанности консультанта отдела юридического сопровождения, муниципальных услуг, защиты информации и ИКТ Администрации Пристенского района Курской области.

3. Возложить на начальника отдела ЗАГС - Н.Н. Смородину функциональные обязанности администратора информационной системы

«ЗАГС» отдела ЗАГС Администрации Пристенского района Курской области. В случае отсутствия обязанности выполняет сотрудник, исполняющий обязанности начальника отдела ЗАГС Администрации Пристенского района Курской области.

4. Утвердить прилагаемую инструкцию администратора безопасности информации информационной системы.

5. Утвердить прилагаемую инструкцию администратора информационной системы.

6. Отделу организационной, кадровой работы и делопроизводства (Гольцовой Е.Н.) ознакомить сотрудников Администрации Пристенского района Курской области в части касающейся с настоящим постановлением под роспись.

7. Контроль за исполнением настоящего постановления возложить на заместителя главы администрации, управляющего делами Администрации Пристенского района Курской области – В.В. Катыхина.

8. Постановление вступает в силу со дня его подписания.

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

С постановлением ознакомлен (а): Дронова А.А. 04.07.2022

С постановлением ознакомлен (а): Ушт - Смородина Н.Н. 04.07.2022

УТВЕРЖДЕНА
постановлением Администрации
Пристенского района Курской
области
от 04.07.2022 № 387-па

ИНСТРУКЦИЯ
администратора безопасности информации

1. Общие положения

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

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

1.3. Администратор в своей работе руководствуется настоящей инструкцией, принятыми локальными нормативными актами Организации 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) Организации.

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 защите 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 защите 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 защите 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 Организации.

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 Организации 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;

– ведение и контроль использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов;

– 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 и взаимодействующими с ней информационными системами.

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

5.4. 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).

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

5.6. Все пользователи должны иметь ограниченный набор прав доступа, каждый доступ должен быть обоснован производственной необходимостью и предоставляться только для выполнения служебных задач. В случае изменения состава задач пользователя права пользователя должны быть пересмотрены, излишние права отозваны.

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

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

6. Ответственность

6.1. Ответственность за сохранность и правильное использование информации, ставшей известной в процессе обработки конфиденциальной информации несет Администратор.

6.2. Возможность получения технического доступа к конфиденциальной информации не дает права Администратору обработки такой информации, если ему не предоставлены права доступа к этой

информации. Такие действия рассматриваются как попытки несанкционированного доступа.

6.3. 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.

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

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

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;
- использовать удаленный доступ от имени привилегированных учетных записей (администраторов) для администрирования ИС и ее системы защиты информации.

УТВЕРЖДЕНА
постановлением Администрации
Пристенского района Курской
области
от 04.07.2022 № 387-па

ИНСТРУКЦИЯ
администратора информационных систем Администрации Пристенского района Курской области

1. Общие положения

1.1. Настоящая Инструкция определяет обязанности администратора информационных систем Администрации Пристенского района Курской области (далее – Администратор ИС).

1.2. Администратор ИС назначается постановлением Администрации Пристенского района Курской области.

1.3. Администратор ИС в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России, ФСБ России, регламентирующими документами Организации и другими документами в сфере защиты информации.

1.4. Администратор ИС подчиняется руководителю Организации и ответственному за организацию обработки персональных данных.

1.5. Методическое руководство работой Администратора ИС в вопросах обеспечения безопасности информации осуществляется ответственным за защиту информации.

1.6. Администратор ИС отвечает за обеспечение устойчивой работоспособности программных и аппаратных элементов информационной системы.

1.7. Администратор ИС несет персональную ответственность за качество проводимых им работ по обеспечению работоспособности программных и аппаратных элементов информационной системы, в т.ч. за их установку и настройку.

1.8. Администратор ИС при выполнении своих обязанностей должен исключить удаленный доступ от имени привилегированных учетных записей (администраторов) для администрирования информационной системы.

2. Должностные обязанности

Администратор ИС обязан:

2.1. 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.

2.2. Обеспечивать установку, настройку и своевременное обновление элементов автоматизированной системы:

– программного обеспечения автоматизированных рабочих мест (АРМ) (операционные системы, прикладное и специальное программное обеспечение (ПО);

– аппаратных средств;

– аппаратных и программных средств защиты.

2.3. Обеспечивать работоспособность элементов информационной системы и вычислительной сети.

2.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.5. В случае отказа работоспособности технических средств и программного обеспечения элементов информационной системы принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

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

2.7. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации, в пределах возложенных полномочий.

2.8. Информировать Администратора безопасности информационной системы о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам информационной системы.

2.9. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования информационной системы.

2.10.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 защищаемой информации, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации.

2.11.Присутствовать при выполнении технического обслуживания элементов информационной системы, сторонними физическими лицами и организациями.

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

3. Права Администратора ИС

Администратор ИС имеет право:

3.1. Отключать от ресурсов информационной системы пользователей, осуществивших НСД к защищаемым ресурсам информационной системы или нарушивших другие требования по ИБ.

3.2. Давать пользователям обязательные для исполнения указания и рекомендации по вопросам обеспечения нормального функционирования программных и аппаратных элементов информационной системы и локальной вычислительной сети.

3.3. Осуществлять контроль информационных потоков, генерируемых пользователями информационной системы при работе с корпоративной электронной почтой, съемными носителями информации, подсистемой удаленного доступа.

3.4. Осуществлять взаимодействие с руководством и персоналом информационной системы по вопросам нормального функционирования программных и аппаратных элементов информационной системы и локальной вычислительной сети.

3.5. Запрещать устанавливать на автоматизированных рабочих местах нештатное программное и аппаратное обеспечение.

3.6. Запрашивать и получать от начальников и специалистов структурных подразделений Организации информацию и материалы, необходимые для организации своей работы.

3.7. Вносить на рассмотрение руководства предложения по улучшению нормального функционирования программных и аппаратных элементов информационной системы и локальной вычислительной сети.

3.8. Принимать участие в проведении мероприятий по контролю за обеспечением безопасности информации.

3.9. Действовать в обход установленных процедур идентификации и аутентификации только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

4. Ответственность Администратора ИС

4.1. Администраторы информационной системы, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители законодательства РФ в области защиты информации и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.