УТВЕРЖДАЮ
И.о.директора ОБПОУ «КГТТС»
_____ Т.В.Пыжова
Приказ № 299/о от 15.09.2016

ИНСТРУКЦИЯ
администратора безопасности информации

1. Общие положения

1.1. Администратор безопасности информации (далее – Администратор) назначается приказом директора ОБПОУ «КГТТС» (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 безопасности информации) по вопросам обеспечения защиты информации и сопровождения системы защиты персональных данных.

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 персональных данных, 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 и 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 ситуаций 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.

3. Права

Ответственный за обеспечение безопасности персональных данных имеет право:

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

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.

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.