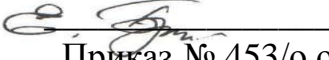


УТВЕРЖДАЮ
Директор ОБПОУ «КГТТС»
 Е.Н.Брежнев
Приказ № 453/о от 30.12.2016

ИНСТРУКЦИЯ
пользователя информационной системы персональных данных Регионального сегмента единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам в Курской области (АИС «Контингент»)
(далее – Информационная система)

1. Общие положения

1.1. Пользователь Информационной системы (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.2. Пользователем является работник организации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной (не автоматизированной) обработки информации, в том числе персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией и прочими действующими локальными нормативными актами в ОБПОУ «КГТТС».

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

2. Функциональные обязанности

2.1. Допуск пользователей для работы в ИСПДн осуществляется в соответствии с приказом директора ОБПОУ «КГТТС» и разрешительной системой доступа.

2.2. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам компьютера. При этом для хранения файлов, содержащих конфиденциальную информацию, разрешается использовать только специально выделенные каталоги на несъемных носителях информации, а также соответствующим образом учтенные съёмные носители информации.

2.3. Присвоение пользователю полномочий доступа к ресурсам компьютера, состав необходимого системного и прикладного программного обеспечения для решения поставленных задач и определение возможного времени работы пользователя Информационной системы осуществляется при первичной регистрации пользователя администратором безопасности информации.

2.4. Пользователь отвечает за правильность включения и выключения технических средств и систем, входа в систему и все действия при работе в Информационной системе.

2.5. Вход пользователя в систему осуществляется на основе ввода персонального пароля. Требования к парольной защите определяется инструкцией по парольной защите.

2.6. В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам пользователя осуществляется **периодическая** (не более чем, через 120 дней) замена пароля постоянного пользователя. Замена личного пароля осуществляется Администратором безопасности информации.

2.7. При работе со съемными носителями информации пользователь каждый раз перед началом работы обязан проверить их на наличие вирусов с использованием установленных антивирусных программ, в соответствии с Инструкцией по антивирусной защите.

3. Ответственность

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

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

3.3. При выявлении инцидентов с доступом к конфиденциальной информации доступ пользователей к ней может быть ограничен до окончания расследования инцидента, о чем пользователь 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.

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

3.5. При нарушениях пользователем правил, связанных с информационной безопасностью, он несет ответственность, установленную действующим законодательством Российской Федерации.

Пользователь обязан:

- знать и строго выполнять установленные правила и обязанности по доступу к защищаемым ресурсам и соблюдению принятого режима информационной безопасности;
- обеспечить правильность вводимых данных;
- своевременно сообщать администратору безопасности об изменениях статуса пользователя;
- незамедлительно сообщить администратору безопасности факты выявления инцидентов с доступом к конфиденциальной информации.

В процессе работы пользователю запрещается:

- использовать для постоянного хранения и обработки конфиденциальной информации каталоги несъемных носителей информации, 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;
- пытаться подменять функции администратора по перераспределению времени работы и полномочий доступа к ресурсам компьютера;
- покидать помещение с незаблокированной учетной записью;
- отключать установленные средства защиты информации;
- использовать машинные носители без их предварительной проверки антивирусными средствами;
- устанавливать программное обеспечение;
- 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.