УТВЕРЖДАЮ
Директор ОБПОУ «КГТТС»
_____Е.Н.Брежнев
Приказ № 314 от 01.09.2015

ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ
администратора безопасности информации в автоматизированных системах объектов информатизации ОБПОУ «КГТТС»

Допуск администратора безопасности информации (далее – администратор) для работы в автоматизированных системах объектов информатизации (далее – АС ОИ) осуществляется в соответствии с приказом директора ОБПОУ «КГТТС» и разрешительной системой доступа.

Администратор 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.

Присвоение администратору полномочий доступа к ресурсам компьютера, состав необходимого системного и прикладного программного обеспечения для решения поставленных задач и определение возможного времени работы администратора в АС ОИ осуществляется при первичной регистрации администратора ответственным за обеспечение режима ограничения доступа к информации (далее – ответственный за безопасность информации).

Администратор отвечает за правильность включения и выключения технических средств и систем, входа в систему и все действия при работе в АС ОИ.

Вход администратора в систему осуществляется на основе ввода имени, присвоенного при первичной регистрации и ввода личного пароля. Требования к парольной защите определяются Инструкцией по парольной защите.

В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам администратора осуществляется периодическая (один раз в месяц) замена пароля постоянного администратора. Замена личного пароля осуществляется администратором самостоятельно.

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.

Администратор 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 ответственному за безопасность информации об изменениях статуса администратора;

– незамедлительно сообщить ответственному за безопасность информации факты выявления инцидентов с доступом к конфиденциальной информации.

В процессе работы администратору 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 ответственного за безопасность информации 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;

– использовать пароль, предоставленный ответственным за безопасность информации для первоначального доступа в качестве постоянного рабочего пароля;

– использование различными администраторами одной и той же учетной записи, даже если администраторы имеют одинаковые полномочия по доступу;

– 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 Российской Федерации.