Приложение 5
Утверждены
постановлением Администрации
Ребрихинского района Алтайского края

от 28.12.2018 №745

ИНСТРУКЦИЯ
по работе пользователей в информационных системах Администрации Ребрихинского района Алтайского края

1. Общие положения

1.1. Данная инструкция определяет общие принципы работы пользователей в информационных системах Администрации Ребрихинского района Алтайского края (далее - ИС). Пользователи ИС несут персональную ответственность за свои действия.

1.2. Допуск пользователей для работы в ИС осуществляется в соответствии с их должностными обязанностями после ознакомления с документами по работе в ИС.

1.3. Доступ пользователей в ИС обеспечивает начальник отдела информатизации Ребрихинского района Алтайского края (далее - администратор безопасности ИС).

2. Порядок работы пользователей в ИС

2.1. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ИС, присвоенными администратором безопасности ИС. При этом для хранения информации ограниченного доступа разрешается использовать только учтенные носители информации (дискеты, компакт-диски, USB Flash-накопители, жесткие диски и т.д.), учтенные по журналу учета и выдачи машинных носителей информации, предназначенных для обработки и хранения информации ограниченного доступа.

2.2. Пользователь ИС отвечает за правильность включения и выключения ПЭВМ, входа/выхода в/из ИС и действия при работе в ней.

2.3. Вход пользователя в ИС осуществляется на основе ввода (по запросу системы) имени (идентификатора), присвоенного при регистрации администратором безопасности ИС, и пароля. Требования к сложности пароля и периодичности его замены установлены в инструкции по организации парольной защиты в ИС.

2.4. В случае отказа ИС в идентификации пользователя, либо не подтверждения личного пароля следует немедленно обратиться к администратору безопасности ИС.

2.5. Резервное копирование, уничтожение и восстановление защищаемой информации осуществляются пользователем в рамках выделенных полномочий, либо администратором безопасности ИС, в

соответствии с инструкцией по организации резервного копирования информации в ИС.

2.6. Перед началом работы с носителями информации пользователь ИС обязан проверить их на наличие вредоносного программного обеспечения с использованием антивирусного программного обеспечения, установленного в ИС, в соответствии с инструкцией по проведению антивирусного контроля в ИС. В случае обнаружения вредоносного программного обеспечения на носителе информации пользователь обязан немедленно сообщить администратору безопасности ИС.

3. В процессе работы пользователю запрещается:

3.1. использовать для хранения и обработки защищаемой информации носители, не учтенные соответствующим образом;

3.2. осуществлять попытки неправомерного доступа к ресурсам ИС других пользователей;

3.3. пытаться подменять функции администратора безопасности ИС по перераспределению времени работы и полномочий доступа к ресурсам ИС;

3.4. оставлять ПЭВМ с незавершенным сеансом. При отсутствии визуального контроля за ПЭВМ, доступ к ПЭВМ должен быть заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>;

3.5. допускать посторонних лиц к ПЭВМ;

3.6. сообщать (или передавать) посторонним лицам атрибуты доступа к ресурсам ИС;

3.7. самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических средств или программного обеспечения;

3.8. открывать общий доступ к папкам на ПЭВМ;

3.9. работать на ПЭВМ при обнаружении неисправности;

3.10. самостоятельно вносить изменения в конфигурацию, размещение ПЭВМ и другие узлы ИС.

4. Ответственность

4.1. Ответственность за допуск пользователя к ресурсам и установленные ему полномочия несет руководитель структурного подразделения.

4.2. Пользователи ИС, нарушившие требования данной инструкции, несут ответственность в соответствии с действующим законодательством и внутренними организационно-распорядительными документами.