**УТВЕРЖДАЮ:**

**Глава Мастюгинского сельского поселения**

**Острогожского муниципального района Воронежской области**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.С. Грызлов**

**«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_2015 г.**

**Инструкция
пользователю автоматизированных систем ИСПДн**

**администрации Мастюгинского сельского поселения Острогожского муниципального района Воронежской области**

Допуск пользователей для работы в ИСПДн «Бухгалтерия», «Кадры», «Административная комиссия» осуществляется в соответствии с распоряжением администрации Мастюгинского сельского поселения Острогожского муниципального района Воронежской области и разрешительной системой доступа.

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.

Присвоение пользователю полномочий доступа к ресурсам компьютера, состав необходимого системного и прикладного программного обеспечения для решения поставленных задач и определение возможного времени работы пользователя в ИСПДн «Бухгалтерия», «Кадры», «Административная комиссия», осуществляется при первичной регистрации пользователя специалистом защиты информации.

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

Вход пользователя в систему осуществляется на основе ввода имени, присвоенного при первичной регистрации и ввода личного пароля. Требования к парольной защите определяется инструкцией по парольной защите.

В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам пользователя осуществляется периодическая (раз в месяц) замена пароля постоянного пользователя. Замена личного пароля осуществляется пользователем 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.

**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 специалисту по защите информации об изменениях статуса пользователя;
* незамедлительно сообщить специалисту по защите информации 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;
* использовать пароль, предоставленный специалистом по защите информации для первоначального доступа в качестве постоянного рабочего пароля;
* использование различными пользователями одной и той же учетной записи, даже если пользователи 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 пользователь.

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.

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.

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

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

* длина пароля должна быть не менее 6 символов;
* в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, \*, % и т.п.);
* пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
* при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;
* личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

Для генерации «стойких» значений паролей могут применяться специальные программные средства.

При наличии технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение специалисту по защите информации.

Опечатанные конверты с паролями исполнителей должны храниться в сейфе. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий должна производиться специалисту по защите информации немедленно.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий администраторов и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой.

В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры по внеплановой смене паролей.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

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

Ведущий специалист Т.А. Деревщикова