Приложение № 10
к приказу Государственного бюджетного учреждения
ветеринарии Тверской области « Селижаровская станция по борьбе
с болезнями животных»

№ ___ от « » _____ 20___ г.

ИНСТРУКЦИЯ
по применению парольной защиты и личных идентификаторов в информационных системах персональных данных

1. Настоящая Инструкция определяет порядок использования, генерации, смены и прекращения действия паролей и личных идентификаторов пользователей в информационных системах персональных данных (ИСПДн) Государственного бюджетного учреждения ветеринарии Тверской области « Селижаровская станция по борьбе с болезнями животных» (далее – ГБУ « Селижаровская СББЖ»), а также контроль действий пользователей при работе с паролями.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, а также контроль действий пользователей при работе с паролями возлагается на администратора безопасности информации.

3. Пароли для всех учетных записей пользователей ИСПДн должны выбираться с учетом следующих требований:

- длина пароля должна быть не менее 5 буквенно-цифровых символов;
- пароль не должен включать в себя легко вычисляемые (угадываемые) сочетания символов (имена, фамилии, отчества, наименования организации и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER, ADM, ADMIN и т.п.);
- максимальное действие пароля - не более чем 90 дней;
- пароль не должен повторяться;
- пользователь не может неправильно ввести пароль учетной записи более 5 раз, в этом случае должна происходить блокировка учетной записи пользователя, до момента снятия блокировки.

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

4.1. При первичной регистрации пользователя в системе пароль ему назначает администратор безопасности информации.

4.2. Пользователи ИСПДн обязаны хранить свой личный пароль втайне от других и не передавать любым способом пароль третьим лицам.

4.3. Пользователь ИСПДн лично должен проводить смену пароля учетной записи регулярно не реже одного раза в три месяца.

5. Привязку идентификатора к пользователю (учетной записи) выполняет администратор безопасности информации.

5.1. Пользователи ИСПДн получают свой идентификатор у администратора безопасности информации.

5.2 В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора безопасности информации.

5.3. Пользователь ИСПДн обязан хранить свой личный идентификатор в недоступных для других сотрудников хранилищах.

5.4. Пользователю ИСПДн запрещается передавать свой личный идентификатор.

5.5. В случае утери личного идентификатора, пользователь ИСПДн должен немедленно доложить об этом администратору безопасности информации.

5.6. При необходимости передачи пароля удаленному легальному пользователю ИСПДн администратор безопасности информации должен обеспечить сохранность передачи данному пользователю пароля путем передачи на электронном носителе в зашифрованном виде, по защищенному каналу связи или путем личной передачи на бумажном носителе в опечатанном конверте. В случае если пользователь не подтвердил факт получения им пароля, администратор безопасности информации должен произвести смену пароля данного пользователя и произвести повторную передачу пароля.

6. При наличии технологической необходимости использования имен и паролей сотрудников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), пароли данных сотрудников должны быть незамедлительно изменены администратором безопасности информации.

7. Полная плановая смена паролей пользователей должна проводиться регулярно, но не реже одного раза в год.

8. В случае прекращения полномочий учетной записи пользователя ИСПДн (увольнение, переход на другую работу, в другой отдел или помещение, а также другие обстоятельства) учетная запись должна быть удалена, а её идентификатор должен быть сдан администратору безопасности информации после окончания последнего сеанса работы данного пользователя в ИСПДн.

9. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администратора безопасности информации или ответственного за организацию обработки персональных данных.

10. В случае компрометации личного пароля или утери личного идентификатора пользователя администратором безопасности информации должны быть немедленно предприняты меры в соответствии с п. 11 настоящей Инструкции.

11. Администратор безопасности информации должен провести служебное расследование для выяснения причин компрометации пароля с целью выработки новых или совершенствования принятых технических и организационных мер по устранению

такой угрозы в будущем, а также выяснению величины ущерба, который может быть нанесен собственнику информационных ресурсов.

Начальник Государственного бюджетного учреждения
ветеринарии Тверской области
« Селижаровская станция по борьбе с
болезнями животных» Л.Н. Ерофеева
«___» _____ 20__ г.

Лист ознакомления

№ п/п	ФИО	Должность	Подпись, дата