Приложение № 6
к приказу Государственного бюджетного учреждения
ветеринарии Тверской области
« Селижаровская станция по борьбе с болезнями животных»

№____ от « » _____ 20___ г.

ТЕХНОЛОГИЧЕСКАЯ ИНСТРУКЦИЯ
по работе администратора безопасности информации информационных систем персональных данных

1. Общие положения

1.1. Администратор безопасности информации - лицо, выполняющее функции по настройке и сопровождению всех программных и технических средств информационных систем персональных данных (ИСПДн)Главного управления, предназначенных для обработки информации, содержащей персональные данные.

1.2. Администратор безопасности информации в пределах своих функциональных обязанностей обеспечивает безопасность информации, обрабатываемой, передаваемой и хранимой в ИСПДн.

1.3. Администратор безопасности информации назначается приказом руководителяГлавного управления «Государственная инспекция по ветеринарии Тверской области» (далее – Главное управление).

1.4. Администратор безопасности информации в своей работе руководствуется положениями нормативно - правовых актов РФ, руководящими документами по безопасности информации, положениями, приказами и нормативными актами министерств и ведомств Российской Федерации и положениями настоящей Инструкции.

2. Основные обязанности

2.1. Основными обязанностями администратора безопасности информации являются:

– управление средствами и системами защиты информации (СЗИ) ИСПДн и поддержание их функционирования;

– восстановление функций программных и технических СЗИ от несанкционированного доступа (НСД) к информации;

– генерация паролей для пользователей ИСПДн;

– формирование и управление списком необходимых реквизитов и значением атрибутов объектов и субъектов доступа;

– назначение прав доступа, полномочий и привилегий пользователей к объектам доступа (программам, файлам, каталогам, портам и устройствам ввода-вывода);

– контроль целостности эксплуатируемого в ИСПДн программного обеспечения, в том числе самих СЗИ, с целью недопущения и выявления несанкционированных модификаций;

– выявление, анализ и устранение уязвимостей и иных недостатков в программном обеспечении;

– текущий, после сбоев и периодический (не реже 1 раза в год) контроль работоспособности средств и систем защиты информации;

– контроль соблюдения пользователями ИСПДн требований инструкций и порядка работы при обработке информации в ИСПДн по вопросам защиты информации от НСД;

– контроль выполнения утвержденной технологии обработки информации в ИСПДн;

– контроль состава технических средств, программного обеспечения и средств зашиты информации;

– контроль за установкой программного обеспечения, запрет установки неразрешённого программного обеспечения (в том числе средств обработки и отладки);

– контроль установки обновлений программного обеспечения;

– обеспечение доступа пользователей (при необходимости)к информации посредствам технологий беспроводного доступа, и контроль за использованием данных технологий;

– контроль за использованием в информационной системе мобильных технических средств;

– выявление подозрительных действий пользователей и попыток НСД к информации, обрабатываемой в ИСПДн, путем анализа системных журналов информационной безопасности при работе в ИСПДн;

– организация антивирусной защиты информации и программных средств в ИСПДн;

– контроль электронного журнала сообщений, и обеспечение доступа к нему лицам, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей;

– определение событий, относящихся к безопасности персональных данных, и подлежащих регистрации;

– определение состава и содержания информации о событиях, относящихся к безопасности персональных данных и подлежащих регистрации;

– просмотр и анализ результатов регистрации событий, относящихся к безопасности персональных данных, и реагирование на них;

– контроль безотказного функционирования технических средств, принятие мер по восстановлению отказавших средств.

–

3. Права

3.1. Администратор безопасности информации имеет право:

– требовать от пользователей ИСПДн выполнения установленной технологии обработки информации, инструкций по обеспечению информационной безопасности ИСПДн;

– останавливать обработку информации в ИСПДн в случаях подтвержденных нарушений установленной технологии обработки данных, приводящих кнарушению функционирования средств защиты информации и технических средств.

4. Ответственность

4.1. На администратора безопасности информации возлагается персональная ответственность за качество и полноту проводимых им работ по обеспечению защиты информации в соответствии с его функциональными обязанностями.

4.2. Администратор безопасности информации несет ответственность по законодательству РФ за нарушение требований нормативно – методических документов по защите информации и настоящей инструкции.

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