УТВЕРЖДАЮ
Директор
ОГБУ «Липецкая облветлаборатория»

_____/ М.А. Зибров

Приложение №3 к Приказу
№ 110 от «29» декабря 2018г.
М.П.

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ОГБУ «Липецкая областная ветеринарная лаборатория»

1. Общие положения

1.1 Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) определяют план и порядок проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

1.2 Основные понятия, используемые в настоящих Правилах, соответствуют основным понятиям, установленным Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон №152-ФЗ).

2. План проведения внутренних проверок

2.1 План проведения внутренних проверок (далее – План) приведен в приложении №1 к настоящим Правилам.

2.2 План содержит перечень внутренних проверок и определяет для каждой из них:

- название проверки;
- периодичность проведения проверки;
- ответственного исполнителя.

2.3 Общий срок проведения проверки не должен превышать 30 рабочих дней.

2.4 Информация о проведенной проверке, дата ее начала и окончания, а также ее результаты, фиксируется в «Журнале учета мероприятий по осуществлению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных» (приложение №2).

3. Порядок проведения внутренних проверок

3.1 **Порядок проведения контроля выполнения обязанностей, предусмотренных Федеральным законом №152-ФЗ, и соблюдения прав субъектов персональных данных**

В ходе проведения проверки необходимо:

– Провести проверку соблюдения условий по обработке персональных данных, совместимых с целями сбора персональных данных;

– Провести проверку наличия согласий субъектов персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством РФ;

– Провести проверку соблюдения требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных;

– Провести проверку наличия запросов или обращений субъектов персональных

данных по предоставлению информации, касающейся обработки их персональных данных, уточнению, блокированию или уничтожению персональных данных;

– Провести проверку выполнения ОГБУ «Липецкая облветлаборатория» в сроки, установленные законодательством РФ, обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных;

– Провести проверку выполнения ОГБУ «Липецкая облветлаборатория» в сроки, установленные законодательством РФ, требования субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

– Провести проверку ведения Журнала учета обращений и запросов субъектов персональных данных по вопросам обработки персональных данных.

3.2 **Порядок проведения контроля выполнения требований, утвержденных Постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»**

В ходе проведения проверки необходимо:

– Провести проверку исполнения обязанностей по соблюдению условий хранения материальных носителей персональных данных, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ;

– Провести проверку соблюдения мер по обеспечению раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

– При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, провести проверку соблюдения мер по обеспечению раздельной обработки персональных данных (при осуществлении таких действий как использование, распространение, уничтожение, блокирование).

3.3 **Порядок проведения контроля выполнения требований, утвержденных Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»**

В ходе проведения проверки необходимо провести анализ реализации требований, утвержденных Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ОГБУ «Липецкая облветлаборатория», утвержденных приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3.3.1 **Порядок проведения контроля установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации**

В ходе проведения проверки необходимо:

– Проверить соответствие версий общесистемного, прикладного и специального программного обеспечения, включая программное обеспечение средств защиты информации;

– Проверить наличие отметок в эксплуатационной документации (формуляр, паспорт) об установке (применении) обновлений;

3.3.2. **Порядок проведения контроля работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации**

В ходе проведения проверки необходимо:

– Проверить работоспособность (неотключение) программного обеспечения и средств защиты информации;

– Проверить правильность функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации;

– Проверить соответствие настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;

– В случае возникновения необходимости восстановить работоспособность, правильное функционирование, а также параметры настройки программного обеспечения и средств защиты информации, в том числе с использованием резервных копий и (или) дистрибутивов.

3.3.3. **Порядок проведения контроля состава технических средств, программного обеспечения и средств защиты информации**

В ходе проведения проверки необходимо:

– Проверить соответствие состава программного обеспечения, технических средств и средств защиты информации приведенному в локальных документах ОГБУ «Липецкая облветлаборатория» и эксплуатационной документации;

– Исключить из состава информационной системы несанкционированно установленные (удаленные) технические средства, программное обеспечение и средства защиты информации;

– Проверить выполнение условий и сроков действия сертификатов соответствия на средства защиты информации;

– В случае возникновения необходимости принять меры, направленные на устранение выявленных недостатков.

3.3.4. **Порядок проведения контроля правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе персональных данных**

В ходе проведения проверки необходимо:

– Проверить соблюдение пользователями и администраторами правил генерации и смены паролей пользователей;

– Проверить соответствие заведенных и удаленных учетных записей пользователей локальным документам ОГБУ «Липецкая облветлаборатория»;

– Осуществить проверку реализации правил разграничения доступа и полномочий пользователей в соответствии с матрицей доступа;

– Провести контроль наличия документов, подтверждающих разрешение изменения учетных записей пользователей, их параметров, правил разграничения доступа, установленных полномочий пользователей;

– В случае возникновения необходимости принять меры, направленные на устранение выявленных недостатков.

3.3.5. **Порядок проведения проверки соблюдения режима защиты персональных данных при их обработке в информационной системе персональных данных**

В ходе проведения проверки необходимо:

– Определить соблюдают ли работники, участвующие в процессе обработки персональных данных в информационной системе персональных данных, принятые меры по обеспечению безопасности персональных данных;

– Произвести контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена;

– Осуществить проверку наличия машинных носителей персональных данных;

– Произвести контроль над выполнением резервного копирования и архивирования информации ограниченного доступа.

3.3.6. **Порядок проведения анализа и пересмотра существующих мер по обеспечению безопасности персональных данных в информационной системе персональных данных**

В ходе проведения проверки необходимо:

– Определить изменения в базовой конфигурации информационной системы, проверить наличие данных о внесении изменений в документацию на систему защиты информации информационной системы персональных данных;

– Провести анализ произведенных изменений на предмет возникновения дополнительных угроз безопасности персональных данных в информационной системе персональных данных;

– В случае выявления новых источников угроз провести уточнение и дополнение модели угроз безопасности;

– Провести соотношение выявленных угроз информационной безопасности с реализованными мерами по обеспечению безопасности персональных данных, в случае необходимости применить дополнительные меры по обеспечению безопасности;

– По результатам анализа изменённой модели угроз и выбора необходимых дополнительных мер по обеспечению безопасности – принять решение об обновлении либо модернизации системы защиты информации;

– Принять решение о необходимости переаттестации информационной системы персональных данных или проведении дополнительных аттестационных испытаний.

3.4 **Порядок проведения проверки наличия и актуальности внутренней нормативной документации по обработке персональных данных**

В ходе проведения проверки необходимо:

– Проверить наличие в ОГБУ «Липецкая облветлаборатория» и соответствие действующему законодательству РФ необходимой внутренней нормативной базы, регулирующей вопросы обработки персональных данных;

– Проверить наличие доказательств ознакомления работников ОГБУ «Липецкая облветлаборатория» с организационно-распорядительными документами ОГБУ «Липецкая облветлаборатория» по обработке персональных данных;

– Принять решение о необходимости актуализации внутренней нормативной базы.

3.5 **Порядок проведения проверки наличия и актуальности внутренней нормативной документации по защите персональных данных**

В ходе проведения проверки необходимо:

– Проверить наличие в ОГБУ «Липецкая облветлаборатория» и соответствие действующему законодательству РФ необходимой внутренней нормативной базы, регулирующей вопросы защиты персональных данных;

– Проверить наличие доказательств ознакомления работников ОГБУ «Липецкая облветлаборатория» с организационно-распорядительными документами ОГБУ «Липецкая облветлаборатория» по защите персональных данных;

– Принять решение о необходимости актуализации внутренней нормативной базы.

Приложение №1

к Правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям
к защите персональных данных в
ОГБУ «Липецкая облветлаборатория»

План проведения внутренних проверок

Проверка	Периодичность	Методика (программа) проверки	Ответственный исполнитель
Контроль выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ, и соблюдения прав субъектов персональных данных	1 раз в год	Пункт 3.1 настоящих Правил	Ответственный за организацию обработки персональных данных
Контроль выполнения требований, утвержденных Постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»	1 раз в год	Пункт 3.2 настоящих Правил	Ответственный за организацию обработки персональных данных
Контроль выполнения требований, утвержденных Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	-	Пункты 3.3.1 – 3.3.6 настоящих Правил	-
Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	1 раз в год	Пункт 3.3.1 настоящих Правил	Администратор безопасности системы защиты персональных данных ИСПДн
Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	1 раз в год	Пункт 3.3.2 настоящих Правил	Администратор безопасности системы защиты персональных данных ИСПДн
Контроль состава технических средств, программного обеспечения и средств защиты информации	1 раз в год	Пункт 3.3.3 настоящих Правил	Администратор безопасности системы защиты персональных данных ИСПДн
Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе персональных данных	1 раз в год	Пункт 3.3.4 настоящих Правил	Ответственный за обеспечение безопасности персональных данных в ИСПДн

Проверка соблюдения режима защиты персональных данных при их обработке в информационной системе персональных данных	1 раз в год	Пункт 3.3.5 настоящих Правил	Ответственный за обеспечение безопасности персональных данных в ИСПДн
Анализ и пересмотр существующих мер по обеспечению безопасности персональных данных в информационной системе персональных данных	1 раз в год	Пункт 3.3.6 настоящих Правил	Ответственный за обеспечение безопасности персональных данных в ИСПДн
Проверка наличия и актуальности внутренней нормативной документации по обработке персональных данных	1 раз в год, а также перед проверками регуляторов	Пункт 3.4 настоящих Правил	Ответственный за организацию обработки персональных данных
Проверка наличия и актуальности внутренней нормативной документации по защите персональных данных	1 раз в год, а также перед проверками регуляторов	Пункт 3.5 настоящих Правил	Ответственный за организацию обработки персональных данных; Ответственный за обеспечение безопасности персональных данных в ИСПДн

Приложение №2
к Правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям
к защите персональных данных в
ОГБУ «Липецкая облветлаборатория»

ЖУРНАЛ
учета мероприятий по осуществлению внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных данных
(форма)

№ п/п	Мероприятие	Дата	Фамилия И.О. исполнителя	Результат	Подпись исполнителя