

УТВЕРЖДАЮ



Директор
ОГБУ «Липецкая областная ветеринарная
лаборатория»

М.А. Зибров

«20» мая 2024 г.

**Положение о защите информации,
обрабатываемой в информационных системах
ОГБУ «Липецкая областная ветеринарная лаборатория»**

Основные термины и определения

В настоящем документе используются следующие термины и их определения.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с ПДн.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Обозначения и сокращения

АРМ – автоматизированное рабочее место

ИС – государственная информационная система

ЖМД – жесткий магнитный диск

ИС – информационная система

МНИ – машинный носитель информации

ОРД – организационно – распорядительная документация

ПДн – персональные данные

ПО – программное обеспечение

СЗИ – средства защиты информации

СОВ – система обнаружения вторжений

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение о защите информации (далее - Положение) утверждается руководителем ОГБУ «Липецкая областная ветеринарная лаборатория» и определяет мероприятия, процедуры и правила по защите информации в информационных системах.

1.1. Положения настоящей Политики обязательны к исполнению для всех пользователей (далее – Пользователи), а также для администраторов безопасности и системных администраторов (далее - Администраторы).

1.2. Целями настоящего Положения являются:

- обеспечение конфиденциальности, целостности, доступности защищаемой информации;
- предотвращение утечек защищаемой информации;
- мониторинг событий безопасности и реагирование на инциденты безопасности;
- нейтрализация актуальных угроз безопасности информации;
- выполнение требований действующего законодательства по защите информации.

1.3. В настоящем Положении используются термины и определения, установленные законодательством Российской Федерации об информации, информационных технологиях и о защите информации, а также термины и определения, установленные национальными стандартами в области защиты информации.

1.4. Настоящее Положение разработана с учетом положений, следующих законодательных и нормативно-правовых актов:

- Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;
- Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»;
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;
- «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;
- методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утверждённые приказом ФСБ России № 378 от 10.07.2014;
- «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ от 9 февраля 2005 №66;
- «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСи от 13 июня 2001 №15

2. ПОРЯДОК ПРОЦЕДУРЫ ИДЕНТИФИКАЦИИ, АУТЕНТИФИКАЦИИ И УПРАВЛЕНИЯ ДОСТУПОМ ПОЛЬЗОВАТЕЛЕЙ

2.1. Порядок идентификации и аутентификации пользователей ИС, являющихся сотрудниками ОГБУ «Липецкая областная ветеринарная лаборатория»:

2.1.1. При предоставлении доступа к персональным данным и любой иной конфиденциальной информации пользователям запрещены любые действия до прохождения ими процедур идентификации и аутентификации.

2.1.2. Пользователь ИС является частью системы защиты ИС и обязан соблюдать правила информационной безопасности, указанные в Инструкции пользователя ИС по обеспечению информационной безопасности;

2.1.3. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику ОГБУ «Липецкая областная ветеринарная лаборатория», допущенному к работе с ресурсами ИС присваивается уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИС.

2.1.4. Персональный идентификатор (учетная запись) пользователя создается администратором безопасности и передаётся пользователю.

2.1.5. Персональному идентификатору пользователя соответствуют определенные полномочия в ИС и пароль, обеспечивающий аутентификацию (проверку подлинности) в ИС.

2.1.6. Права пользователя по доступу к информационным ресурсам ИС, определяются матрицей доступа.

2.1.7. Использование одного и того же имени пользователя несколькими пользователями (или группового имени для нескольких пользователей) в ИС запрещено.

2.1.8. Персональные идентификаторы должны быть заблокированы администратором безопасности при превышении времени неиспользования более 90 дней. Персональные идентификаторы должны быть удалены из информационной системы при увольнении сотрудника ОГБУ «Липецкая областная ветеринарная лаборатория» немедленно по окончании последнего сеанса работы сотрудника, а уволенный сотрудник должен быть исключен из числа пользователей ИС.

2.1.9. При приеме (увольнении) на работу сотрудника ОГБУ «Липецкая областная ветеринарная лаборатория» или изменении полномочий (временное или бессрочное) действующего сотрудника ОГБУ «Липецкая областная ветеринарная лаборатория», включение (исключение) его данных в список доступа к информационным ресурсам ИС и генерацию (уничтожение) идентификатора и пароля, производит администратор безопасности.

2.1.10. При первом доступе пользователь обязан изменить выданный ему пароль, руководствуясь требованиями к сложности пароля:

- длина пароля должна быть не менее 8 буквенно-цифровых символов;
- алфавит пароля должен быть не менее 70 символов (среди символов пароля должны присутствовать латинские буквы в верхнем и нижнем регистрах, цифры или специальные символы);
- настройку максимального количества неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки осуществляет Администратор ИС. Количество вводов неправильного пароля устанавливается от 3 до 4 попыток;
- блокировка АРМ или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации в течение от 15 до 60 минут, смена паролей не более чем через 60 дней;
- пароль не должен включать в себя легко вычисляемые сочетания символов имени, фамилии, дни рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства, наименования информационных систем,

общепринятые сокращения: USER, GUEST, ADMINISTRATOR и т.д., и другие данные, которые могут быть подобраны путем анализа информации о пользователе;

- пароли не должны устанавливаться по единому для всех пользователей АРМ правилу, позволяющему определить пароли других работников, зная хотя бы один действующий пароль;
- в качестве пароля не может быть использован один и тот же повторяющийся символ либо повторяющаяся комбинация из нескольких символов;
- в качестве пароля не может быть использована комбинация символов, набираемых в закономерном порядке на клавиатуре (например, 123456, qwerty и т. п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- в качестве пароля не должны использоваться ранее использовавшиеся пароли.

2.1.11. Администратор ИС организует настройку в информационной системе параметров блокирования сеанса доступа при времени бездействия пользователя более 30 минут или по запросу пользователя.

2.2. Порядок идентификации/аутентификации внешних пользователей ИС

2.2.1. Присвоение идентификатора и выдача атрибутов аутентификации внешним пользователям ИС, осуществляется Администратором ИС. Учет внешних пользователей, допущенных к обработке персональных данных, осуществляет Администратор ИС в матрице доступа.

2.2.2. Выдачу и смену паролей, учет паролей, учет аппаратных средств аутентификации внешних пользователей, допущенных к обработке конфиденциальной информации (в т.ч. ПДн), организует Администратор ИС.

2.2.3. Доступ внешних пользователей к ресурсам ИС организует администратор безопасности и осуществляется по защищенному каналу связи.

2.3. Порядок управления аппаратными средствами аутентификации

2.3.1. Первичное хранение, выдачу, инициализацию, блокирование, утилизацию аппаратных средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации организует администратор безопасности;

2.3.2. Учет выдачи аппаратных средств аутентификации осуществляет администратор безопасности.

2.3.3. Для администратора безопасности ИС, для системных администраторов ИС, для удаленных пользователей (пользователей, работающих с ресурсами ис через внешние телекоммуникационные сети, но являющихся сотрудниками ОГБУ «Липецкая областная ветеринарная лаборатория»), для внешних пользователей ИС (пользователей, не являющихся сотрудниками ИС) предусмотрена двухфакторная аутентификация в ИС. Двухфакторная аутентификация подразумевает под собой обязательное выполнение двух факторов: предъявление физического электронного ключа RuToken, и ввод пароля (пин-кода) доступа к памяти электронного ключа.

2.3.4. Идентификация и аутентификация на сетевом оборудовании (коммутаторы, маршрутизаторы, точки доступа и т. д.) разрешена только администраторам безопасности, системным администраторам и сотрудникам сторонней организации, производящим работы в сети ОГБУ «Липецкая областная ветеринарная лаборатория» на договорной основе под контролем Администратора. При вводе в эксплуатацию сетевого оборудования на нем обязательно меняются идентификационные и аутентификационные данные, установленные производителем устройства по умолчанию. Новые идентификационные данные на сетевых устройствах должны соответствовать установленной парольной политике.

2.4. Порядок организации режима безопасности помещений, где осуществляется работа с конфиденциальной информацией (в т.ч. ПДн)

2.4.1. Методы и средства охраны помещений в организации включают в себя:

- систему контроля и управления доступом в здание организации (наличие при входе в здание пункта контрольного пропуска, определение внешнего контролируемого периметра);
- система контроля перемещения лиц в здании и управления доступом в помещения (наличие помещений с активным сетевым оборудованием с определенными правами доступа, наличие пожарной сигнализаций в помещениях организации, использование замков в помещениях, использование сейфов, шкафов, а также хранение конфиденциальной информации (в т.ч. ПДн) на внутренних и внешних носителях.

2.4.2. Методы контроля доступа в помещения:

- Размещение помещений и оборудования способом, исключающим возможность бесконтрольного проникновения в эти помещения и к этому оборудованию посторонних лиц, включая работников других подразделений;
- После окончания рабочего дня дверь рабочих помещений и помещений, в которых эксплуатируется информационные системы, закрывается на ключ. Все помещения имеют разные замки. Дубликаты ключей хранятся в запираемом шкафу. В случае выхода из помещения в течение рабочего дня всех работников, дверь помещения закрывается на ключ.
- Доступ посторонних лиц в помещения после окончания рабочего дня, установленного в подразделении, ограничен. Уборка помещения производится в присутствии одного из сотрудников этого помещения.
- Доступ работников в помещения подразделения по выходным и праздничным дням осуществляется только по предварительному распоряжению уполномоченных лиц.
- Строгое ограничение доступа посторонних лиц к сетевому оборудованию.
- В случае утраты ключей, об этом немедленно докладывается руководителю, и принимаются меры к немедленной замене замков.

2.4.3. Методы защиты носителей информации в помещении.

Защита мест хранения носителей конфиденциальной информации (USB flash-накопитель, CD, внешних ЖМД) от беспрепятственного доступа и наблюдения, защита персональных данных от неправомерного использования, предусматривает следующие мероприятия:

- Приказом директора ОГБУ «Липецкая областная ветеринарная лаборатория» определяются места хранения носителей.
- Все носители, содержащие конфиденциальную информацию (в том числе и персональные данные), хранятся в шкафах или сейфах, запираемых на ключ, который хранится у ответственных работников. В конце каждого рабочего дня носители убираются в указанные шкафы или сейфы.
- Регулярное проведение инвентаризации мест хранения носителей, содержащих конфиденциальную информацию (в том числе и персональные данные). Факты обнаружения недостачи, порчи, утери носителей доводятся до сведения руководителя. К виновным лицам применяются меры дисциплинарной ответственности.

3. ПОРЯДОК ОБ ОГРАНИЧЕНИИ ПРОГРАММНОЙ СРЕДЫ

3.1. На АРМ пользователей ИС допускается использование только лицензионного программного обеспечения;

3.2. Установку (обновление) ПО ИС осуществляет системный администратор, системы защиты информации ИС осуществляет администратор безопасности, имеющие необходимые полномочия в соответствии с матрицей доступа.

3.3. Установка ПО производится с рабочих копий оригинальных лицензионных дистрибутивных носителей (компакт дисков и т.п.), полученных законным порядком. Устанавливаемое ПО должно иметь необходимую эксплуатационную документацию.

3.4. Устанавливаемое ПО должно быть предварительно проверено (протестировано) администратором безопасности на работоспособность, отсутствие опасных функций, а также на совместимость с установленными в ИС программными и техническими средствами, в том числе ПО СЗИ.

3.5. После установки (обновления) программного обеспечения системный администратор и администратор безопасности, каждый в своей части, выполняют необходимые настройки, выполняют тестирование работоспособности и вносят необходимые изменения в эксплуатационную документацию на ИС и ее систему защиты информации;

3.6. Администратор безопасности проводит оценку изменений в ПО на условия отклонения технологического процесса обработки конфиденциальной информации (в т.ч. ПДн) в ИС от ранее принятого. При обнаружении отклонений администратор безопасности докладывает об обнаруженных отклонениях руководителю. На основании полученной информации руководитель принимает решение о действиях, связанных с изменением конфигурации ИС.

3.7. После обновления ПО администратор безопасности заменяет носители с дистрибутивом неактуального программного обеспечения на носители с дистрибутивом обновленного ПО.

4. ПОРЯДОК УЧЕТА, ХРАНЕНИЯ И УНИЧТОЖЕНИЯ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

4.1. Учет машинных носителей информации

4.1.1. Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

4.1.2. Учет съемных машинных носителей (флэш-накопители, внешние накопители на жестких дисках и иные устройства) информации ведется в Журнале учета и выдачи машинных носителей информации в информационной системе.

4.1.3. Учет встроенных в портативные или стационарные технические средства машинных носителей информации (накопители на жестких дисках) может вестись в составе соответствующих технических средств. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

4.2. Выдача машинных носителей

4.2.1. Пользователи получают носитель от администратора информационной безопасности

4.2.2. При получении пользователем носителя информации делается соответствующая запись в Журнале учета и выдачи машинных носителей информации.

4.2.3. По окончании работ или установленного срока использования пользователь сдает носитель информации администратору информационной безопасности, о чем делается соответствующая запись в Журнале учета и выдачи машинных носителей информации.

4.3. Хранение машинных носителей информации

4.3.1. Конфиденциальная информация субъекта, хранящаяся на машинных носителях, находится в ведении подразделений Организации, осуществляющих эксплуатацию данных автоматизированных рабочих мест или машинных носителей, используемых в информационной системе для хранения и обработки информации. Допуск имеют работники Организации, которым ПДн необходимы в связи с исполнением ими трудовых обязанностей.

4.3.2. В целях недопущения воздействия на технические средства обработки информации, в результате которого нарушается их функционирование, организуется режим обеспечения безопасности помещений, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

4.3.3. Материальные носители, представленных в бумажном виде, должны храниться в сейфе, в запираемом металлическом шкафу или другим способом, исключающим несанкционированный доступ. Организуется режим обеспечения безопасности помещений, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

4.3.4. Запрещается хранить носители информации на рабочих столах, оставлять без присмотра, передавать на хранение третьим лицам.

4.4. Действия при утрате и порче машинных носителей информации

4.4.1. В случае утраты или порчи МНИ, содержащих конфиденциальную информацию, ставится в известность администратор безопасности. Администратор информационной безопасности вносит соответствующую запись в Журнал учета машинных носителей информации

4.4.2. Носители, пришедшие в негодность или с истекшим сроком эксплуатации, подлежат уничтожению в установленном порядке.

4.5. Уничтожение машинных носителей информации

4.5.1. Уничтожение машинных носителей информации организует администратор информационной безопасности с составлением Акта об уничтожении машинных носителей информации (Приложение А).

4.5.2. Уничтожение носителей информации производится способом, гарантирующим невозможность восстановления информации, содержащейся на носителе.

4.6. Ограничения и ответственность

4.6.1. Всем пользователям запрещено использовать учтенные машинные носители информации для личных целей.

4.6.2. Пользователям запрещено передавать носители информации кому-либо.

5. ПОРЯДОК УПРАВЛЕНИЯ СОБЫТИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Процесс управления событиями информационной безопасности осуществляется на этапе эксплуатации ИСи предназначен для обеспечения целостности и доступности конфиденциальной информации (в т.ч. ПДн), а также защиты конфиденциальной информации (в т.ч. ПДн) от несанкционированного доступа к информации за счёт своевременного распознавания технических неисправностей и попыток несанкционированного доступа на основе анализа фиксируемых событий, связанных с отклонениями от штатного режима работы ИС.

5.2. Перечень событий безопасности ИС, подлежащих регистрации

5.2.1. К событиям безопасности ИС, которые подлежат регистрации, относятся:

— события безопасности, имеющие отношение к возможности реализации угроз безопасности конфиденциальной информации (в т.ч. ПДн), описанных в модели угроз безопасности ИС;

— события безопасности, регистрируемые в журналах операционной системы технических средств ИС средств защиты информации (далее – СЗИ);

— организационно-технические события информационной безопасности в инфраструктуре ИС.

5.2.2. Состав и содержание информации по каждому событию, включенному в список реИСТрации должны идентифицировать источник, время и результат события.

5.3. Порядок сбора, записи и хранения информации о событиях безопасности

5.3.1. Настройку журналов регистрации событий информационной безопасности в программном обеспечении ИС СЗИ осуществляет администратор безопасности.

5.3.2. Системные администраторы и администратор безопасности должны **не реже 1 раза в неделю** просматривать журналы регистрации событий безопасности.

5.3.3. Настройки журналов регистрации событий информационной безопасности должны обеспечивать запись в память технических средств ИС и СЗИ информации о поступающих событиях безопасности без переполнения памяти в течение **1 месяца**.

5.3.4. Информация о событиях безопасности в ИС, не подлежащая автоматической реИСТрации (нерегистрируемые программно-аппаратные сбои и неисправности, нарушения организационно-правового плана), должна фиксироваться администратором безопасности при её обнаружении в журнале событий безопасности.

5.3.5. Администратор безопасности должен исследовать наиболее часто повторяющиеся события безопасности, выяснять причины их возникновения и устранять эти причины.

5.4. Защита информации о событиях безопасности

5.4.1. Права доступа к файлам отчетов журналов безопасности и настройкам журналов установлены администратору безопасности и системным администраторам ИС и отражены в матрице доступа.

6. ОРГАНИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

6.1. Процесс антивирусной защиты осуществляется на этапе эксплуатации ИС предназначен для обеспечения целостности и доступности конфиденциальной информации (в т.ч. ПДн), а также защиты конфиденциальной информации (в т.ч. ПДн) от несанкционированного доступа к информации с помощью своевременного распознавания атак вредоносных программ (вирусов) и их нейтрализации.

6.2. Порядок организации антивирусной защиты:

6.2.1. Программное обеспечение антивирусной защиты (далее – антивирусное ПО) устанавливают на все средства вычислительной техники, входящие в состав ИС. Антивирусное ПО обеспечивает защиту от внедрения вредоносного программного обеспечения со съемных носителей, через электронные отправления, из информационно-вычислительной сети, из сетей связи общего пользования и международного информационного обмена (Интернет).

6.2.2. Антивирусная защита ИС строится как единая система, которая обеспечивает:

- управление конфигурацией и логической структурой всего программного обеспечения системы антивирусной защиты;
- управление установкой и обновлением лицензионных ключей средств антивирусной защиты;

- управление рассылкой и установкой обновлений баз средств антивирусной защиты;
- ограничение доступа пользователей на рабочих местах к настройкам установленных средств антивирусной защиты;
- настройку рассылки сообщений об обнаружении вирусов, о сбоях в работе средств антивирусной защиты и т.п.;
- решение проблем, возникающих в процессе использования средств антивирусной защиты.

6.2.3. На все применяемые в ИС средства антивирусной защиты должны быть документы, подтверждающие права ОГБУ «Липецкая областная ветеринарная лаборатория» на их использование и действующие сертификаты ФСТЭК России;

6.2.4. При осуществлении антивирусной защиты ИС выполняются следующие обязательные мероприятия:

- контроль съемных носителей информации на предмет наличия на них вредоносного программного обеспечения до начала работы с ними;
- проверка всех электронных отправок на предмет наличия вредоносного программного обеспечения;
- периодическая проверка на предмет наличия вредоносного программного обеспечения жестких магнитных дисков (не реже одного раза в неделю);
- внеплановая проверка жестких магнитных дисков и съемных носителей информации в случае подозрения на наличие вредоносного программного обеспечения; восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами;

6.2.5. Обновления баз данных средств антивирусной защиты в ИС осуществляется в автоматическом режиме (не реже одного раза в сутки).

6.2.6. Установку и настройку антивирусного ПО осуществляет администратор безопасности совместно с системным администратором в соответствии с эксплуатационной документацией на данное ПО.

6.3. Порядок действий при обнаружении вредоносного ПО

6.3.1. При обнаружении вредоносного программного обеспечения на съемных носителях, в электронных отправлениях или при посещении ресурсов сети Интернет пользователь ИС обязан:

- приостановить работу с источником угрозы (съемным носителем, электронным отправлением, Интернет-ресурсом), иные работы на автоматизированном рабочем месте не запрещаются;
- сообщить администратору безопасности об обнаружении вредоносного программного обеспечения;
- принять меры по локализации и удалению вредоносного программного обеспечения, рекомендованные администратором безопасности;

6.3.2. Администратор безопасности по факту событий должен зарегистрировать вирусную атаку в соответствующем журнале.

6.3.3. При обнаружении вредоносного программного обеспечения на серверном или телекоммуникационном оборудовании, администратор безопасности обязан:

- немедленно сообщить ответственному за организацию обработки конфиденциальной информации (в т.ч. ПДн) об обнаружении вредоносного программного обеспечения;
- принять меры по локализации и удалению вредоносного программного обеспечения, а также по выявлению источника и способа проникновения вредоносного программного обеспечения, предпринять действия в соответствии с требованиями по управлению инцидентами.

7. ПОРЯДОК ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

7.1. Процесс обнаружения вторжений осуществляется на этапе эксплуатации ИСи предназначен для обеспечения целостности и доступности конфиденциальной информации (в т.ч. ПДн), а также защиты от несанкционированного доступа к информации с помощью своевременного распознавания программных вторжений с целью получения несанкционированного доступа к ресурсам ИС, их нейтрализации.

7.2. Порядок организации системы обнаружения вторжений

7.2.1. СОВ представляет собой программно-аппаратный комплекс, который для эффективного обнаружения вторжений необходимо настроить перед началом эксплуатации и в дальнейшем контролировать состояние настроек и производить их изменение при необходимости.

7.2.2. За управление СОВ и за действия при обнаружении вторжений отвечает администратор безопасности.

7.2.3. К действиям по управлению СОВ относятся:

- подключение и настройка параметров работы СОВ;
- загрузка в СОВ решающих правил;
- настройка параметров автоматической загрузки решающих правил;
- назначение решающих правил детекторам атак;
- добавление в СОВ собственных и корректировка уже имеющихся правил при такой необходимости;
- настройка и контроль обновлений базы решающих правил.

7.2.4. Доступ к управлению СОВ разрешен только администратору безопасности с помощью пароля, устанавливаемого самим администратором безопасности. Правила назначения пароля в соответствии требованиями по идентификации и аутентификации.

7.2.5. Конфигурация настроек СОВ должна быть сохранена на съемном носителе.

7.2.6. Хранение и учет съемных носителей, содержащих настройки СОВ, обеспечивает администратор безопасности по правилам по защите машинных носителей.

7.2.7. Конкретные действия администратора безопасности по управлению СОВ приведены в Руководстве администратора СОВ.

7.2.8. Действия при обнаружении СОВ вторжения должны быть определены ответственным за организацию обработки персональных данных совместно с администратором безопасности исходя из возможностей СОВ и требований к технологии обработки персональных данных. На основе принятых решений администратор безопасности настраивает параметры СОВ.

7.2.9. Обнаруженные вторжения квалифицируются как инциденты и обрабатываются по правилам, установленным в требованиях по управлению инцидентами.

7.3. Обновление базы решающих правил

7.3.1. Решающие правила, используемые в СОВ определяют эффективность обнаружения вторжений. Решающие правила загружаются в СОВ при вводе ее в эксплуатацию.

7.3.2. В условиях постоянно изменяющихся способов и алгоритмов вторжений решающие правила для надежного обнаружения вторжений должны быть актуальны.

7.3.3. Актуальность решающих правил обеспечивается своевременным обновлением баз решающих правил.

7.3.4. Для обеспечения своевременного автоматического обновления баз решающих правил при проведении первоначальной настройки СОВ администратор безопасности должен загрузить в СОВ сертификаты для получения и последующего обновления баз решающих правил.

7.3.5. Контроль обновлений баз решающих правил в СОВ осуществляет администратор безопасности по требованиям по управлению программным обеспечением.

8. ПОРЯДОК КОНТРОЛЯ И АНАЛИЗА ЗАЩИЩЕННОСТИ ИС

8.1. Процесс контроля защищенности ИС осуществляется на этапе эксплуатации ИС и предназначен для обеспечения целостности и доступности конфиденциальной информации (в т.ч. ПДн), а также защиты от неучтенных и вновь возникающих угроз информационной безопасности.

8.2. Порядок действий системных администраторов и администратора безопасности с целью:

- выявления ошибок и недостатков программного обеспечения и аппаратных средств ИС и СЗИ;
- контроля установки обновлений программного обеспечения, контроля работоспособности и настроек программного обеспечения;
- контроля состава технических средств ИСи системы защиты информации;
- контроля правил работы с паролями и учетными записями.

8.3. Ответственный за защиту информации в ИСи Администратор безопасности должны систематические проводить мероприятия по анализу защищенности ИСи тестированию работоспособности СЗИ в порядке и с периодичностью, установленными в «Правилах осуществления внутреннего контроля (мониторинга) за обеспечением уровня защищенности информации в ИС» в части их касающейся.

8.4. Информация о проведенной проверке, дата ее начала и окончания, а также ее результаты, фиксируется в «Журнале учета мероприятий по осуществлению внутреннего контроля за обеспечением уровня защищенности информации ИСПДн». Форма журнала утверждается приказом директора ОГБУ «Липецкая областная ветеринарная лаборатория».

8.5. Выявление, анализ и устранение уязвимостей

8.5.1. Уязвимость – это недостаток ИС или системы защиты информации, который может привести к реализации угрозы безопасности конфиденциальной информации (в т.ч. ПДн), обрабатываемой в ИС.

8.5.2. Периодичность плановых процедур выявления, анализа и устранения уязвимостей ИС составляет 1 раз в год. Внеплановые процедуры выявления, анализа и устранения уязвимостей ИС проводят по распоряжению ответственного за обеспечение безопасности информации в случае необходимости. Необходимость внеплановой процедуры выявления и устранения уязвимостей определяет ответственный за обеспечение безопасности информации на основе анализа журналов событий безопасности.

8.5.3. В ИС должно осуществляться выявление и устранение следующих типов уязвимостей:

- недостатки и (или) ошибки программного обеспечения ИСи её системы защиты;
- недостатки аппаратных средств ИС, в том числе аппаратных средств защиты информации;
- организационно-технические недостатки.

8.5.4. Мероприятия по выявлению, анализу и устранению уязвимостей организует ответственный за обеспечение безопасности информации. Непосредственными исполнителями мероприятий по выявлению, анализу и устранению уязвимостей в ИС является администратор безопасности.

8.6. Выявление, анализ и устранение недостатков программного обеспечения

8.6.1. Проверка конфигурации и настроек программно-технических средств ИСи системы защиты персональных данных на соответствие требованиям эксплуатационной документации и требований к защите персональных данных.

8.6.2. Проверка наличия и сроков действия лицензий на установленное программное обеспечение.

8.6.3. Проверка наличия последних обновлений используемого программного обеспечения:

- проверка соответствия обновлений версиям программного обеспечения, установленного в ИС и системе защиты конфиденциальной информации (в т.ч. ПДн);
- проверка обновлений вирусных баз;
- проверка обновлений баз решающих правил для средств обнаружения вторжений.

8.6.4. Анализ сообщений об уязвимостях из специальных источников.

8.6.5. Устранение обнаруженных недостатков на основании своих полномочий осуществляет администратор безопасности.

8.6.6. При наличии в ИС сканеров безопасности, администратор безопасности осуществляет процесс сканирования и анализ отчетов об обнаруженных уязвимостях.

8.6.7. Результаты сканирования должны быть отсортированы администратором безопасности по степени критичности (опасности реализации известных угроз безопасности) обнаруженных уязвимостей и сведены в таблицу результатов сетевого сканирования.

8.7. Выявление, анализ и устранение недостатков аппаратных средств

8.7.1. К недостаткам аппаратных средств, используемых в ИС, относят низкую надежность функционирования (частые аппаратные сбои, отключения), нарушения аппаратной конфигурации, низкое качество контактных соединений.

8.7.2. При выявлении недостатков аппаратных средств проверяют:

- техническое состояние аппаратных средств;
- наличие сертификатов соответствия на примененные в ИС и её системе защиты аппаратные средства;
- наличие у поставщиков обновленных версий аппаратных средств, примененных в ИС и системе защиты конфиденциальной информации (в т.ч. ПДн);
- перечень событий информационной безопасности за период контроля, связанных с отказами и неисправностями аппаратных средств;
- конфигурацию соединений и установки аппаратных средств, условия их эксплуатации.

8.7.3. Проверку осуществляет администратор безопасности и при необходимости оформляет ее результаты в виде таблицы.

8.7.4. Обнаруженные в ходе проверки отклонения от конфигурации ИС устраняет администратор безопасности. Координирует работы администратор безопасности. При обнаружении аппаратных средств с низкой надежностью, частыми выходами из строя администратор безопасности принимает меры по ремонту или замене этих аппаратных средств.

8.8. Выявление, анализ и устранение организационно-технических недостатков

8.8.1. Проверка состояния и актуальности организационно-распорядительной документации (далее – ОРД) по защите конфиденциальной информации (в т.ч. ПДн), обрабатываемых в ИС.

8.8.2. Проверка заполнения рабочих документов ОРД (записи в журналах, перечнях, актах и других формах по требованиям ОРД).

8.8.3. Проверка соответствия выполнения правил генерации и смены паролей пользователей принятым требованиям.

8.8.4. Проверка соответствия выполнения правил заведения и удаления учетных записей пользователей принятым требованиям.

8.8.5. Проверка соответствия выполнения правил разграничения доступа к конфиденциальной информации (в т.ч. ПДн) и ресурсам ИС принятым требованиям.

8.8.6. Проверка соответствия полномочий пользователей принятым требованиям.

8.8.7. Проверка наличия документов, подтверждающих правомерность изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей.

8.8.8. Проверка состояния физической защиты ИС(средства охраны и физического доступа в контролируемой зоне ИС).

8.8.9. Проверка знания и соблюдения пользователями ИС основных нормативно-правовых актов в области защиты конфиденциальной информации (в т.ч. ПДн) и требований ОРД.

8.8.10. Проверки организует ответственный за обеспечение безопасности информации с участием администратора безопасности.

8.8.11. Выполнение требований инструкции в части его касающейся и контроль соблюдения пользователями требований инструкции обеспечивает администратор безопасности.

9. ПОРЯДОК ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ И ДОСТУПНОСТИ ИНФОРМАЦИИ

9.1. Целостность информационной системы

9.1.1. Способы контроля целостности программного обеспечения определяются администратором безопасности перед началом эксплуатации ИС. В зависимости от принятого способа контроля администратор безопасности организует безопасное хранение между проверками контрольных сумм или ключей хеширования для используемого программного обеспечения (далее – ПО).

9.1.2. Контроль целостности программного обеспечения осуществляется периодически не реже 1 раза в три месяца по определенному плану, неизвестному пользователям ИС. План контроля целостности программного обеспечения ИС разрабатывает администратор безопасности.

9.1.3. Контроль целостности программного обеспечения осуществляется комиссией под председательством администратора безопасности с использованием специального программного обеспечения.

9.2. Обеспечение доступности информации в информационной системе. Порядок резервного копирования конфиденциальной информации (в т.ч. ПДн)

9.2.1. Под резервным копированием понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности ИС в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных, обрабатываемых в ИС.

9.2.2. Резервному копированию подлежит информация следующих основных категорий:

- персональная информация пользователей (личные каталоги) и групповая информация;
- информация, обрабатываемая пользователями в ИС, а также информация, необходимая для восстановления работоспособности ИС;
- рабочие копии установочных компонент программного обеспечения общего назначения и специализированного программного обеспечения ИС;
- информация, необходимая для восстановления серверов и систем управления базами данных ИС, локальной вычислительной сети, системы электронного документооборота;
- регистрационная информация системы информационной безопасности ИС;

- другая информация ИС, по мнению пользователей, системных администраторов и администратора безопасности, являющаяся критичной для работоспособности ИС.

9.2.3. Регламент резервного копирования для ИС определен следующими требованиями:

- состав и объем копируемых данных, необходимая периодичность проведения резервного копирования;
- максимальный срок хранения резервных копий;
- надежность и защищенность хранения резервных копий.

9.2.4. К носителям информации, содержащим резервные копии, а также к резервируемым программным средствам допускаются только работники ОГБУ «Липецкая областная ветеринарная лаборатория», указанные в Регламенте инструкции по резервному копированию.

9.2.5. О выявленных попытках несанкционированного доступа к резервируемой информации и аппаратным средствам, а также иных нарушениях информационной безопасности, произошедших в процессе архивирования (резервного копирования), сообщается администратору безопасности.

9.2.6. Предварительный учет съемных носителей резервных копий производится в отдельном журнале учета съемных носителей для резервного копирования, который находится у администратора безопасности.

9.2.7. Все съемные носители с резервными копиями маркируются, на них указывается предназначение носителя.

9.2.8. В случае неотделимости носителей резервной информации от системы резервного копирования допускается их не маркировать и учитывать всю систему как одно целое.

9.2.9. Хранение отдельных съемных носителей резервных копий организуется в отдельном от используемых данных помещении. Физический доступ к резервным копиям строго ограничен. Контроль за физическим доступом возлагается на администратора безопасности.

9.2.10. Доступ к носителям резервных копий имеют только системные администраторы ИС, которые несут персональную ответственность за сохранность резервных копий и невозможность ознакомления с ними лиц, не имеющих на то права.

9.2.11. Съемные носители для резервных копий изымаются для работы только системным администратором, непосредственно осуществляющим резервное копирование, под роспись в журнале учета носителей.

9.2.12. Уничтожение съемных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательной записью в журнале их учета.

9.2.13. Ответственность за периодичность и полноту резервного копирования, а также состояние системы резервного копирования возлагается на администратора безопасности, осуществляющего резервное копирование.

9.2.14. Ответственность за контроль над своевременным осуществлением резервного копирования, а также за выполнением требований по хранению резервных копий и предотвращению несанкционированного доступа к ним возлагается на администратора безопасности.

9.2.15. В случае обнаружения попыток несанкционированного доступа к носителям резервной информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается администратору безопасности в течение рабочего дня после обнаружения указанного события.

9.2.16. Резервное копирование специализированного программного обеспечения производится при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.

9.2.17. Резервное копирование открытой информации делается не позднее чем через сутки после ее изменения, но не реже одного раза в месяц.

9.2.18. Информация, содержащаяся в постоянно изменяемых базах данных ИС, сохраняется в соответствии со следующим графиком:

- ежедневно проводится копирование измененной и дополненной информации. Носители с ежедневной информацией должны храниться в течение недели;
- еженедельно проводится резервное копирование всей базы данных. Носители с еженедельными копиями хранятся в течение месяца;
- ежемесячно производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится постоянно.

9.2.19. Не реже одного раза в год на носители длительного хранения записывается информация, не относящаяся к постоянно изменяемым базам данных (приказы, распоряжения, открытые издания и т.д.).

9.2.20. Контроль результатов всех процедур резервного копирования осуществляется администраторами ИС, в срок до конца рабочего дня, следующего за установленной датой выполнения этих процедур. В случае обнаружения ошибки результат сообщается администратору безопасности.

9.2.21. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, осуществляется ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для ее хранения.

9.2.22. Система резервного копирования обеспечивает возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивает восстановление текущей информации ИС в случае отказа любого из устройств резервного копирования.

9.2.23. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются администраторами ИС. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек. Информация ограниченного доступа с носителей, которые перестают использоваться в системе резервного копирования, уничтожается.

9.3. Порядок восстановления персональных данных

9.3.1. В случае необходимости восстановление персональных данных из резервных копий производится администраторами ИС.

9.3.2. Восстановление персональных данных из резервных копий происходит в случае их исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев

9.3.3. Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с дистрибутивных носителей в соответствии с инструкциями производителя.

9.3.4. Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

9.3.5. Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.

9.3.6. При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной копии.

Акт

об уничтожении машинных носителей конфиденциальной информации (в т.ч. персональных данных)

Комиссия в составе:

Председатель – _____

Члены комиссии – _____

провела отбор машинных носителей конфиденциальной информации (в т.ч. персональных данных) и установила, что в соответствии с требованиями руководящих документов по защите информации указанные носители и информация, записанная на них в процессе эксплуатации, подлежит гарантированному уничтожению и составила акт о том, что произвела уничтожение носителей конфиденциальной информации (в т.ч. ПДн) в составе:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя	Категория информации	Примечание

На указанных носителях конфиденциальная информация (в т.ч. ПДн) уничтожены путем _____
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные материальные носители конфиденциальной информации (в т.ч. персональных данных) уничтожены путем _____
(разрезания, сжигания, механического уничтожения и т.п.)

Председатель комиссии: _____ / _____ /

Члены комиссии: _____ / _____ /

_____ / _____ /

_____ / _____ /