

Общество с ограниченной ответственностью

«Медицинская организация «Лотос»

ОГРН : 1192536014109 ИНН 2536317050

РФ, 690034, г. Владивосток, ул. Стрелковая, д. 23А, офис 11

ПРИКАЗ

5 декабря 2024 года

№

г. Владивосток

Об утверждении внутренних нормативных актов по защите информации

С целью исполнения требований Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить Политику ООО МО «Лотос» в отношении обработки персональных данных (Приложение 1).
2. Утвердить Положение об обработке и защите персональных данных (Приложение 2).
3. Утвердить инструкцию пользователя в информационных системах персональных данных ООО МО «Лотос» (Приложение 3).
4. Утвердить инструкцию по организации парольной защиты в информационных системах персональных данных ООО МО «Лотос» (Приложение 4).
5. Утвердить инструкцию по организации антивирусной защиты в ООО МО «Лотос» (Приложение 5).
6. Контроль за исполнением настоящего приказа оставляю за собой.

Директор

А.А. Левченко

**Политика ООО МО «Лотос»
в отношении обработки персональных данных**

1. Введение.

1.1. Обеспечение конфиденциальности и безопасности обработки персональных данных в ООО МО «Лотос» является одной из приоритетных задач организации.

1.2. В ООО МО «Лотос» для этих целей введен в действие комплект организационно-распорядительной документации, обязательный к исполнению всеми сотрудниками компании, допущенными к обработке персональных данных.

1.3. Обработка, хранение и обеспечение конфиденциальности и безопасности персональных данных осуществляется в соответствии с действующим законодательством РФ в сфере защиты персональных данных, и в соответствии с локальными актами ООО МО «Лотос».

1.4. Настоящая Политика определяет принципы, порядок и условия обработки персональных данных работников, соискателей, пациентов, контрагентов ООО МО «Лотос» и иных лиц, чьи персональные данные обрабатываются организацией, с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также устанавливает ответственность должностных лиц ООО МО «Лотос», имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

2. Понятие и состав персональных данных.

2.1. Сведениями, составляющими персональные данные, в ООО МО «Лотос» является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.2. Перечень персональных данных, подлежащих защите в ООО МО «Лотос» утверждается отдельным приказом руководителя ООО МО «Лотос».

3. Цели обработки персональных данных.

3.1. ООО МО «Лотос» осуществляет обработку персональных данных в следующих целях:

3.1.1. Реализации кадрового учета компании, обеспечения соблюдения законов и иных нормативно-правовых актов в данной области; ведения кадрового делопроизводства, исполнения требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнения первичной статистической документации, в соответствии с Трудовым кодексом РФ, Налоговым кодексом РФ, федеральными законами, в частности: от 1 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и других нормативно-правовых актов.

3.1.2. Организации оказания медицинской помощи гражданам, а также исполнения обязательств и компетенций в соответствии с Федеральными законами от 21 ноября 2011 г. №

323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными Постановлением Правительства Российской Федерации от 4 октября 2012 г. № 1006.

4. Сроки обработки персональных данных.

4.1. Сроки обработки персональных данных определяются в соответствии со сроком действия договора (соглашением) с субъектом персональных данных, Приказом Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения», сроком исковой давности, а также иными требованиями законодательства РФ.

4.2. В ООО МО «Лотос» создаются и хранятся документы, содержащие сведения о субъектах персональных данных. Требования к использованию в ООО МО «Лотос» данных типовых форм документов установлены Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

5. Права и обязанности.

5.1. ООО МО «Лотос» как оператор персональных данных в праве:

5.1.1. Отстаивать свои интересы в суде.

5.1.2. Предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.).

5.1.3. Отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством.

5.1.4. Использовать персональные данные субъекта без его согласия в случаях, предусмотренных законодательством.

5.2. Субъект персональных данных имеет право:

5.2.1. Требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

5.2.2. Требовать перечень своих персональных данных, обрабатываемых ООО МО «Лотос» и источник их получения.

5.2.3. Получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения.

5.2.4. Требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.2.5. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных.

6. Принципы и условия обработки персональных данных.

6.1. Обработка персональных данных в ООО МО «Лотос» производится на основе соблюдения принципов:

6.1.1. Законности целей и способов обработки персональных данных.

6.1.2. Соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных.

6.1.3. Соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных.

6.1.4. Достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных.

6.1.5. Недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные.

6.1.6. Хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

6.1.7. Уничтожения по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении.

6.2. Отказ клиента ООО МО «Лотос» от предоставления согласия на обработку его персональных данных влечет за собой невозможность достижения целей обработки.

7. Обеспечение безопасности персональных данных.

7.1. ООО МО «Лотос» предпринимает необходимые организационные и технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.

7.2. В целях координации действий по обеспечению безопасности персональных данных в ООО МО «Лотос» назначен ответственный за организацию обработки персональных данных.

8. Заключительные положения.

8.1. Настоящая Политика предназначена для размещения в информационных ресурсах общественного пользования ООО МО «Лотос».

8.2. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года.

8.3. Контроль исполнения требований настоящей Политики осуществляется ответственным за организацию обработки персональных данных ООО МО «Лотос».

Ответственность должностных лиц ООО МО «Лотос», имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами ООО МО «Лотос».

Положение об обработке и защите персональных данных в ООО МО «Лотос»

1. Общие положения.

1.1. Настоящее Положение о порядке обработки и защите персональных данных (далее – ПДн) в ООО МО «Лотос» (далее – Положение) определяет цели, содержание и порядок обработки ПДн, меры, направленные на защиту ПДн, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области ПДн, в ООО МО «Лотос» (далее – Организация).

1.2. Настоящее Положение определяет политику ООО МО «Лотос» как оператора, осуществляющего обработку ПДн, в отношении обработки и защиты ПДн.

1.3. Настоящее Положение разработано в соответствии со следующими нормативно-правовыми актами:

1.3.1. Конституция Российской Федерации.

1.3.2. Гражданский кодекс Российской Федерации.

1.3.3. Трудовой кодекс Российской Федерации.

1.3.4. Кодекс Российской Федерации об административных правонарушениях.

1.3.5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1.3.6. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

1.3.7. Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

1.3.8. Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации».

1.3.9. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.3.10. Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.3.11. Приказ Федеральной службы по техническому и экспортному контролю России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.3.12. Руководящие и методические документы Министерства здравоохранения Российской Федерации.

1.3.13. Внутренние нормативные документы Организации.

1.4. Настоящее Положение является локальным актом Организации, обязательным для исполнения всеми работниками Организации, в должностные обязанности которых входит обработка персональных данных в соответствии с Перечнем лиц, допущенных к обработке персональных данных в информационных системах персональных данных (далее – лица, допущенные к работе с ПДн), утверждаемым приказом руководителя, по форме в соответствии с Приложением №1 к настоящему Положению.

1.5. Для целей настоящего Положения используются следующие основные понятия и сокращения:

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

1.5.2. Оператор персональных данных (оператор) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.5.3. Обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

1.5.4. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

1.5.5. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

1.5.7. Доступ к информации – возможность получения информации и ее использования.

1.5.8. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

1.5.10. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1.5.11. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.5.12. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

1.5.13. ИСПДн – информационная система персональных данных.

1.5.14. ПДн – персональные данные.

1.6. Обработка ПДн в Организации осуществляется с соблюдением принципов и условий, предусмотренных настоящим Положением и законодательством Российской Федерации в области ПДн.

1.7. Обязанности оператора ПДн определены в главе 4 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.8. Целями обработки ПДн в Организации являются:

1.8.1. Реализация кадрового учета Организации, обеспечения соблюдения законов и иных нормативно-правовых актов в данной области; ведения кадрового делопроизводства, исполнения требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога, пенсионного законодательства при формировании и представлении персонализированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнения первичной статистической документации, в соответствии с Трудовым кодексом РФ, Налоговым кодексом РФ, федеральными законами, в частности: от 1 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонализированном) учете в системе обязательного пенсионного страхования», от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и других нормативно-правовых актов.

1.8.2. Организация оказания медицинской помощи населению, а также исполнения обязательств и компетенций в соответствии с Федеральными законами от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными Постановлением Правительства Российской Федерации от 4 октября 2012 г. № 1006.

1.9. ООО МО «Лотос», являясь оператором, осуществляет обработку ПДн следующих категорий субъектов:

№ п/п	Общее название группы субъектов ПДн	Категории субъектов ПДн, входящих в группу
1	Работники Организации	<ul style="list-style-type: none"> – лица, состоящие в трудовых отношениях с Организацией (в т. ч. ПДн кандидатов на вакантные должности) – родственники лиц, состоящих в трудовых отношениях с Организацией; – лица, с которыми прекращены трудовые отношения; – родственники лиц, с которыми прекращены трудовые отношения; – физические лица, состоящие в договорных и иных гражданско-правовых отношениях с Организацией
2	Лица, обратившиеся за медицинской помощью	<ul style="list-style-type: none"> – потребители медицинских услуг. Заказчики медицинских услуг в интересах потребителя; – законные представители (опекуны, попечители) лиц, которым оказываются медицинские услуги.

2. Общий порядок и условия обработки ПДн.

2.1. Принципы обработки ПДн определены в статье 5, условия обработки ПДн определены в статье 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2.2. Обработка ПДн в Организации осуществляется в информационных системах персональных данных, определенных в перечне информационных систем персональных данных, утвержденном соответствующим приказом.

2.3. Организация осуществляет смешанную обработку ПДн (как с использованием средств автоматизации, так и без использования таких средств).

2.4. Обработка ПДн без использования средств автоматизации (неавтоматизированная обработка ПДн) производится лицами, допущенными к работе с ПДн, в соответствии с положениями постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об

утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2.5. Организация осуществляет обработку ПДн субъектов ПДн только при наличии согласия субъекта ПДн, либо его законного представителя на обработку его ПДн.

2.6. Все ПДн следует получать у самого субъекта ПДн или из общедоступных источников ПДн. Если ПДн возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие (за исключением случаев, предусмотренных законодательством Российской Федерации).

2.7. Согласие на обработку ПДн дается в любой позволяющей подтвердить факт его получения форме, в том числе в форме электронного документа, заверенного усиленной квалифицированной электронной подписью.

2.8. Согласие в письменной форме субъекта ПДн на обработку его ПДн должно включать в себя сведения, содержащиеся в части 4 статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2.9. В случае отзыва субъектом ПДн согласия на обработку ПДн Организация вправе продолжить обработку ПДн без согласия субъекта ПДн на основании части 2 статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» при наличии оснований, указанных в пунктах 2 – 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 данного Федерального закона.

2.10. Субъект ПДн предоставляет достоверные сведения о себе. Лица, допущенные к работе с ПДн, проверяют достоверность сведений, сверяя данные, предоставленные субъектом ПДн, с имеющимися у субъекта ПДн документами.

3. Порядок и условия обработки ПДн работников Организации.

3.1. Обработка ПДн работников осуществляется в целях реализации кадрового учета Организации, обеспечения соблюдения законов и иных нормативно-правовых актов в данной области; ведения кадрового делопроизводства, исполнения требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнения первичной статистической документации, в соответствии с Трудовым кодексом РФ, Налоговым кодексом РФ, федеральными законами, в частности: от 1 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и других нормативно-правовых актов.

3.2. Бланк согласия на обработку ПДн работников Организации утверждается отдельным приказом руководителя Организации.

3.3. В целях, указанных в пункте 3.1 настоящего Положения, обрабатывается необходимый набор ПДн работников Организации, утверждённый отдельным приказом руководителя Организации.

3.4. Информация, предоставляемая работником при поступлении на работу в Организацию, должна иметь документальную форму. При заключении трудового договора лицо, поступающее на работу в Организацию, предъявляет кадровому специалисту документы в соответствии со статьей 65 Трудового кодекса Российской Федерации.

3.5. Передача и использование ПДн работников Организации осуществляется только в случаях и в порядке, предусмотренных федеральными законами.

4. Порядок и условия обработки ПДн лиц, обратившихся за медицинской помощью.

4.1. Обработка ПДн лиц, обратившихся за медицинской помощью, осуществляется в целях оказания медицинской помощи населению, а также исполнения обязательств и компетенций в соответствии с Федеральными законами от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными Постановлением Правительства Российской Федерации от 4 октября 2012 г. № 1006.

4.2. Бланк согласия на обработку ПДн лица, обратившегося за медицинской помощью, утверждается отдельным приказом руководителя Организации.

4.3. В целях, указанных в пункте 4.1 настоящего Положения, обрабатывается необходимый набор ПДн лиц, обратившихся за медицинской помощью, утверждённый отдельным приказом руководителя Организации.

4.4. Информация, предоставляемая лицом при обращении за медицинской помощью, должна иметь документальную форму.

5. Общедоступные ПДн.

5.1. В соответствии с пунктом 10 части 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», ПДн, сделанными общедоступными субъектом ПДн, считаются ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн либо по его просьбе.

5.2. В соответствии с частью 1 статьи 8 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в целях информационного обеспечения в Организации существуют и могут создаваться новые общедоступные источники ПДн.

5.3. В категорию «Общедоступные ПДн» с письменного согласия работника Организации включаются: фамилия, имя, отчество; пол; сведения о полученном образовании; сведения о месте работы; сведения (даты) о нахождении в командировке, отпуске; сведения о наградах и достижениях; фотография.

5.4. Сведения о субъекте ПДн должны быть в любое время исключены из категории «Общедоступные ПДн» по письменному требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов.

6. Порядок доступа работников ООО МО «Лотос» в помещения, в которых осуществляется обработка и хранение персональных данных.

6.1. Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных достигается в том числе установлением правил доступа в помещения, в которых осуществляется хранение ПДн, обработка ПДн без использования средств автоматизации, доступ к информационным системам персональных данных.

6.2. Для помещений организуется режим обеспечения безопасности, при котором обеспечивается сохранность документов, содержащих ПДн, технических средств обработки защищаемой информации, средств защиты информации и носителей защищаемой информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

6.3. При хранении материальных носителей персональных данных (в том числе документов, содержащих ПДн) должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключаяющие несанкционированный доступ к ним посторонних лиц.

6.4. Нахождение лиц, не допущенных к обработке ПДн, в помещениях Организации, в которых осуществляется обработка и хранение персональных данных, возможно только в

присутствии уполномоченного сотрудника Организации на время, ограниченное необходимостью решения вопросов, связанных с исполнением функций и (или) осуществлением полномочий структурного подразделения Организации.

6.5. О попытках неконтролируемого проникновения посторонних лиц в помещения работник Организации обязан незамедлительно сообщать руководителю своего структурного подразделения.

6.6. Перед закрытием помещений, в которых ведется обработка персональных данных, по окончании рабочего времени работники, имеющие право доступа в помещения, обязаны:

6.6.1. Убрать бумажные носители персональных данных и электронные носители персональных данных (диски, флеш-накопители) в шкафы, сейфы.

6.6.2. Отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение.

6.6.3. Закрыть окна.

6.7. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на руководителей структурных подразделений Организации, обрабатывающих персональные данные.

6.8. Внутренний контроль за соблюдением порядка доступа в помещения проводится лицом, назначенным приказом Организации, ответственным за организацию обработки персональных данных в Организации.

7. Передача персональных данных третьим лицам.

7.1. Передача ПДн субъектов ПДн контрольно-надзорным органам и в государственные информационные системы, содержащие ПДн, осуществляется в соответствии с действующим законодательством Российской Федерации.

7.2. Доступ к ПДн работников Организации на основании и во исполнение федеральных законов предоставляется:

7.2.1. Федеральной инспекции труда и федеральным органам исполнительной власти, осуществляющим функции по контролю и надзору в установленной сфере деятельности.

7.2.2. Федеральной налоговой службе и межрегиональным инспекциям и управлениям Федеральной налоговой службы Российской Федерации по субъектам Российской Федерации.

7.2.3. Главному управлению по вопросам миграции Министерства внутренних дел Российской Федерации.

7.2.4. Федеральной службе государственной статистики и её территориальным органам.

7.2.5. Федеральному фонду обязательного медицинского страхования и его территориальным органам.

7.2.6. Военным комиссариатам.

7.2.7. Фонд пенсионного и социального страхования Российской Федерации;

7.2.8. Иным федеральным органам в соответствии с законодательством Российской Федерации.

7.3. Передача ПДн субъектов ПДн страховым компаниям, банкам, благотворительным организациям, негосударственным пенсионным фондам, посольствам, другим организациям; родственникам, членам семьи и другим лицам осуществляется по письменному запросу о предоставлении ПДн на имя руководителя или главного врача с указанием цели предоставления и характера ПДн. Передача ПДн осуществляется только при условии получения письменного согласия субъекта, ПДн которого запрашиваются, либо по письменному заявлению самого субъекта ПДн.

7.4. При передаче ПДн субъектов ПДн Организация должна соблюдать следующие требования:

7.4.1. Не сообщать ПДн субъекта ПДн третьей стороне без его письменного согласия (либо согласия его законного представителя), за исключением случаев, установленных законодательством Российской Федерации.

7.4.2. Не сообщать ПДн субъекта ПДн в коммерческих целях без его письменного согласия (либо согласия его законного представителя).

7.4.3. Предупредить лиц, получивших ПДн субъекта ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

7.4.4. Лица, получившие ПДн субъекта ПДн, обязаны соблюдать режим конфиденциальности.

7.4.5. Осуществлять передачу ПДн субъектов ПДн в пределах Организации в соответствии с настоящим Положением в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

7.4.6. Разрешать доступ к ПДн только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПДн, которые необходимы для выполнения их должностных обязанностей.

7.4.7. Применять меры защиты конфиденциальной информации, действующие в Организации, при сборе, обработке и хранении ПДн – как для бумажных, так и для электронных (автоматизированных) носителей информации.

8. Правила и порядок уточнения, блокирования и уничтожения персональных данных.

8.1. Блокирование информации, содержащей ПДн субъектов ПДн, производится в случае:

8.1.1. Если ПДн являются неполными, устаревшими, недостоверными.

8.1.2. Если сведения являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

8.2. В случае подтверждения факта недостоверности ПДн сотрудник структурного подразделения Организации, обрабатывающий данную категорию ПДн, обязан уточнить ПДн и снять их блокирование.

8.3. В случае выявления неправомерных действий с ПДн сотрудник структурного подразделения Организации, обрабатывающего данную категорию ПДн, обязан устранить (организовать устранение) допущенные нарушения.

8.4. Организация обязана осуществлять уничтожение ПДн субъектов ПДн в следующих случаях:

8.4.1. Выявление неправомерной обработки ПДн, в том числе по обращению субъекта ПДн или его законного представителя либо запросу уполномоченного органа по защите прав субъектов ПДн, если обеспечить правомерность обработки ПДн невозможно.

8.4.2. Достижение целей обработки ПДн или утрата необходимости в достижении этих целей.

8.4.3. Отзыв субъектом ПДн согласия на обработку его ПДн, если сохранение ПДн более не требуется для целей обработки ПДн.

8.4.4. Истечение сроков хранения ПДн, установленных нормативными правовыми актами Российской Федерации.

8.4.5. Иные установленные законодательством Российской Федерации случаи.

8.5. Уничтожение ПДн должно быть осуществлено в соответствии со сроками, указанными частями 3 – 5 статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», с даты наступления указанных в п. 7.4 настоящего Положения случаев. Соглашением между Организацией и субъектом ПДн могут быть установлены иные сроки уничтожения ПДн при достижении цели обработки ПДн. В случае отсутствия возможности уничтожения персональных данных оператор осуществляет их блокирование в соответствии с частью 6 статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

8.6. Уничтожение носителей, содержащих ПДн субъектов ПДн, должно соответствовать следующим правилам:

8.6.1. Быть конфиденциальным, исключать возможность последующего восстановления.

8.6.2. Оформляться юридически, в частности, актом о выделении к уничтожению документов, содержащих ПДн субъектов ПДн (Приложение №2) и актом об уничтожении носителей, содержащих ПДн субъектов ПДн (Приложение №3).

8.6.3. Проводится Комиссией по уничтожению ПДн, созданной на основании приказа руководителя или главного врача.

8.7. Уничтожение ПДн на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление ПДн, или удалением ПДн с электронных носителей методами и средствами гарантированного удаления остаточной информации.

9. Рассмотрение запросов субъектов персональных данных.

9.1. Субъекты, чьи ПДн обрабатываются Организацией, имеют право на получение информации, касающейся обработки их ПДн, в том числе содержащей:

9.1.1. Подтверждение факта обработки ПДн в Организации.

9.1.2. Правовые основания и цели обработки ПДн.

9.1.3. Применяемые в Организации способы обработки ПДн.

9.1.4. Обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом.

9.1.5. Порядок осуществления субъектом ПДн прав, предусмотренных законодательством Российской Федерации в области ПДн.

9.1.6. Иные сведения, предусмотренные законодательством Российской Федерации в области ПДн.

9.2. Субъекты ПДн вправе требовать от Организации уточнения их ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

9.3. Сведения, указанные в пункте 9.1 настоящего Положения, предоставляются субъекту ПДн или его законному представителю на основании письменного запроса.

9.4. В случае если сведения, указанные в пункте 9.1 настоящего Положения, а также обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно в Организацию или направить повторный запрос в целях получения указанных сведений и ознакомления с такими ПДн не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

9.5. Субъект ПДн вправе обратиться повторно в Организацию и направить повторный запрос в целях получения сведений, указанных в пункте 9.1 настоящего Положения, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в пункте 9.4 настоящего Положения, в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения.

9.6. Организация вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 9.4 и 9.5 настоящего Положения. Такой отказ должен быть мотивированным.

9.7. Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, в том числе если доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

10. Защита персональных данных в Организации.

10.1. Организация самостоятельно или с привлечением внешней организации, обладающей лицензией Федеральной службы по техническому и экспортному контролю (ФСТЭК России) на деятельность по технической защите конфиденциальной информации, определяет необходимый уровень защищённости ПДн при их обработке в каждой из ИСПДн, оператором которой он является.

10.2. Организация самостоятельно или с привлечением организации, обладающей лицензиями на деятельность по технической защите конфиденциальной информации и на деятельность по выполнению работ и оказанию услуг в области шифрования информации, определяет и осуществляет организационные и технические мероприятия, которые должны выполняться для нейтрализации угроз ПДн, признанных актуальными.

10.3. Организация обеспечивает выполнение следующих мероприятий:

10.3.1. Обеспечивает режим безопасности помещений, в которых размещены ИСПДн, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

10.3.2. Обеспечивает сохранность носителей ПДн.

10.3.3. Обеспечивает актуальность перечня лиц, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей.

10.3.4. Использует средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

10.4. Лицо, ответственное за организацию обработки ПДн в Организации, получив информацию о факте нарушения действующих законодательных норм по обеспечению безопасности ПДн в ИСПДн, организует служебное расследование для выявления лиц, в результате действий или бездействия которых произошло нарушение законодательных норм по обеспечению безопасности ПДн.

10.5. Лица, виновные в нарушении норм, регулирующих обработку и защиту ПДн, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральным законодательством Российской Федерации и настоящим Положением.

11. Порядок предоставления доступа работников Организации к ПДн.

11.1. Доступ к ПДн имеют только работники Организации, которые обязаны осуществлять их обработку в связи с исполнением своих должностных обязанностей (лица, допущенные к работе с ПДн).

11.2. Процедура предоставления работнику доступа к ПДн предусматривает:

11.2.1. Ознакомление работника под подпись с настоящим Положением, иными локальными актами Организации по вопросам обработки ПДн, а также локальными актами, устанавливающими процедуры, направленные на выявление нарушений законодательства Российской Федерации в области обработки и защиты ПДн и устранение последствий таких нарушений.

11.2.2. Информирование работника о категориях обрабатываемых ПДн, об особенностях и правилах осуществления обработки ПДн.

11.2.3. Проведение инструктажа по соблюдению правил обработки и защиты ПДн. Форма журнала проведения инструктажа по информационной безопасности представлена в Приложении №4.

11.3. При увольнении работника, имеющего доступ к ПДн, документы и иные носители, содержащие ПДн, передаются другому работнику, имеющему доступ к ПДн по указанию руководителя увольняющегося работника.

11.4. Допуск работников к обработке ПДн до прохождения процедуры предоставления доступа запрещается.

[Оформляется на бланке организации]

АКТ

«__» _____ 20__ г.

г. Владивосток

№ _____

О выделении к уничтожению документов, содержащих ПДн субъектов ПДн

Комиссией в следующем составе:

председатель комиссии (указывается ФИО и должность председателя комиссии):

— _____;

члены комиссии (указывается ФИО и должность членов комиссии):

— _____;

— _____;

— _____.

действующей на основании: _____

составлен настоящий акт о том, что произведен отбор носителей персональных данных, подлежащих уничтожению. Уничтожению подлежат следующие носители персональных данных:

№ п/п	ФИО субъекта ПДн	Категория ПДн	Наименование ИСПДн	Наименование материального носителя (если обработка без средств автоматизации)	Кол-во страниц	Наименование информационной системы (если обработка с использованием средств автоматизации)	Причина
1							

Всего внесено в акт и подлежит уничтожению _____ (_____) документов (листов документов) путем (указывается способ уничтожения носителей персональных данных) _____.

Председатель комиссии: _____ И. О. Фамилия

Члены комиссии: _____ И. О. Фамилия

_____ И. О. Фамилия

_____ И. О. Фамилия

[Оформляется на бланке организации]

АКТ

«__» _____ 20__ г.

г. Владивосток

№ _____

Об уничтожении документов, содержащих персональные данные субъектов персональных данных

Комиссией в следующем составе:

председатель комиссии (указывается ФИО и должность председателя комиссии):

— _____;

члены комиссии (указывается ФИО и должность членов комиссии):

— _____;

— _____;

— _____.

действующей на основании: _____

составлен настоящий акт о том, что согласно утвержденному акту о выделении к уничтожению носителей, содержащих персональные данные субъектов персональных данных, от «__» _____ 20__ г. произведено уничтожение носителей персональных данных путем (указывается способ уничтожения носителей персональных данных) _____.

Все перечисленные в акте о выделении к уничтожению носителей, содержащих персональные данные субъектов персональных данных, от «__» _____ 20__ г. носители персональных данных, в количестве _____ сверены с актом и полностью уничтожены в присутствии всех членов комиссии.

Председатель комиссии: _____ И. О. Фамилия

Члены комиссии: _____ И. О. Фамилия

_____ И. О. Фамилия

_____ И. О. Фамилия

Общество с ограниченной ответственностью «Медицинская организация «Лотос»

УТВЕРЖДАЮ

Директор

_____ А.А. Левченко

«_____» _____ 20__ г.

Ж У Р Н А Л

проведения инструктажа по информационной безопасности

Начат «_____» _____ 20__ г.

Окончен «_____» _____ 20__ г.

Инструкция пользователя в информационных системах персональных данных ООО МО «Лотос»

1. Общие положения.

1.1. С целью автоматизации процессов, в ООО МО «Лотос» (далее – Организация) введены информационные системы персональных данных (далее – ИСПДн). Их перечень представлен в соответствующем приказе, утверждаемым руководителем Организации.

1.2. К работе с компонентами ИСПДн допущены системные администраторы, специалисты технической поддержки, администратор информационной безопасности (далее – Администратор) и пользователи информационной системы (далее – Пользователи). В Организации назначен ответственный за организацию обработки персональных данных (далее – Ответственный).

1.3. С целью защиты информации от несанкционированного нарушения ее конфиденциальности, целостности и доступности в ИСПДн организационными и техническими средствами реализована система защиты информации.

1.4. Несмотря на то, что многие действия по защите информации производятся прозрачно для Пользователя, он остается активным участником процесса по защите конфиденциальной информации и является вовлеченным в процессы обеспечения информационной безопасности в Организации.

1.5. Пользователи ИСПДн не являются привилегированными пользователями информационной системы. Каждому Пользователю предоставляется минимально необходимый для выполнения своих служебных обязанностей доступ к ресурсам ИСПДн.

1.6. Пользователи ИСПДн при работе с техническими средствами и информационными технологиями, являющимися частью ИСПДн должны соблюдать положения настоящей Инструкции.

1.7. Настоящая инструкция разработана с учетом положений следующих законодательных и нормативно-правовых актов:

1.7.1. Федеральный закон от 27.07.2006 года № 149-ФЗ «Об информации, информатизации и защите информации»;

1.7.2. Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных»;

1.7.3. «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ от 01.11.2012 № 1119;

1.7.4. «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России от 18.02.2013 № 21;

1.7.5. «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 от 10.07.2014 № 378;

1.7.6. «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ от 09.02.2005 № 66;

1.7.7. «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 13.06.2001 № 152.

2. Общие обязанности пользователя по защите информации в ИСПДн.

2.1. Пользователь в ИСПДн выполняет только те действия, которые необходимы для выполнения его служебных обязанностей. Любые посторонние действия в ИСПДн запрещены.

2.2. Пользователь незамедлительно оповещает Администратора о любой подозрительной активности в ИСПДн.

2.3. Пользователю запрещено использовать личные технические средства (ноутбуки, смартфоны, планшеты, фотокамеры, флеш-носители, съемные жесткие диски и пр.) для несанкционированного копирования, фотографирования, распространения и передачи защищаемой информации.

2.4. Пользователь визуально контролирует целостность технических средств на своем рабочем месте (отсутствие попыток физического вскрытия системного блока и пр.). При подозрении на нарушение целостности технических средств ИСПДн, Пользователь сообщает об этом Администратору. Пользователю запрещен самостоятельный ремонт технических средств ИСПДн, а также привлечение посторонних лиц для такого ремонта.

2.5. В целях блокирования возможности несанкционированного ознакомления с защищаемой информацией на экране монитора, Пользователь должен блокировать сеанс работы в ИСПДн при покидании рабочего места более чем на 2 минуты. Блокировка сеанса работы в ИСПДн производится нажатием комбинации клавиш Win+L.

2.6. Пользователю запрещены любые действия в ИСПДн до прохождения процедуры идентификации и аутентификации в системе (до ввода логина и пароля).

2.7. Пользователю запрещено изменение источника загрузки своего автоматизированного рабочего места (далее – АРМ) и загрузка АРМ с внешних носителей.

2.8. Пользователю запрещается в любых целях самостоятельное вскрытие системного блока АРМ.

2.9. Антивирусная защита в ИСПДн реализована прозрачно для пользователя, установка антивирусных программ, обновление антивирусных баз, запуск антивирусных проверок, сбор информации о найденных вирусах производится Администратором централизованно. Пользователю запрещено изменять настройки антивирусного программного обеспечения или отключать его (даже на короткое время). Пользователь должен оповещать Администратора о локальных сообщениях антивирусного программного обеспечения на его АРМ. Пользователь должен оповещать Администратора о любых аномалиях в работе АРМ.

2.10. Пользователю запрещается самостоятельная установка любого программного обеспечения, даже необходимого для выполнения своих служебных обязанностей. Установка разрешенного в ИСПДн программного обеспечения осуществляется Администратором и системными администраторами ИСПДн. Также к установке и настройке программного обеспечения в ИСПДн, при условии соблюдения мер по защите информации, допускаются сотрудники сторонних организаций.

2.11. Пользователь должен пресекать попытки посторонних лиц (или лиц, не имеющих соответствующих полномочий) тем или иным образом получить доступ к его учетным данным, конфиденциальной информации в ИСПДн, ключевой информации криптосредства и к любой другой защищаемой информации. Пользователь незамедлительно сообщает Администратору о подобных попытках (как удачных, так и неудачных).

2.12. Администратор отключает возможность использования на АРМ технологий мобильного кода (JavaScript, Adobe Flash, макросы в Microsoft Office и др.). Пользователю запрещено использовать технологии мобильного кода в обход принятых в Организации политик информационной безопасности.

2.13. Пользователь в меру своих сил и возможностей содействует проведению служебных расследований, инициированных в связи с инцидентами информационной безопасности.

2.14. Пользователь осуществляет обработку защищаемой информации в ИСПДн в соответствии с технологическими процессами обработки информации, описанными в Политике в отношении обработки персональных данных.

2.15. Пользователь принимает меры по противодействию несанкционированному просмотру защищаемой информации с экрана монитора посторонними лицами. К таким мерам относятся:

2.15.1. Сворачивание окна, в котором отображена защищаемая информация или блокирование сеанса Пользователя при нахождении посторонних лиц вблизи рабочего места Пользователя с фронтальной стороны монитора;

2.15.2. Ориентация монитора задней частью к дверным проемам и окнам.

2.15.3. В случае вынужденной ориентации монитора фронтальной частью к окну, Пользователь во время работы с защищаемой информацией закрывает шторы или жалюзи.

2.16. Пользователь должен знать и соблюдать положения настоящей Инструкции, а также других внутренних нормативных документов Организации. При возникновении у Пользователя вопросов по защите информации и защите персональных данных в Организации, он обращается к Администратору и Ответственному.

2.17. При работе с криптографическими средствами защиты информации (СКЗИ) Пользователь выполняет предписание Инструкции по обеспечению безопасности эксплуатации СКЗИ.

3. Правила управления идентификаторами, учетными записями и паролями.

3.1. В Организации с целью обеспечения информационной безопасности внедрены политики управления идентификаторами, учетными записями и паролями.

3.2. Внутренними руководящими документами, определяющими политики управления идентификаторами, учетными записями и паролями являются:

3.2.1. Политика в отношении обработки персональных данных.

3.2.2. Положение об обработке и защите персональных данных.

3.2.3. Инструкция администратора информационной безопасности.

3.2.4. Инструкция пользователя ИСПДн.

3.2.5. Инструкция по организации парольной защиты в ИСПДн.

3.3. Пользователю запрещено записывать и хранить пароли в местах, доступных для просмотра посторонним лицам (на отдельных листах бумаги, в не запираемой тумбе, под клавиатурой, на мониторе и т. п.).

3.4. Пользователь должен удостовериться, что при вводе пароля никто не наблюдает за процессом ввода пароля.

3.5. Пользователю запрещено разглашать другим пользователям свой пароль, в том числе Администратору.

3.6. Пользователю запрещено вводить свои учетные данные для предоставления возможности временной работы в ИСПДн другим Пользователями или посторонним лицам, поскольку все выполненные этими лицами действия в ИСПДн будут считаться действиями, выполненными Пользователем. Ответственность за неправомерные действия таких посторонних лиц несет Пользователь.

3.7. Пользователю запрещено оставлять без присмотра персональный идентификатор (электронный ключ).

3.8. При подозрении на компрометацию пароля или иной идентификационной информации, Пользователь должен незамедлительно сообщить об этом Администратору.

4. Противодействие методам социальной инженерии и правила работы с электронной почтой.

4.1. Применение злоумышленником методов социальной инженерии является самым эффективным и разрушительным способом нарушения информационной безопасности на любом предприятии в обход всех технических мер по защите информации. Методы социальной инженерии направлены на использование человеческого фактора (человеческих слабостей и недостатков) с целью получения от Пользователя защищаемой информации или его учетных данных в ИСПДн (логин и пароль). Злоумышленники - социальные инженеры для достижения своих целей могут эксплуатировать следующие особенности того или иного Пользователя:

4.1.1. Лень.

4.1.2. Спешка (паника).

4.1.3. Безразличие.

4.1.4. Профессиональный интерес.

4.1.5. Желание.

4.1.6. Жадность.

4.1.7. Сострадание.

4.1.8. Доверчивость.

4.1.9. Страх.

4.2. Основным способом реализации методов социальной инженерии является обман Пользователя. Поскольку социальная инженерия нацелена на слабости человека, а не на технические недоработки или уязвимости информационной системы, наиболее эффективным методом противодействия социальной инженерии является повышение осведомленности Пользователей о методах социальной инженерии.

4.3. Взаимодействие социального инженера с Пользователем бывает трех типов: контактное (личное), телефонное и взаимодействие через электронные каналы связи. Наиболее распространено взаимодействие через электронные каналы связи, в особенности по электронной почте.

4.4. При личном и телефонном общении Пользователь должен убедиться, что разговаривает именно с тем человеком, за которого себя выдает собеседник. При личном или телефонном взаимодействии социальный инженер обычно использует следующие тактики:

4.4.1. Представившись сотрудником технической поддержки какого-либо сервиса или службы, социальный инженер сообщает Пользователю о какой-либо поломке или нарушении в функционировании того или иного необходимого в работе сервиса, вызывая тем самым панику и заставляя Пользователя сообщить свои учетные данные.

4.4.2. Представившись руководителем высокого ранга, социальный инженер изображает гнев и недовольство действием или бездействием Пользователя, вынуждая сообщить учетные данные или иную конфиденциальную информацию.

4.4.3. Представившись сотрудником организации, деятельность которой так или иначе может быть интересна Пользователю вынуждает сообщить учетную или иную конфиденциальную информацию.

4.4.4. Иные подобные тактики.

4.5. При взаимодействии через электронную почту, социальный инженер преследует одну из двух основных целей:

4.5.1. Заражение АРМ Пользователя вредоносным программным обеспечением через запуск вложенного к письму файла или переходом по вредоносной ссылке.

4.5.2. Переход Пользователя по поддельной ссылке, по которой находится точная копия формы авторизации легального сервиса и ввод в эту форму идентификационной информации (как правило, при первом вводе логина и пароля поддельная форма сообщает о неправильном вводе пароля и перенаправляет на настоящую форму авторизации сервиса).

4.6. Наиболее распространенные примеры применения методов социальной инженерии с использованием каналов электронной почты:

4.6.1. Письмо от налоговой инспекции с предложением установить из вложенного файла новые формы для сдачи налоговых деклараций.

4.6.2. Письмо из банка о просроченном платеже по кредиту, подробности во вложенном файле.

4.6.3. Письмо из суда о возбуждении административного/уголовного дела, подробности во вложении.

4.6.4. Письмо от провайдера об одностороннем изменении тарифного плана, подробности во вложении.

4.6.5. Письмо от банка (или любого другого учреждения) о блокировке учетной записи на сайте или личного кабинета, необходимо пройти по ссылке, ввести учетные данные и вручную разблокировать личный кабинет или учетную запись.

4.6.6. Письмо от сервиса электронной почты (gmail.com, mail.ru, yandex.ru и т. п.) о грядущей блокировке почтового ящика, об исчерпании свободного места и т. д., необходимо пройти по ссылке, ввести учетные данные и выполнить некоторые действия.

4.7. При работе с электронной почтой в контексте противодействия методам социальной инженерии Пользователь руководствуется следующей информацией:

4.7.1. Совпадение адреса отправителя электронного письма с доверенным адресом не является гарантией подлинности самого письма, поскольку поле «от кого» может быть подделано злоумышленником.

4.7.2. Любые письма с вложениями являются подозрительными.

4.7.3. Любые письма, в которых отсутствует альтернативная контактная информация отправителя (ФИО, должность, мобильный, рабочий телефон, почтовый адрес) являются подозрительными.

4.7.4. При получении неожиданного электронного письма с вложением или ссылкой от якобы доверенного отправителя, необходимо по альтернативным каналам связи (лично, по телефону, через мессенджер) уточнить факт отправки такого письма.

4.7.5. Государственные и иные организации (банки, операторы связи и т. д.) не уведомляют своих клиентов о каких-либо проблемах, исках, блокировках по электронной

почте, это делается официальным письмом на бумажном носителе, через СМС (например, в случае подключенного онлайн банкинга) или по телефону.

4.7.6. Необходимо тщательно проверять корректность ссылок, по которым просят пройти в письме, чаще всего злоумышленники используют похожие, но другие доменные имена, чтобы ввести Пользователя в заблуждение, например, заменяя букву «b» на букву «d» или цифру «1» на букву «l» и наоборот.

4.8. Атаки социальных инженеров могут быть веерными (нацеленными на как можно большее число жертв), так и целенаправленными (нацеленными на конкретную организацию или на конкретного человека). В случае целенаправленных атак, социальный инженер изучает информацию о потенциальной жертве и об организации из открытых источников (сайт компании, сайты партнеров и контрагентов, электронные биржи труда, социальные сети, новостные ленты и прочие ресурсы). В случае, если о Пользователе публикуется информация в открытых источниках или он сам публикует информацию о своем месте работы, роде деятельности, должностных обязанностях, Пользователь должен быть готов к применению этой информации социальным инженером против него.

4.9. В случае подозрения Пользователя на применение против него методов социальной инженерии, Пользователь незамедлительно сообщает о данном факте Администратору.

5. Работа со съемными носителями информации.

5.1. Пользователю разрешается использовать только учтенные съемные носители информации в ИСПДн (флеш-накопители, съемные жесткие диски, карты памяти и пр.).

5.2. При необходимости выноса съемного носителя из помещения, Пользователь обеспечивает защиту съемного носителя от утери, кражи или компрометации защищаемой информации на этом носителе.

5.3. В случае утери, кражи или компрометации учтенного носителя, Пользователь оперативно сообщает об этом Администратору.

5.4. Пользователь несет ответственность за сохранность выданных ему съемных носителей информации и за конфиденциальность защищаемой информации, записанной на него.

Инструкция по организации парольной защиты в информационных системах персональных данных ООО МО «Лотос»

1. Общие положения.

1.1. Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее – ИСПДн) в ООО МО «Лотос» (далее – Организация), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2. Идентификация/аутентификация пользователей осуществляется посредством использования паролей, при технической возможности - средствами усиленной аутентификации.

1.3. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн Организации возлагается на администратора безопасности.

2. Порядок организации работы пользователя ИСПДн с использованием пароля.

2.1. Доступ к защищаемым информационным активам Организации должен производиться с использованием персональных учетных записей и периодически сменяемых буквенно-цифровых паролей, удовлетворяющих следующим требованиям:

2.1.1. Пароль содержит не менее шести символов, включая буквы обоих регистров и цифры.

2.1.2. Не является профессиональным термином, в том числе набранным в другой раскладке клавиатуры.

2.1.3. Не основывается на семейной, служебной и другой легко доступной информации (фамилии, имена, даты рождения, клички животных, автомобильные и телефонные номера, названия организаций, адреса сайтов и т. п.).

2.1.4. Не содержит легко угадываемые последовательности символов (123456, aaabbb, qwerty, q1w2e3, qazwsx, qazxsw и т. п.).

2.1.5. Не совпадает с номером помещения, названием подразделения, месяцем (312313, бухгалтерия, январь, март2011).

2.2. Одним из способов создания безопасных, но легко запоминающихся паролей является кодирование стихотворной строки или осмысленного утверждения. Так, пароль, созданный на основе фразы: "Вот один пример надежного и запоминающегося пароля", может быть таким: «VotlPN&ZP».

2.3. Ещё одним из способов создания безопасных, но легко запоминающихся паролей является кодирование фразы первыми тремя буквами каждого слова. Так, пароль, созданный на основе фразы «хозяйственный фермер заколол петуха», будет таков «[jpathpfrgtn», что соответствует буквам на русской раскладке «хозферзакпет».

2.4. Временный пароль, создаваемый при заведении учетной записи или смене забытого пароля, должен быть уникальным, передаваться способом, исключающим доступ к

нему других лиц, и быть сменен пользователем при первом обращении к активу. Пароли, предустановленные производителем, должны сменяться до начала эксплуатации актива.

2.5. Пользователям запрещается:

2.5.1. Сообщать свой персональный пароль другим лицам или записывать его на материальных носителях, доступных для других лиц (кроме предусмотренных случаев сохранения паролей ключевых учетных записей владельцем информационного актива);

2.5.2. Сохранять пароль в программно-технических средствах в открытом виде или использовать средства его автоматического ввода;

2.5.3. Использовать легко угадываемый алгоритм смены пароля (например, «F%1hTR8» => «F%1hTR9»)

2.5.4. Использовать учетные записи других лиц;

2.5.5. Использовать вне Организации пароли, совпадающие с паролями доступа к его информационно-технологическим активам;

2.5.6. Использовать в качестве паролей примеры, приведенные в Инструкции.

2.6. Резервирование паролей в Организации не предусмотрено.

3. Порядок смены паролей.

3.1. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в три месяца.

3.2. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн проводится в случае прекращения его полномочий (увольнение, переход на другую работу внутри территориального органа организации и т.п.).

3.3. В случае компрометации личного пароля пользователя ИСПДн проводится внеплановая смена пароля в зависимости от полномочий владельца скомпрометированного пароля.

4. Заключительные положения.

4.1. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на руководителей подразделений Организации, периодический контроль – возлагается на администратора безопасности.

4.2. В зависимости от критичности информационно-технологического актива, его владельцем могут быть установлены более высокие требования к сложности пароля и периодичности смены.

4.3. Процессы создания, изменения, использования, блокирования, удаления учетных записей, а также смены паролей должны контролироваться.

Инструкция по организации антивирусной защиты в ООО МО «Лотос»

1. Общие положения.

1.1. Настоящая инструкция определяет требования к организации защиты информационных ресурсов и программных средств вычислительной техники от разрушающего воздействия компьютерных вирусов, а также порядок применения средств антивирусного контроля в информационных системах, предназначенных для обработки сведений ограниченного доступа, не относящихся к государственной тайне.

1.2. Для выполнения антивирусного контроля и защиты информационных систем допускаются только лицензионные антивирусные средства.

1.3. Определение параметров и режимов работы средств антивирусного контроля осуществляется администратором безопасности.

1.4. Установка и настройка средств антивирусного контроля в информационных системах осуществляется администратором безопасности, системным администратором или специалистом технической поддержки.

2. Требования по применению средств антивирусного контроля.

2.1. Обязательному антивирусному контролю подлежат все файлы на машинных носителях, получаемые для обработки в защищенных информационных системах, а также передаваемые из одних систем для дальнейшей обработки в других информационных системах.

2.2. Вновь получаемые файлы должны пройти антивирусный контроль до начала их обработки в информационной системе.

2.3. Используемые для записи и хранения машинные носители информации перед использованием должны проходить антивирусный контроль.

2.4. Передаваемые в сторонние организации документы и файлы на машинных носителях должны проходить антивирусный контроль непосредственно перед записью на носитель, а запись должна быть выполнена за время текущего сеанса работы пользователя.

2.5. Машинные носители информации с программным обеспечением при постановке на учет (реестр, список, журнал) должны быть предварительно проверены администратором безопасности на отсутствие угрозы заражения.

2.6. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и др.) пользователь обязан немедленно сообщить о своих подозрениях администратору безопасности и затем выполнить внеочередной антивирусный контроль.

2.7. Если при проведении антивирусной проверки информационных ресурсов информационной системы были обнаружены вирусы или их воздействие на носители информации, администратор безопасности обязан:

2.7.1. Приостановить обработку информации в информационной системе.

2.7.2. Провести очистку зараженных файлов.

2.7.3. В случае обнаружения нового вируса, не поддающегося «лечению» применяемыми антивирусными средствами, исключить из обработки зараженный вирусом файл.

2.7.4. Выполнить проверку всех машинных носителей информации в информационной системе, которые могли стать носителями вируса.

2.7.5. По факту обнаружения зараженных вирусом файлов администратор безопасности составляет служебную записку в адрес директора с указанием предположительного источника зараженного файла, типа зараженного файла, характера распространения, применённых мер по устранению вируса.