Общество с ограниченной ответственностью «Дента-Л»
ООО «Дента-Л»

ПРИКАЗ

«09» января 2017 г. №24

г. Ставрополь

об утверждении должностных инструкций в области информационной безопасности

Во исполнение требований Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить Должностную инструкцию ответственного за организацию обработки персональных данных, Должностную инструкцию администратора безопасности информационных систем персональных данных, Должностную инструкцию работников, допущенных к обработке конфиденциальной информации согласно приложениям.
2. Ответственному за организацию работы по обработке и защите персональных данных – заместителю генерального директора по медицинской части Савченко Ю. А. ознакомить под роспись работников с настоящим приказом.
3. Контроль за исполнением настоящего приказа оставляю за собой.
4. Приказ вступает в силу со дня его подписания.

Руководитель организации **Генеральный директор** _____ **А. И. Латиган**
(должность) (личная подпись) (расшифровка подписи)

С приказом (распоряжением) работник ознакомлен _____ 09 01 2017 г.
(личная подпись)

Приложение № 1
к приказу от «09» января 2017

УТВЕРЖДАЮ:
Генеральный директор
ООО «Дента-Л»

А. И. Латиган

«09» января 2017 г.

ФОРМА

должностной инструкции ответственного за организацию обработки персональных данных

УТВЕРЖДАЮ:
Генеральный директор
ООО «Дента-Л»

А. И. Латиган

«_____»_____ 201__ г.

Должностная инструкция ответственного за организацию обработки персональных данных

I. Общие положения

1.1. Должностная инструкция разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных».

1.2. Ответственный за организацию обработки персональных данных в ООО «Дента-Л» назначается приказом генерального директора.

1.3. Ответственный за организацию обработки персональных данных в своей деятельности руководствуется Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных», Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01 ноября 2012 г. №1119, Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15 сентября 2008 г. №687, приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. №21 «Об

обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», другими законодательными и нормативно-правовыми актами по вопросам обработки и защиты персональных данных.

II. Обязанности ответственного за организацию обработки персональных данных

2.1. Ответственный за организацию обработки персональных данных обязан:

- осуществлять внутренний контроль за соблюдением работниками законодательства Российской Федерации, локальных актов по обработке персональных данных, требований к защите персональных данных и принимать меры по устранению выявленных нарушений;
- организовывать проведение занятий и (или) доведение до сведения работников положений законодательства Российской Федерации о персональных данных, локальных актов Федерального казначейства по вопросам обработки персональных данных, требований к защите персональных данных;
- руководить разработкой приказов, положений, инструкций, правил, порядков, перечней и других документов, регламентирующих порядок обработки персональных данных по вопросам защиты персональных данных в соответствии с требованиями законодательства и нормативно-правовых актов Российской Федерации и Федерального казначейства;
- организовывать и контролировать прием и обработку обращений и запросов субъектов персональных данных или их представителей;
- при организации обработки персональных данных принимать необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного намеренного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных;
- докладывать директору о выявленных нарушениях обработки персональных данных или требований по их защите, принимаемых мерах и способах устранения выявленных нарушений.

III. Ответственность лица, ответственного за организацию обработки персональных данных

3.1. В соответствии с законодательством Российской Федерации ответственный за организацию обработки персональных данных несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность за невыполнение или халатное выполнение обязанностей по организации, контролю и обеспечению выполнения требований законодательства, нормативно-правовых актов Российской Федерации по вопросам обработки и защиты персональных данных.

IV. Права ответственного за организацию обработки персональных данных

4.1. Ответственный за организацию обработки персональных данных имеет право:

- требовать от работников письменных объяснений по фактам нарушения ими требований законодательства Российской Федерации, локальных актов о персональных данных и защите персональных данных;

- вносить предложения генеральному директору об отстранении работников от обработки персональных данных, применению к ним дисциплинарных взысканий, в том числе об увольнении работников, при обнаружении нарушения ими требований законодательства Российской Федерации, локальных актов по вопросам обработки персональных данных или требований к защите персональных данных.

Приложение № 2
к приказу от «09» января 2017

УТВЕРЖДАЮ:
Генеральный директор
ООО «Дента-Л»

А. И. Латиган

«09» января 2017 г.

ФОРМА

должностной инструкции администратора безопасности информационных систем персональных данных

УТВЕРЖДАЮ:
Генеральный директор
ООО «Дента-Л»

А. И. Латиган

«_____»_____ 201__ г.

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ
администратора безопасности информационных систем персональных данных

1 Область применения

1.1. Настоящая инструкция определяет уровень квалификации, круг ответственности и должностные обязанности администратора безопасности информационных систем персональных данных.

2 Нормативные ссылки

ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения

ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.

3 Определения и сокращения

В настоящей инструкции приняты следующие сокращения:

АВЗ — антивирусная защита;

Администратор — администратор безопасности информационных систем персональных данных;

ИС — информационная система
ЛВС — локальная вычислительная сеть
НСД — несанкционированный доступ
ОС — операционная система
СЗИ – средства защиты информации
СКЗИ — средства криптографической защиты информации
ЭП – электронная подпись

4 Общие положения

4.1. Настоящая инструкция разработана в соответствии с требованиями:

- Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- приказа ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4.2. Инструкция определяет основные задачи, функции, обязанности, права и ответственности администратора безопасности информационных систем.

4.3. Администратор безопасности назначается приказом генерального директора или лицом его заменяющим, из сотрудников руководящего состава, и является лицом, выполняющим функции по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники ИС, в пределах своей зоны ответственности.

4.4. Закрепление функциональных обязанностей и разделение зон ответственности производится приказом генерального директора.

4.5. В своей деятельности Администратор руководствуется требованиями действующих федеральных законов, общегосударственных, ведомственных, а также внутренних нормативных документов по вопросам защиты информации и обеспечивает их выполнение пользователями ИС.

4.6. Настоящая инструкция является дополнением к действующим нормативным документам по вопросам защиты информации и не исключает обязательного выполнения их требований.

5 Состав нормативно-методического обеспечения

5.1. Администратор для обеспечения соответствия уровня своей квалификации должностным обязанностям должен владеть нормативно-методическим обеспечением, приведенным в таблице 1.

№п/п	Нормативно-методическое обеспечение
1	Федеральный закон РФ от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»
2	Федеральный закон от 27.07.2006г №152-ФЗ «О персональных данных»
3	Федеральный закон от 06.04.2011г №63-ФЗ. «Об электронной подписи»
4	Федеральный закон от 04.05.2011г. №99-ФЗ «О лицензировании отдельных видов деятельности»
5	Указ Президента Российской Федерации от 6 марта 1997 г. №188 «Перечень сведений конфиденциального характера»
6	Указ Президента РФ от 12.05.2004 №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
7	Постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
8	Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных системах персональных данных»
9	Приказ ФСБ РФ от 27.12.2011 №796 "Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра"
10	Приказ ФСБ РФ от 09.02.2005 №66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)"
11	Приказ ФАПСИ №152 от 13.06.2001
12	Нормативные документы ФСТЭК России в части обеспечения защиты конфиденциальной информации
13	Нормативные документы ФСБ России в части использования СКЗИ при защите конфиденциальной информации
14	Организационно распорядительные документы

6 Состав специальных знаний Администратора

6.1 Администратор для обеспечения соответствия уровня своей квалификации должностным обязанностям должен владеть специальными знаниями, приведенными в таблице 2.

Таблица 2

№п/п	Специальные знания
1	Операционные системы семейства Windows на уровне администратора безопасности ОС
2	Сетевые технологии на уровне администратора безопасности ЛВС и администратора безопасности информационных сервисов
3	Средства криптографической защиты информации на уровне администратора
4	Средства защиты информации от НСД на уровне администратора
5	Системы АВЗ на уровне администратора
6	Средства ЭП

6.2 В своей деятельности Администратор руководствуется:

- действующим законодательством РФ;
- руководящими документами регуляторов в области защиты информации;
- Организационно распорядительными документами;
- заданиями генерального директора.

6.3 На время отсутствия Администратора его замещение возлагается на должностное лицо, назначаемое приказом директора.

7 Состав должностных обязанностей Администратора

7.1 В сферу ответственности Администратора входит исполнение следующих обязанностей, приведенных в таблице 3.

Таблица 3.

№п/п	Должностная обязанность
1.	Выполнять мероприятия по соблюдению требований информационной безопасности
2.	Участвовать в составе рабочих групп при проведении контрольно-ревизионных мероприятий по соблюдению требований информационной безопасности
3.	Обеспечивать организацию мероприятий по разработке и актуализации нормативных документов по ИБ
4.	Отслеживать изменения в законодательной базе по вопросам обеспечения информационной безопасности с подготовкой докладных записок руководителю
5.	Разрабатывать и актуализировать внутренние требования, методик, инструкций и регламентов по обеспечению ИБ с учетом реальных режимов эксплуатации ИС для последующего их согласования и включения в нормативную базу по ИБ
6.	Осуществлять мероприятия по созданию и модернизации систем ИБ
7.	Организовывать и участвовать в расследованиях инцидентов информационной безопасности

№п/п	Должностная обязанность
8.	Организовывать и участвовать в мероприятиях по оценке защищенности конфиденциальной информации, обрабатываемой в ИС
9.	Оказывать практическую помощь по вопросам информационной безопасности работникам
10.	Организовывать и обеспечивать сохранность зафиксированной на бумажных и электронных носителях конфиденциальной информации
11.	Вести учет (по вопросам обеспечения безопасности информации) и знать перечень установленных СЗИ и перечень задач, решаемых с их использованием;
12.	Вести журнал учета средств защиты информации, эксплуатационной и технической документации к ним;
13.	Вести журнал учета машинных носителей персональных данных;
14.	Осуществлять непосредственное управление режимами работы и административную поддержку функционирования (настройку и сопровождение) применяемых на автоматизированных рабочих местах специальных программных и программно-аппаратных СЗИ;
15.	Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных АРМ и серверов, осуществлять проверку работоспособности системы защиты после установки (обновления) программных средств ИС;
16.	Периодически проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки (выборочное тестирование);
17.	Контролировать соответствие технического паспорта ИС фактическому составу (комплектности) ИС и вести учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения в ИС);
18.	Периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищенных АРМ;
19.	Вести журнал учета нештатных ситуаций, фактов вскрытия и опечатывания АРМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств ИС;
20.	Проводить периодический инструктаж сотрудников (пользователей ИС) по правилам работы с используемыми средствами и системами зашиты информации;
21.	Участвовать в разработке и знать перечень защищаемых информационных ресурсов.

7.2 Администратор разрабатывает для ИС решения по:

- определению информационных связей между сегментами сети и требований к их изоляции;

пользования, с указанием состава допущенных к ним пользователей и режимов допуска;

- осуществлению контроля над использованием разделяемых ресурсов;
- разработке порядка выхода пользователей в сети связи общего пользования и использованию встроенных СЗИ в сервисных программах;
- определению режимов использования СЗИ: защита паролей, защита в протоколах передачи данных, шифрование файлов, подключение алгоритмов криптографической защиты;
- разработке политики аудита: определению состава регистрируемых событий и списка лиц, имеющих допуск к журналам аудита;
- осуществлению учета и периодического контроля над составом и полномочиями пользователей ИС;
- контролю и требованию соблюдения установленных правил по организации парольной защиты в ИС;
- осуществлению оперативного контроля над работой пользователей защищенных АРМ, анализа содержимого журналов событий операционных систем, систем управления базами данных, пакетов прикладных программ и СЗИ всех АРМ и реагированию на возникающие внештатные ситуации.
- обеспечению строгого выполнения требований по обеспечению безопасности информации при организации технического обслуживания АРМ и отправке их в ремонт (контролировать стирание информации на съемных носителях);
- организации учета, хранения, приема и выдачи персональных идентификаторов ответственным исполнителям, осуществление контроля над правильностью их использования;
- осуществлению периодического контроля над порядком учета, создания, хранения и использования резервных и архивных копий массивов данных;
- своевременному и точному отражению изменений в организационно-распорядительных и нормативных документах по управлению СЗИ, установленных в ИС по указанию руководства;
- контролю обеспечения защиты конфиденциальной информации при взаимодействии пользователей с информационными сетями связи общего пользования.

7.3 Администратор наделен функцией контролировать эффективность защиты информации, в том числе:

- проводить работу по выявлению возможности вмешательства в процесс функционирования ИС и осуществления НСД к информации

- докладывать ответственному по обеспечению безопасности о выявленных угрозах безопасности информации, обрабатываемой в ИС,
- об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ;
- участвовать в расследовании причин возникновения нарушений и внештатных ситуаций в ИС.

7.4 Администратору запрещается:

- используя служебное положение, создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к информации и предоставлять его другим с целью ознакомления, модификации, копирования, уничтожения, блокирования доступа к информации;
- использовать ставшие доступными в ходе исполнения обязанностей идентификационные данные пользователей (имя, пароль, ключи и т. п.) для маскирования своих действий;
- самостоятельно (без согласования с подразделением автоматизации) вносить изменения в настройки серверной части ИС;
- использовать в своих и в чьих-либо личных интересах ресурсы ИС, предоставлять такую возможность другим;
- выключать средства защиты информации без письменной санкции руководства;
- передавать третьим лицам тем или иным способом сетевые адреса, имена, пароли, информацию о привилегиях пользователей, конфигурационные настройки;
- производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы ИС, блокированию доступа, потере информации без санкции руководства и предупреждения пользователей;
- нарушать правила эксплуатации оборудования ИС;
- корректировать, удалять, подменять журналы аудита.

8 Права и ответственность администратора

8.1. Администратор имеет право:

- получать доступ к программным и аппаратным средствам ИС, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах ИС и АРМ пользователей;
- требовать от пользователей ИС выполнения инструкций по обеспечению безопасности и защите информации в ИС;
- участвовать в служебных расследованиях по фактам нарушения

НСД, утраты, порчи защищаемой информации и технических компонентов ИС;

- осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности;
- производить анализ защищенности ИС путем применения специального программного обеспечения, осуществления попыток взлома системы защиты ИС. Такие работы должны проводиться в часы наименьшей информационной нагрузки с обязательным уведомлением сотрудников подразделений автоматизации и обеспечение безопасности информации;
- вносить свои предложения по совершенствованию мер защиты в ИС.

9 Ответственность

9.1. Администратор несет ответственность за:

- реализацию принятой локальной документации по информационной безопасности;
- программно - технические средства защиты информации, средства вычислительной техники, информационно - вычислительные комплексы, сети и ИС обработки информации, закрепленные за ним приказом, а также за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями;
- разглашение сведений, конфиденциального характера, ставших известными ему по роду работы;
- качество и последствия проводимых им работ по контролю действий пользователей при работе в ИС;
- неисполнение или ненадлежащее исполнение своих обязанностей, предусмотренных настоящей инструкцией;
- несоблюдение действующего законодательства и внутренних документов по информационной безопасности и защите персональных данных;
- разглашение служебной и иной конфиденциальной информации, ставшей ему известной в процессе исполнения служебных обязанностей;
- несоблюдение правил и норм охраны труда, техники безопасности и противопожарной защиты.

Приложение № 3
к приказу от «09» января 2017

УТВЕРЖДАЮ:
Генеральный директор
ООО «Дента-Л»

А. И. Латиган

«09» января 2017 г.

ФОРМА

должностной инструкции работников, допущенных к обработке конфиденциальной информации

УТВЕРЖДАЮ:
Генеральный директор
ООО «Дента-Л»

А. И. Латиган

«_____»_____ 201__ г.

Должностная инструкция
работников, допущенных к обработке конфиденциальной информации

1. Общие положения

1.1. Настоящая инструкция разработана в соответствии с требованиями:

- Федерального закона Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- «Требований к защите персональных данных при их обработке в информационных системах персональных данных» утвержденной постановлением Правительства Российской Федерации от 01.11.2012 №1119.

1.2. Данная инструкция определяет общие обязанности, права и ответственность пользователя информационных систем по обеспечению информационной безопасности при работе со сведениями конфиденциального характера.

1.3. Пользователем ИС (далее – Пользователь) является работник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ

1.4. Пользователь в своей работе руководствуется, кроме должностных и технологических инструкций, действующими нормативными, организационно-распорядительными документами по вопросам информационной безопасности.

1.5. Положения инструкции обязательны для исполнения всеми пользователями и доводятся до сотрудников под роспись. Пользователь должен быть предупрежден о возможной ответственности за ее нарушение.

2. Обязанности пользователя

2.1. При выполнении работ в ИС Пользователь обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС, правила работы и порядок регистрации в ИС, доступа к информационным ресурсам ИС;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (далее - АРМ);
- хранить втайне свои идентификационные данные (имена, пароли и т. д.);
- выполнять требования, предъявляемые к парольной системе (нормативы на длину, состав, периодичность смены пароля и т. д.), осуществлять вход на АРМ только под своими идентификационными данными;
- передавать для хранения установленным порядком свое индивидуальное устройство идентификации, личную ключевую дискету и другие реквизиты разграничения доступа, только руководителю своего подразделения или администратору безопасности ИС (ответственному за информационную безопасность подразделения);
- выполнять требования «Инструкции по организации антивирусной защиты» в части, касающейся действий пользователей ИС;
- немедленно вызывать администратора безопасности ИС и ставить в известность руководителя подразделения в случае утери персональной ключевой дискеты, индивидуального устройства идентификации или при подозрении о компрометации личных ключей и паролей, а также при обнаружении нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к защищенной АРМ, несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ, некорректного функционирования установленных на АРМ технических средств защиты, непредусмотренных отводов кабелей и подключенных устройств;
- присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним АРМ, ставить в известность администратора безопасности ИС при необходимости

- работать в ИС только в разрешенный период времени;
- немедленно выполнять предписания администраторов безопасности ИС, предоставлять свое АРМ администратору безопасности для контроля;
- ставить в известность администраторов ИС в случае появления сведений или подозрений о фактах несанкционированного доступа к информации, своей или чужой, а также отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т. п.), а также перебоев в системе электроснабжения;
- осуществлять установленным порядком уничтожение информации, содержащей сведения конфиденциального характера, с машинных носителей информации и из оперативной памяти АРМ;
- уважать права других пользователей на конфиденциальность и право пользования общими ресурсами;
- сообщать руководителю своего подразделения обо всех проблемах, связанных с эксплуатацией ИС.

2.2. Пользователю категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ИС в неслужебных целях;
- самовольно вносить какие-либо изменения в состав, размещение, конфигурацию аппаратно-программных средств ИС (в том числе АРМ) или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формуляром АРМ;
- осуществлять обработку информации, содержащей сведения конфиденциального характера, в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию на неучтенных носителях информации, в том числе для временного хранения;
- оставлять включенное без присмотра АРМ, не активизировав временную блокировку экрана и клавиатуры (средствами защиты от НСД или операционных систем);
- передавать кому-либо свое индивидуальное устройство идентификации (персональную ключевую дискету) в нарушение установленного порядка, делать неучтенные копии ключевого носителя, и вносить какие-либо изменения в файлы ключевого устройства идентификации;
- оставлять без личного присмотра на рабочем месте или где бы то ни было свою персональную ключевую дискету, персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения конфиденциального характера);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках ИС (в том числе средств защиты), которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность администратора безопасности ИС (ответственного за безопасность

- подбирать и отгадывать чужие пароли, а также собирать информацию о других пользователях;
- осуществлять попытки НСД к ресурсам системы и других пользователей, проводить рассылку ложных, беспокоящих или угрожающих сообщений;
- фиксировать свои учетные данные (пароли, имена, идентификаторы, ключи) на материальных носителях;
- разглашать ставшую известной в ходе выполнения своих обязанностей информацию, содержащую сведения конфиденциального характера;
- вносить изменения в файлы, принадлежащие другим пользователям.

3. Права пользователя

3.1. Пользователь имеет право:

- присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним АРМ;
- участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИС, если данное нарушение произошло под его идентификационными данными;
- своевременно получать доступ к информационным ресурсам ИС, необходимым ему для выполнения своих должностных обязанностей;
- требовать от администратора безопасности смены идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

4. Правила работы в сетях общего доступа

4.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее - Сеть) на элементах ИС, должна производиться при служебной необходимости.

4.2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирусной защиты, средств от несанкционированного доступа и т. д.);
- передавать по Сети защищаемую информацию без использования средств защиты каналов связи;
- запрещается загружать из Сети программное обеспечение;
- запрещается посещение сайтов сомнительной репутации (аморального содержания, содержащие нелегально распространяемое программное обеспечение или иной контент);
- запрещается нецелевое использование подключения к сети.

5. Ответственность пользователя

5.1. Пользователь несет персональную ответственность за:

- ненадлежащее исполнение своих функциональных обязанностей, а также сохранность комплекта АРМ, съемных носителей информации, индивидуального средства идентификации и целостность установленного программного обеспечения.
- разглашение сведений, отнесенных к сведениям конфиденциального характера, и сведений ограниченного распространения, ставших известными ему по роду работы.

5.2. Ответственность за нарушение функционирования ИС, уничтожение, блокирование, копирование, фальсификацию информации несет пользователь, под чьими идентификационными данными было совершено нарушение. Мера ответственности устанавливается по итогам служебного расследования.

5.3. Пользователи, виновные в нарушениях несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством и организационно-распорядительными документами.

Приложение 1

Выдержки из статей Уголовного кодекса РФ, определяющие ответственность пользователей за нарушение установленных правил обработки информации

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок до четырех лет.

Статья 293. Халатность

1. Халатность, то есть неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей вследствие недобросовестного или небрежного отношения к службе, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, - наказывается штрафом в размере от ста до двухсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до двух месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок от шести месяцев до одного года, либо арестом на срок до трех месяцев.

2. То же деяние, повлекшее по неосторожности смерть человека или иные тяжкие последствия, наказывается лишением свободы на срок до пяти лет.

Общество с ограниченной ответственностью «Дента-Л»
ООО «Дента-Л»

ПРИКАЗ

«09» января 2017 г. №25

г. Ставрополь

об утверждении документов
по информационной безопасности
в сфере использования сети
Интернет

Во исполнение требований Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить Регламент доступа и использования сотрудниками ресурсов сети Интернет, Регламент использования электронной почты, Памятку по работе с корпоративной электронной почтой согласно приложениям.
2. Ответственному за организацию работы по обработке и защите персональных данных – заместителю генерального директора по медицинской части Савченко Ю. А. ознакомить под роспись работников с настоящим приказом.
3. Контроль за исполнением настоящего приказа оставляю за собой.
4. Приказ вступает в силу со дня его подписания.

Руководитель организации **Генеральный директор** _____ **А. И. Латиган**
(должность) (личная подпись) (расшифровка подписи)

С приказом (распоряжением) работник ознакомлен _____ 09 01 2017 г.
(личная подпись)

Приложение № 1
к приказу от
«09» января 2017

УТВЕРЖДАЮ:
Генеральный директор
ООО «Дента-Л»

А. И. Латиган

«09» января 2017 г.

РЕГЛАМЕНТ

использования электронной почты

1. Общие положения

Настоящий Регламент разработан в целях установления единого порядка использования корпоративной электронной почты (далее - ЭП), обязательной для использования в работе всеми работниками.

Настоящий Регламент призван обеспечить бесперебойную работу и эффективное использование ЭП в интересах деятельности учреждения.

Настоящий Регламент не определяет порядок работы с документами, направляемыми и получаемыми по ЭП.

Каждый работник, имеющий личный почтовый ящик корпоративной ЭП, обязан использовать его в рамках выполнения своих трудовых обязанностей.

Вся информация и сообщения, которые были созданы, отправлены, приняты или сохранены посредством корпоративной ЭП, принадлежит учреждению, за исключением случаев, предусмотренных законодательством Российской Федерации.

В пределах функционирования корпоративной ЭП обеспечивается конфиденциальность почтовых сообщений и информации о пользователях ЭП, кроме информации из адресной книги и за исключением случаев, предусмотренных законодательством Российской Федерации.

2. Характеристика корпоративной электронной почты

Корпоративная ЭП состоит из следующих компонентов:

- Адресная книга, содержащая информацию о пользователях. Информация Адресной книги доступна всем зарегистрированным пользователям.
- Личные папки - локальные дисковые хранилища почтовых сообщений пользователя, необходимые для хранения большого объема сообщений и их архивирования.

Личные папки могут быть созданы как локально, на рабочем месте пользователя, так и на любом доступном внешнем хранилище. Личные папки используются в следующих целях:

- поддержание размера почтового ящика пользователя, располагающегося на сервере, в пределах обозначенных ему лимитов;
- организация структурированного хранилища путем создания вложенных папок;
- проведение операции архивирования почтовых сообщений, старше заданного срока отправки или получения;
- организация резервного хранилища на выделенном внешнем носителе или сервере.

- Почтовый ящик, содержащий почтовые сообщения пользователей корпоративной ЭП.

Содержимое почтовых ящиков пользователей может храниться следующими способами:

- в почтовом ящике на сервере;
- в личной папке локально на персональном компьютере пользователя;
- в архивных папках, локально на персональном компьютере пользователя;
- в общих папках, специально организованных для работы группы пользователей.

- Листы рассылок.

Список адресов доступен каждому пользователю и включает всех пользователей

- Адресная книга Пользователя – группа, созданная конкретным пользователем для структуризации своих рассылок. Такие группы недоступны для других пользователей.
- Антивирус - автоматическая система сканирования почтовых сообщений на наличие вредоносного вирусного кода (вирусов).

При обнаружении нежелательного содержания в сообщении системой антивируса вставляется сообщение с описанием причины изъятия зараженного содержания сообщения.

- Антиспам - автоматическая система сканирования почтовых сообщений на наличие нежелательной рекламной рассылки (спам).

В ЭП настроена подсистема обнаружения нежелательной почты.

3. Обеспечение контроля почтовых ящиков

Контроль почтовых ящиков в корпоративной ЭП должен в автоматическом режиме обеспечивать выполнение следующих действий:

- направление сообщения при приближении к установленному лимиту размера личного почтового ящика;
- автоматическое блокирование возможности отправки почтовых сообщений при превышении установленных лимитов размеров личных почтовых ящиков;

- ограничение до 100 получателей в одном сообщении для всех пользователей;
- отправление уведомлений о превышении лимита размера личного почтового ящика.

Превышение лимита размера личного почтового ящика автоматически блокируется возможность отправлять сообщения, при этом входящие сообщения продолжают приходить на личный почтовый ящик. В случае превышения лимита размера личного почтового ящика система автоматически направляет информационное сообщение о необходимости чистки личного почтового ящика. После уменьшения пользователем размера личного почтового ящика до установленного лимита (перемещением электронной почты в личную папку, общую папку или удалением), предусмотрено автоматическое восстановление заблокированных возможностей.

Каждый пользователь несет персональную ответственность за соблюдение установленного размера личного почтового ящика, а также своевременное архивирование или удаление информации.

4. Удаление личных почтовых ящиков

Удаление личных почтовых ящиков уволенных работников производится на основании данных об увольнении работника. Процедура удаления предполагает блокировку личного почтового ящика на 1 месяц и безвозвратное удаление по окончании данного срока.

5. Ограничения использования корпоративной электронной почты

При пользовании корпоративной ЭП пользователи обязаны соблюдать следующие правила:

- соблюдать общепринятые нормы и правила обмена почтовыми сообщениями;
- строго следовать ограничениям в рассылке сведений, содержащих персональные данные и иную конфиденциальную информацию, по которым установлен особый режим доступа и использования в соответствии с законодательством Российской Федерации, локальными нормативными актами;
- перед отправлением сообщения проверять правописание, грамматику и перечитывать сообщение;
- не рассылать сообщения противозаконного или неэтичного содержания, а также содержащие угрозы в адрес других пользователей;
- запрещается осуществлять рассылку сообщений рекламного или поздравительного характера;
- неукоснительно соблюдать положения настоящего Регламента.

Информации должна рассылаться только тем адресатам, которым она действительно необходима для выполнения служебных функций.

Все пользователи в обязательном порядке знакомятся с настоящим Регламентом и Памяткой по работе с корпоративной электронной почтой, обеспечивая в работе выполнение требований указанных документов.

Приложение № 2
к приказу от
«09» января 2017

УТВЕРЖДАЮ:
Генеральный директор
ООО «Дента-Л»

А. И. Латиган

«09» января 2017 г.

РЕГЛАМЕНТ

доступа и использования сотрудниками ресурсов сети Интернет

1. Общие положения

1.1. Настоящий Регламент разработан для повышения эффективности работы сотрудников ООО «Дента-Л», использующих электронные информационные ресурсы глобальной сети Интернет, и повышения уровня информационной безопасности локальной информационно-вычислительной сети.
1.2. Генеральный директор устанавливает постоянный контроль за доступом работников к сети Интернет. В случае нарушения сотрудником регламента, работник будет отстранен от использования ресурсов сети Интернет.

2. Назначение доступа к ресурсам сети Интернет

2.1. Доступ к ресурсам сети Интернет предоставляется сотрудникам для выполнениями ими прямых должностных обязанностей.
2.2. Глобальная информационная сеть Интернет используется для:

доступа к мировой системе гипертекстовых страниц (www), доступа к файловым ресурсам Интернета (FTR), доступа к специализированным (правовым и др.) базам данных;

контактов с официальными лицами правительственных структур, подрядчиками, обслуживающими организациями;

обмена электронной почтой с официальными лицами по неконфиденциальным вопросам производственного характера;

повышения квалификации работников, необходимой для выполнения работником своих должностных обязанностей;

поиска и сбора информации по производственным вопросам, если эти вопросы напрямую связаны с выполнением работником должностных обязанностей;

других целей.

3. Доступ к Интернет-ресурсам

3.1. ООО «Дента-Л» обеспечивает доступ пользователей локальной сети к ресурсам сети Интернет по специальным каналам связи в соответствии с настоящим Регламентом.

4. Ограничения при работе в сети Интернет

4.1. Пользователям корпоративной линии подключения к ресурсам глобальной сети Интернет не рекомендуется: посещение и использование игровых, развлекательных и прочих сайтов, не имеющих отношения к деятельности учреждения и деятельности пользователя;
использование электронной почты, досок объявлений, конференций на компьютерах в личных целях в любое время;
публикация корпоративного электронного адреса на досках объявлений, в конференциях и гостевых книгах;
использование некорпоративных e-mail адресов для рассылки служебной информации;
передача учетных данных пользователя;
применение имен пользователей и паролей компьютеров на иных (сторонних) компьютерах;
играть в рабочее время в компьютерные игры автономно или в сети;
единовременное скачивание больших объемов информации;
посещение ресурсов трансляции потокового видео и аудио (веб-камеры, трансляция ТВ - и музыкальных программ в Интернете), создающих большую загрузку сети и мешающих нормальной работе остальных пользователей;
подключение к электронной сети под другим паролем;
создание личных веб-страниц и хостинг (размещение web- или ftp-сервера) на компьютере пользователя.

4.2. Пользователям корпоративной линии подключения к ресурсам глобальной сети Интернет запрещается:
посещение и использование эротико-порнографических ресурсов сети Интернет, ресурсов националистических организаций, ресурсов, пропагандирующих насилие и терроризм;
нарушение закона об авторском праве посредством копирования и использования в служебных или личных целях материалов, защищенных законом об авторском праве;
осуществление деструктивных действий по отношению к нормальной работе электронной системы Предприятия и сети Интернет (рассылка вирусов, ip-атаки и т.п.);
загрузка материалов порнографического содержания, компьютерных игр, анекдотов, других развлекательных материалов;

передача персональных данных, конфиденциальной информации, сведений, составляющих служебную и коммерческую тайну, третьей стороне;
проведение незаконных операций в глобальной сети Интернет;
совершение иных действий, противоречащих законодательству, а также настоящему Регламенту.

5. Обращение в другие организации от имени ООО «Дента-Л»

5.1. Работа в сети Интернет, общение с другими организациями могут быть связаны с необходимостью изложения своих взглядов по отдельным вопросам. Если сотрудник ООО «Дента-Л» высказывает в сообщении собственное мнение, то указанный сотрудник обязан предупредить об этом в конце сообщения фразой: «Прошу считать, что в сообщении указано мое личное мнение, которое необязательно отражает взгляды и политику ООО «Дента-Л» – по предварительному согласованию с непосредственным руководством.
5.2. Официальные обращения по электронной почте к должностным лицам организаций-партнеров и организаций-заказчиков продукции и услуг осуществляются по указанию генерального директора, заместителя генерального директора по медицинской части.

6. Время работы пользователей в сети Интернет

6.1. Время работы пользователей в сети Интернет регламентировано следующим образом: с понедельника по пятницу, с 09.00 до 20.00, в субботу с 9.00 до 16.00; при необходимости работы с ресурсами сети Интернет в выходные дни или в вечернее время пользователь обязан получить разрешение у генерального директора.

7. Контроль использования ресурсов сети Интернет

7.1. Администрация ООО «Дента-Л» оставляет за собой право в целях обеспечения безопасности электронной системы производить выборочные и полные проверки всей электронной системы и отдельных файлов без предварительного уведомления работников.
7.2. После утверждения настоящего Регламента все пользователи ООО «Дента-Л» под личную роспись знакомятся с Регламентом.

Приложение № 3
к приказу от
«09» января 2017

УТВЕРЖДАЮ:
Генеральный директор
ООО «Дента-Л»

А. И. Латиган

«09» января 2017 г.

ПАМЯТКА

по работе с корпоративной электронной почтой

Политика использования электронной почты является важнейшим элементом корпоративной политики информационной безопасности ООО «Дента-Л».

Корпоративная электронная почта может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещается.

Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

При работе с корпоративной системой электронной почты сотрудникам запрещается:

распространять информацию ограниченного доступа, предназначенную для служебного использования, в том числе сведения, составляющие персональные данные и иную конфиденциальную информацию,

распространять материалы, защищаемые авторскими правами, использовать адрес корпоративной почты для оформления подписок,

публиковать свой адрес либо адреса сотрудников на общедоступных Интернет-ресурсах (форумы, конференции) за исключением случаев служебной необходимости,

осуществлять массовую рассылку почтовых сообщений рекламного характера,

рассылать через электронную почту материалы, содержащие вирусы и другие вредоносные продукты или программы, предназначенные для нарушения, уничтожения, либо ограничения функциональности любого

компьютерного или телекоммуникационного оборудования или программ для осуществления несанкционированного доступа,

распространять угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, запрещенную российским законодательством,

предоставлять иным лицам пароль доступа к своему почтовому ящику.