



## **Положение о регламенте использования ресурсов сети Интернет в информационной сети ГАУЗ СО «Стоматологическая поликлиника город Нижний Тагил»**

Разработано на основании Федерального закона №149 от 27.07.2000г.  
«Об информации, информационных технологиях и о защите информации».

### **СТРУКТУРА ПОЛОЖЕНИЯ:**

1. Общие положения.
2. Требования к пользователю.
3. Требования к администратору-программисту.
4. Порядок предоставления сотрудникам доступа к сети Интернет.
  - 4.1 Ограничения доступа.
  - 4.2 Регламент использования ресурсов глобальной сети «Интернет».
  - 4.3 Порядок разрешения споров.

Приложение №1. Памятка по работе с корпоративной электронной почтой.

Приложение №2. Памятка по работе в глобальной сети Интернет.

### **1. Общие положения.**

1.1 Положение предназначено для сотрудников ГАУЗ СО «СП г. Нижний Тагил», выполнение должностных обязанностей которых связано с использованием персональных компьютеров, и определяет их полномочия, обязанности и ответственность при использовании информационных ресурсов глобальной компьютерной сети Интернет.

1.2 Положение является обязательным для выполнения всеми сотрудниками - пользователями Информационной сети ГАУЗ СО «СП г. Нижний Тагил» в части, касающейся их.

1.3 В тексте Положения используются следующие сокращения и основные понятия:

- ПК - персональный компьютер;
- ИВС – информационно-вычислительная сеть;
- пользователь – сотрудник ГАУЗ СО «СП г. Нижний Тагил», выполнение должностных обязанностей которого связано с использованием ПК в ИВС ГАУЗ СО «СП г. Нижний Тагил»;
- IT служба – информационно-техническая служба ГАУЗ СО «СП г. Нижний Тагил», состоящая из администраторов-программистов, техников и операторов.
- информационные ресурсы - отдельные документы и отдельные массивы документов, базы данных, другие виды информационного обеспечения в ИВС с использованием ПК;
- ВСЭС ЗСО – ведомственная система электронных сообщений здравоохранения Свердловской области в защищенной сети РФ ЕГИСЗ для подведомственных учреждений Министерства здравоохранения Свердловской области (Приказ МЗ СО №1961-п от 02.12.2015 г.).
- администратор – сотрудник IT службы, ответственный за подключение к

глобальной сети Интернет и обеспечение работоспособности, надежности сети, сохранности и защиты информационных ресурсов;

- трафик - объем информации, полученной или отправленной пользователем при работе с глобальной компьютерной сетью Интернет;

- контент – Информационное содержание сайта (тексты, графическая, звуковая информация и др.), а также книги, газеты, сборника статей, материалов и др.;

- развлекательные сайты – сайты, предлагающие разный развлекательный контент; порталы досуга, популярных ресурсы развлечений;

- сайты знакомств – интернет-сервис, предоставляющий пользователям Интернета услуги по виртуальному общению с другими пользователями, аналог реальных служб знакомств.

- игровые сайты – сайты для различных игр;

- порнографические сайты (порносайты) - интернет-сайт, цель которого — платное или бесплатное распространение порнографии;

- прочие сайты – сайты, которые не относятся к направлению деятельности сотрудника;

- Чат (Chat) - средство обмена сообщениями по компьютерной сети в режиме реального времени, а также программное обеспечение, позволяющее организовывать такое общение.

- Firewall - (фаервол, брандмауэр) – 'то интегрированное в операционные системы антивирусное обеспечение, защищающее компьютер от несанкционированных проникновений по всевозможным видам сетей.

- съемные носители информации - некоторые типы запоминающих устройств, оформленные, как компактные, носимые человеком, приспособленные для переноса информации.

1.4 Руководители структурных подразделений, пользователи и администраторы обязаны знать и выполнять нормативные правовые акты, затрагивающие вопросы информатизации, защиты информации и информационной безопасности в части соблюдения требований и ограничений по использованию информационных ресурсов.

1.5 Руководители структурных подразделений в обязательном порядке организуют ознакомление пользователей с нормативными правовыми актами, указанными в настоящем Положении.

1.6 Доступ к глобальной компьютерной сети Интернет осуществляется с рабочего ПК пользователя. Ответственность за действия на компьютере другого человека, несет пользователь ПК, с которого совершено это действие.

1.7 Работа пользователей в глобальной компьютерной сети Интернет отслеживается с помощью специального программного или аппаратного обеспечения – шлюзов безопасности, межсетевых экранов. На основе логов проводится анализ по следующим параметрам:

- перечень используемых ресурсов;

- объем трафика и его цена, по тарифам провайдера.

1.8 Настоящее Положение может уточняться и дополняться в установленном порядке.

## **2. Требования к пользователю.**

2.1 Данный раздел отражает полномочия, обязанности и ограничения прав пользователей глобальной компьютерной сети Интернет.

2.2 Пользователю **запрещается**:

- загружать, самостоятельно устанавливать прикладное, операционное, сетевое и другие виды программного обеспечения, а также осуществлять обновления, если эта работа не входит в его должностные обязанности;
- использовать ресурсы Интернет в не служебных целях;
- допускать к работе посторонних лиц;
- строго запрещается подключаться к ресурсам Интернет, используя ПК Компании, через не служебный канал доступа – сотовый телефон, модем, и др. устройства.

2.3 Пользователь обязан знать и уметь пользоваться антивирусным программным обеспечением. При обнаружении вируса он должен сообщить об этом администратору. Пользователю запрещается производить какие-либо действия с информацией, зараженной вирусом.

2.4 Пользователь обязан информировать администратора- программиста о любых нарушениях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе ИВС.

2.5 Пользователь имеет право оспаривать решение администратора –программиста через своего непосредственного руководителя, который в свою очередь обращается в ИТ службу. Если обе стороны не могут прийти к консенсусу, тогда вопрос рассматривает заместитель главного врача по медицинской части.

### **3. Требования к администратору-программисту.**

3.1 Данный раздел отражает функциональные полномочия и обязанности администратора- программиста обеспечивающего доступ к глобальной компьютерной сети Интернет.

3.2 Администратор- программист **обязан**:

- производить подключение к сети Интернет только через специализированное устройство (Firewall) для обеспечения защиты информационной сети.
- знать и правильно использовать аппаратно - программные средства защиты информации и обеспечивать сохранность информационных ресурсов с помощью этих средств;
- оказывать методическую и консультационную помощь пользователям по вопросам, входящим в его компетенцию;
- ежемесячно вести учет и анализ использования ресурсов сети Интернет по каждому пользователю, предоставлять этот отчет руководству;
- информировать руководителей структурных подразделений о любых нарушениях требований настоящего Положения и других негативных ситуациях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети.

3.3 Администратор – программист имеет право:

- при обнаружении доступа к развлекательным сайтам, запретить доступ к сайту.
- при обнаружении использования пользователем программных продуктов, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети, запретить доступ к сети Интернет.

### **4. Порядок предоставления сотрудникам доступа к сети Интернет.**

Система контроля Интернет-доступа в компании предусматривает следующие автоматические ограничения:

1. Запрет входа на определенные сайты;
2. Запрет определенных Интернет-протоколов и портов;

3. Антивирусную проверку Интернет-трафика, с автоматическим отказом принимать вирусный файл.
4. Запрет скачивания определенных типов файлов.
5. Ограничение на использование съемных носителей информации.
6. Автоматическое отключение пользователя и/или групп пользователей от платных ресурсов, при достижении ими ежедневного, еженедельного или ежемесячного лимита.

Кроме того, система контроля Интернет-доступа осуществляет сбор статистики использования Интернета пользователем. Настоящая статистика доступна программисту, главному врачу, заместителю главного врача по медицинской части, начальнику отдела кадров, юрисконсульту и может служить причиной отключения определенных ресурсов, и принятия решений об изменении прав доступа пользователя к Интернету.

#### **4.1 Ограничения доступа.**

Определяются следующие возможные ограничения доступа к Интернету для пользователей:

1. Доступ в Интернет – доступ к сети Интернет с рабочего места.
  2. Ограничения (внешняя электронная почта) – доступ к сайтам предоставляющим услуги электронной почты (mail.ru, mail.yandex.ru, mail.e1.ru и др.)
  3. Ограничения (интернет-пейджеры) – доступ к icq, mail.ru-агенту и др. интернет-пейджерам
  4. Ограничения (порнография, развлечения, баннеры) – ограничения по спискам соответствующих сайтов.
  5. Ограничения (соц. сети) – ограничения по спискам соответствующих сайтов (odnoklassniki.ru, vkontakte.ru и т.д.).
  6. Ограничения (поиск работы) – сайты объявлений о вакансиях и резюме.
- Прочие ограничения – ограничения доступа по списку (фильтру), обусловленные трудовой дисциплиной.

#### **4.2 Регламент предоставления доступа.**

Доступ к Интернету пользователю предоставляется исходя из служебной необходимости, после определения необходимых ограничений доступа (см. пункт 4.1 регламента) с помощью служебной записки на имя непосредственного руководителя, одобренной главным врачом Учреждения.

Изменение прав доступа и различных ограничений, а также ручное включение пользователя после автоматического отключения (после превышения дневного лимита) производится также после служебной записки (или объяснительной) на имя непосредственного руководителя одобренной главным врачом Учреждения.

#### **4.3 Порядок разрешения споров.**

В случае возникновения претензий или вопросов касающихся конкретного запрещенного сайта, типа файла, невозможности продолжения работы в сети Интернет, пользователь обращается к программисту. Если претензию не удастся разрешить двум сторонам - тогда вопрос рассматривает заместитель главного врача.

## **Регламент использования ресурсов глобальной сети Интернет.**

Настоящий Регламент разработан для повышения эффективности работы сотрудников Учреждения, использующих электронные информационные ресурсы глобальной сети Интернет, и повышения уровня информационной безопасности локальной информационно-вычислительной сети ГАУЗ СО «СП г. Нижний Тагил».

В ГАУЗ СО «СП г. Нижний Тагил» устанавливается контроль, и специфицируются виды информации, к которой разрешается доступ сотрудников. В случае нарушения сотрудником Учреждения данного Регламента он отстраняется от использования ресурсов сети Интернет.

### **1. Назначение доступа к ресурсам сети Интернет.**

Доступ к ресурсам сети Интернет предоставляется сотрудникам ГАУЗ СО «СП г. Нижний Тагил» для выполнения ими прямых должностных обязанностей.

Глобальная сеть Интернет используется для:

доступа к всемирной паутине гипертекстовых страниц (WWW) ;

доступа к файловым ресурсам Интернета (FTP);

доступа к специализированным (правовым и др.) базам данных;

контактов с официальными лицами других правительственных структур, с сотрудниками структурных подразделений Учреждения и работниками отраслевых предприятий; производителями и потребителями товаров и услуг в области медицины;

обмена электронной почтой с официальными лицами по не конфиденциальным вопросам производственного характера;

сбора информации о состоянии рынка продукции и услуг, используемых в медицине; повышения квалификации работников, необходимой для выполнения работником своих должностных обязанностей; поиска и сбора информации по управленческим, производственным, финансовым, юридическим вопросам, если эти вопросы напрямую связаны с выполнением работником его должностных обязанностей, и др.

### **2. Доступ к Интернет-ресурсам.**

Учреждение обеспечивает доступ пользователей локальной сети к ресурсам Интернет по специальным (в том числе защищенным) каналам связи в соответствии с установленными в Учреждении правилами и настоящим Регламентом.

Открытие и контроль доступа регулируется IT-службой под руководством администрации Учреждения, а так же Приказами, Постановлениями и пр. документами Правительства Свердловской области и Министерства здравоохранения Свердловской области.

Самостоятельная организация дополнительных точек доступа в глобальную сеть Интернет (удаленный доступ, канал по локальной сети и пр.) запрещена.

### **3. Регистрация пользователя.**

Каждому физически подключенному к сети компьютеру назначается ответственный за этот компьютер пользователь, информация о котором заносится в базу данных пользователей соответствующего домена локальной сети Учреждения.

Регистрация выполняется программистом Учреждения.

Пользователь обязан хранить свои идентификационные данные (пароли, ID и т.п.) в тайне. Запрещена передача идентификационных данных третьим лицам.

За все деструктивные действия, произведенные в сети, отвечает сотрудник - пользователь учетной записи (идентификационных данных), использовавшейся при их проведении.

При подозрении на то, что идентификационные данные стали известны третьим лицам, пользователь должен немедленно обратиться к программисту с целью их изменения.

### **4. Основные ограничения при работе в сети Интернет.**

Ограничен доступ пользователей локальной ИВС Учреждения к сервисам ИАС ТФОМС согласно приказу «Об утверждении списка лиц, и списка персональных компьютеров допущенных к работе в ИАС ТФОМС» от 01.10.2015г., а также ко всем почтовым серверам, в том числе и бесплатным почтовым службам, кроме ВЭС ЗСО (Приказ МЗ СО №1961-п «Об организации процесса получения и обработки информации посредством Ведомственной системы электронных сообщений от исполнительных органов государственной власти Свердловской области в сфере здравоохранения» от 02.12.2015г.) и корпоративного сервера. В случае если пользователю в служебных целях необходимо завести почтовый ящик в домене, отличном от \*\*\*\*@stpol.ru или \*\*\*\*@mis66.ru, необходимо письменное разрешение вышестоящего руководителя пользователя, согласованное с IT службой.

#### **Запрещается:**

использование некорпоративной (личной) электронной почты, досок объявлений, конференций на компьютерах Учреждения в личных целях в любое время;

публикация корпоративных электронных адресов типа \*\*\*\*@stpol.ru или \*\*\*\*@mis66.ru на досках объявлений, в конференциях и гостевых книгах.

посещение пользователем ресурсов с непристойным содержанием (эротико-порнографические ресурсы, нацистские или националистические ресурсы, ресурсы, призывающие к насилию, экстремизму); посещение игровых, развлекательных и прочих сайтов, не имеющих отношения к деятельности медицинского Учреждения и должностным обязанностям пользователя;

передача кому бы то ни было учетных данных пользователя;

применение имен пользователей и паролей компьютеров Учреждения на иных (сторонних) компьютерах;

игры на компьютере автономно и в сети;

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; загрузка материалов порнографического содержания, компьютерных игр, анекдотов, других развлекательных материалов;

передача конфиденциальной информации третьей стороне;  
подключение к электронной сети под другим логином и паролем;  
нанесение вреда электронной системе Учреждения, саботирование, физическое отключение любым способом от ИВС;  
проведение незаконных операций и других незаконных действий в глобальной сети Интернет;  
создание личных веб-страниц и хостинг (размещение web- или ftp-сервера, создание виртуальных серверов) на компьютере пользователя;  
любые попытки деструктивных действий по отношению к нормальной работе электронной системы Учреждения и сети Интернет (рассылка вирусов, ip-атаки и т.п.);  
нарушение закона об авторском праве: копирование и использование материалов и программ, защищенных законом об авторском праве;  
совершение действий, противоречащих законодательству, а также настоящему Регламенту.

### **5. Соблюдение субординации.**

Работа в сети Интернет, общение с другими организациями может быть связана с необходимостью изложения своих взглядов по отдельным вопросам. Если сотрудник Учреждения высказывает в сообщении собственное мнение, то он, по предварительному согласованию с непосредственным руководством, обязан предупредить об этом в конце сообщения фразой: "прошу считать, что в сообщении указано мое личное мнение, которое необязательно отражает взгляды и политику Администрации Учреждения".

Обращение по электронной почте в подведомственные организации осуществляется по согласованию с главным врачом (заместителем) учреждения или заведующим отделением.

### **6. Контроль использования ресурсов сети Интернет.**

Руководство ГАУЗ СО «СП г. Нижний Тагил» оставляет за собой право в целях обеспечения безопасности электронной системы производить выборочные и полные проверки всей электронной системы или ее сегментов, а так же отдельных файлов без предварительного уведомления работников.

Информационная служба Учреждения ведет учет использования ресурсов Интернет, обеспечивает контроль за соблюдением настоящего Регламента, обеспечивает безопасное использование ресурсов сети.

Администрация Учреждения оставляет за собой право, в порядке надзора за исполнением настоящего Положения, просматривать любые данные пользователя, включая переписку.

После утверждения настоящего Регламента все пользователи Учреждения под личную роспись знакомятся с Регламентом и его Приложениями.

**Приложение №1  
к Регламенту использования ресурсов  
глобальной сети Интернет  
в ГАУЗ СО «СП г. Нижний Тагил».**

**Памятка по работе с корпоративной электронной почтой.**

Политика использования электронной почты является важнейшим элементом общекорпоративной политики информационной безопасности Учреждения и неотделима от нее.

Электронная почта является собственностью ГАУЗ СО «СП г. Нижний Тагил» и может быть использована ТОЛЬКО в служебных целях. Использование электронной почты в других целях категорически запрещено.

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 Учреждения **запрещается:**

использовать адрес корпоративной почты для оформления подписок;  
публиковать свой адрес, либо адреса других сотрудников Учреждения на общедоступных Интернет-ресурсах (форумы, конференции и т.п.) за исключением случаев служебной необходимости;  
осуществлять массовую рассылку почтовых сообщений рекламного характера;  
рассылать через электронную почту материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также ссылки на вышеуказанную информацию;  
распространять защищаемые авторскими правами материалы, затрагивающие какой-либо патент, торговую марку, коммерческую тайну, врачебную тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;  
распространять информацию, содержание и направленность которой запрещены международным и российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.;  
распространять информацию ограниченного доступа, предназначенную для служебного использования;  
предоставлять кому бы то ни было пароль доступа к своему почтовому ящику.  
С настоящей памяткой ознакомлен (а)

\_\_\_\_\_ (\_\_\_\_\_)

(подпись) (Ф.И.О.)

" \_\_\_\_ " \_\_\_\_\_ 200\_\_ г.



**Приложение №2  
к Регламенту использования  
ресурсов глобальной сети  
Интернет в ГАУЗ СО «СП г. Нижний Тагил»**

### **Памятка по работе в глобальной сети Интернет.**

Настоящий документ описывает общепринятые нормы работы в сети Интернет, соблюдение которых является обязательным для всех пользователей. Действие этих норм распространяется на использование ресурсов Сети. Здесь и далее словом Сеть обозначены сеть Интернет и доступные из нее другие сети.

#### **Являются недопустимыми:**

- массовая рассылка не согласованных предварительно электронных писем (mass mailing). Под массовой рассылкой подразумевается, как рассылка множеству получателей, так и множественная рассылка одному получателю. Здесь и далее под электронными письмами понимаются сообщения электронной почты, ICQ и других подобных средств личного обмена информацией;
- несогласованная рассылка электронных писем рекламного, коммерческого или агитационного характера, а также писем, содержащих грубые и оскорбительные выражения и предложения;
- размещение в любой конференции Usenet или другой конференции, форуме или электронном списке рассылки статей, которые не соответствуют тематике данной конференции или списку рассылки (off-topic). Здесь и далее под конференцией понимаются телеконференции (группы новостей) Usenet и другие конференции, форумы и электронные списки рассылки;
- размещение в любой конференции сообщений рекламного, коммерческого или агитационного характера, кроме случаев, когда такие сообщения явно разрешены правилами такой конференции либо их размещение было согласовано с владельцами или администраторами такой конференции предварительно;
- размещение в любой конференции статьи, содержащей приложенные файлы, кроме случаев, когда вложения явно разрешены правилами такой конференции либо такое размещение было согласовано с владельцами или администраторами такой конференции предварительно;
- рассылка информации получателям, высказавшим ранее явное нежелание получать эту информацию;
- использование собственных или предоставленных информационных ресурсов (почтовых ящиков, адресов электронной почты, страниц WWW и т.д.) в качестве контактных координат при совершении любого из вышеописанных действий, вне зависимости от того, из какой точки Сети были совершены эти действия;
- запрет несанкционированного доступа и сетевых атак. Не допускается осуществление попыток несанкционированного доступа к ресурсам Сети, проведение или участие в сетевых атаках и сетевом взломе, за исключением случаев, когда атака на сетевой ресурс проводится с явного разрешения владельца или администратора этого ресурса.

#### **В том числе запрещены:**

- действия, направленные на нарушение нормального функционирования элементов Сети (компьютеров, другого оборудования или программного

обеспечения), не принадлежащих пользователю;

- действия, направленные на получение несанкционированного доступа, в том числе привилегированного, к ресурсу Сети (компьютеру, другому оборудованию или информационному ресурсу), последующее использование такого доступа, а также уничтожение или модификация программного обеспечения или данных, не принадлежащих пользователю, без согласования с владельцами этого программного обеспечения или данных либо администраторами данного информационного ресурса;
- передача компьютерам или оборудованию Сети бессмысленной или бесполезной информации, создающей паразитную нагрузку на эти компьютеры или оборудование, а также промежуточные участки Сети, в объемах, превышающих минимально необходимые для проверки связности сетей и доступности отдельных ее элементов.

### **Соблюдение правил, установленных владельцами ресурсов.**

Владелец любого информационного или технического ресурса Сети может установить для этого ресурса собственные правила его использования. Правила использования ресурсов либо ссылка на них публикуются владельцами или администраторами этих ресурсов в точке подключения к таким ресурсам и являются обязательными к исполнению всеми пользователями этих ресурсов. Пользователь обязан соблюдать правила использования ресурса либо немедленно отказаться от его использования.

### **Недопустимость фальсификации.**

Значительная часть ресурсов Сети не требует идентификации пользователя и допускает анонимное использование. Однако в ряде случаев от пользователя требуется предоставить информацию, идентифицирующую его, и используемые им средства доступа к Сети.

### **При этом пользователю запрещается:**

- использование идентификационных данных (имен, адресов, телефонов и т.п.) третьих лиц, кроме случаев, когда эти лица уполномочили пользователя на такое использование. В то же время пользователь должен принять меры по предотвращению использования ресурсов Сети третьими лицами от его имени (обеспечить сохранность паролей и прочих кодов авторизованного доступа);
- фальсификация своего IP-адреса, а также адресов, используемых в других сетевых протоколах, при передаче данных в Сеть;
- использование несуществующих обратных адресов при отправке электронных писем.
- настройка собственных ресурсов.

При работе в Сети Интернет пользователь становится ее полноправным участником, что создает потенциальную возможность для использования сетевых ресурсов, принадлежащих пользователю, третьими лицами. В связи с этим пользователь должен принять надлежащие меры по такой настройке своих ресурсов, которая препятствовала бы недобросовестному использованию этих ресурсов третьими лицами, а также оперативно реагировать при обнаружении случаев такого использования. Примерами потенциально проблемной настройки сетевых ресурсов являются:

- открытый ретранслятор электронной почты (SMTP-relay) - отказ в приеме почты

от таких ретрансляторов регламентирован RFC 2505;

- общедоступные для неавторизованной публикации серверы новостей (конференций, групп);
- средства, позволяющие третьим лицам неавторизованно скрыть источник соединения (открытые прокси-серверы и т.п.);
- общедоступные широковещательные адреса локальных сетей;
- электронные списки рассылки с недостаточной авторизацией подписки или без возможности ее отмены.

Ответственность за все действия в Сети, произведенные под именем и с паролем пользователя им самим или другими физическими, или юридическими лицами и организациями, полностью лежит на самом пользователе. Администрация ГАУЗ СО «СП г. Нижний Тагил» не несет никакой юридической, материальной или иной ответственности за качество, содержание, законность и любое другое свойство полученной или переданной пользователем информации в нарушение настоящего Регламента.

Учреждение не несет никакой юридической, материальной и иной ответственности за использование пользователем платных услуг других организаций, предоставляющих услуги в Сети.

С настоящей памяткой ознакомлен (а)

\_\_\_\_\_ ( \_\_\_\_\_ )  
(подпись) (Ф.И.О.)

" \_\_\_\_ " \_\_\_\_\_ 2016\_ г.

---