Образовательная автономная некоммерческая организация высшего образования

«МОСКОВСКИЙ ТЕХНОЛОГИЧЕСКИЙ ИНСТИТУТ»

УТВЕРЖДЕНО
На заседании Ученого совета
ОАНО ВО «МосТех»
протокол № 06 от 28 февраля 2025 г.

УТВЕРЖДАЮ
Ректор
_____ Ю.В. Вепринцева
«28» февраля 2025 г.

ПОЛОЖЕНИЕ
О ЗАЩИТЕ ОБУЧАЮЩИХСЯ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ И(ИЛИ) РАЗВИТИЮ, ЗАПРЕЩЕННОЙ К РАСПРОСТРАНЕНИЮ В РОССИЙСКОЙ ФЕДЕРАЦИИ, А ТАКЖЕ НЕ СООТВЕТСТВУЮЩЕЙ ЗАДАЧАМ ОБРАЗОВАНИЯ

РЕКОМЕНДОВАНО
на заседании Студенческого совета
ОАНО ВО «МосТех»
протокол № 06
от 28 февраля 2025 г.

РЕКОМЕНДОВАНО
на заседании Совета родителей
ОАНО ВО «МосТех»
протокол № 06
от 28 февраля 2025 г

Москва 2025

1. Назначение и область применения

1.1 Настоящее Положение определяет порядок применения административных и организационных мер, технических и программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию, запрещенной к распространению на территории Российской Федерации, а также не соответствующей задачам образования (далее – Положение) в образовательной автономной некоммерческой организации высшего образования ОАНО ВО «МосТех» (далее – Институт).

1.2 Настоящее Положение является обязательным для исполнения всеми работниками Института и обучающимися.

2. Нормативные документы

Настоящее Положение разработано на основе:

– Федерального закона от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;

– Федерального закона от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности»;

– Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

– Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

– приказа Минкомсвязи России от 29.08.2012 № 217 «Об утверждении порядка проведения экспертизы информационной продукции в целях обеспечения информационной безопасности детей»;

– приказа Министерства связи и массовых коммуникаций Российской Федерации от 16.06.2014 161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию»;

– письма Минобрнауки России от 28.04.2014 № ДЛ-115/03 «О методических рекомендациях по ограничению в образовательных организациях доступа, обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования»;

–- письма Минпросвещения Российской Федерации от 07.06.2019 № 04-474 «О методических рекомендациях».

3. Термины и определения

В настоящем Положении используются следующие термины и определения:

– **дети** – лица, не достигшие возраста восемнадцати лет (совершеннолетия).

– **доступ детей к информации** – возможность получения и использования детьми свободно распространяемой информации;

– **знак информационной продукции** – графическое и (или) текстовое обозначение информационной продукции в соответствии с классификацией информационной продукции, предусмотренной частью 3 статьи 6 Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» (далее – Закон о защите детей от информации);

– **зрелищное мероприятие** (далее – мероприятие) – демонстрация информационной продукции в месте, доступном для детей, и в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи, в том числе посредством проведения театрально-зрелищных, культурно-просветительных и зрелищно-развлекательных мероприятий;

– **информационная безопасность обучающихся** – состояние защищенности обучающихся, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию;

– **информационная продукция** – предназначенные для оборота на территории Российской Федерации продукция средств массовой информации, печатная продукция, аудиовизуальная продукция на любых видах носителей, программы для электронных вычислительных машин (программы для ЭВМ) и базы данных, а также информация, распространяемая посредством зрелищных мероприятий, посредством информационно-телекоммуникационных сетей, в том числе сети «Интернет», и сетей подвижной радиотелефонной связи;

– **информационная продукция для детей** – информационная продукция, соответствующая по тематике, содержанию и художественному оформлению физическому, психическому, духовному и нравственному развитию детей;

– **информация порнографического характера** – информация, представляемая в виде натуралистических изображений или описания половых органов человека и (или) полового сношения либо сопоставимого с половым сношением действия сексуального характера, в том числе такого действия, совершаемого в отношении животного;

– **информация, нарушающая законодательство Российской Федерации**, – информация экстремистского характера, экстремистские материалы, включенные в федеральный список экстремистских материалов, а также иная информация, за

распространение которой предусмотрена административная или уголовная ответственность;

– **классификация информационной продукции** – распределение информационной продукции в зависимости от ее тематики, жанра, содержания и художественного оформления по возрастным категориям детей в порядке, установленном Законом о защите детей от информации;

– **маркировка** – нанесение условных знаков, букв, цифр, графических знаков или надписей на объект, с целью его дальнейшей идентификации (узнавания), указания его свойств и характеристик;

– **места, доступные для детей** – общественные места, доступ ребенка в которые и (или) нахождение ребенка в которых не запрещены, в том числе общественные места, в которых ребенок имеет доступ к продукции средств массовой информации и (или) размещаемой в информационно-телекоммуникационных сетях информационной продукции;

– **натуралистические изображение или описание** – изображение или описание в любой форме и с использованием любых средств человека, животного, отдельных частей тела человека и (или) животного, действия (бездействия), события, явления, их последствий с фиксированием внимания на деталях, анатомических подробностях и (или) физиологических процессах;

– **негативная информация** – виды информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования и воспитания;

– **оборот информационной продукции** – предоставление и (или) распространение информационной продукции, включая ее продажу (в том числе распространение по подписке), аренду, прокат, раздачу, выдачу из фондов общедоступных библиотек, публичный показ, публичное исполнение (в том числе посредством зрелищных мероприятий), распространение посредством эфирного или кабельного вещания, информационно-телекоммуникационных сетей, в том числе сети «Интернет», и сетей подвижной радиотелефонной связи;

– **ребенок (множ. дети)** – лицо, не достигшее возраста восемнадцати лет;

– **символика экстремистской организации** – символика, описание которой содержится в учредительных документах организации, в отношении которой по основаниям, предусмотренным Федеральным законом от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности», судом принято вступившее в законную силу решение о ликвидации или запрете деятельности в связи с осуществлением экстремистской деятельности;

– **экстремистская организация** – общественное или религиозное объединение

либо иная организация, в отношении которой по основаниям, предусмотренным Федеральным законом от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности», судом принято вступившее в законную силу решение о ликвидации или запрете деятельности в связи с осуществлением экстремисткой деятельности;

– **экстремистские материалы** – предназначенные для обнародования документы или информация на иных носителях, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности, в том числе труды руководителей национал-социалистической рабочей партии Германии, фашистской партии Италии, публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой-либо этнической, социальной, расовой, национальной или религиозной группы.

4. Общие положения

4.1. Целью настоящего Положения является обеспечение реализации задач, направленных на ограничение доступа детей к информации, причиняющей вред их здоровью и (или) развитию, запрещенной к распространению на территории Российской Федерации, а также не соответствующей задачам образования, в том числе распространяемой посредством информационно-телекоммуникационной сети «Интернет» (далее – также сети «Интернет»).

4.2. К информации, причиняющей вред здоровью и (или) развитию детей, относится информация:

– запрещенная для распространения среди детей;

– распространение которой среди детей определенных возрастных категорий ограничено.

4.3. Перечень видов информации в соответствии с указанными группами представлен в приложении 1.

4.4. К информации, распространение которой в Российской Федерации запрещено, относится информация экстремистского характера, экстремистские материалы, включенные в Федеральный список экстремистских материалов, пропаганда войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иная информация, за распространение которой предусмотрена уголовная или административная ответственность.

4.5. К экстремистской деятельности (экстремизму) относятся:

– насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации;

– публичное оправдание терроризма и иная террористическая деятельность;

возбуждение социальной, расовой, национальной или религиозной розни; пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;

– нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;

– воспрепятствование осуществлению гражданами их избирательных прав и права на участие в референдуме или нарушение тайны голосования, соединенные с насилием либо угрозой его применения;

– воспрепятствование законной деятельности государственных органов, органов местного самоуправления, избирательных комиссий, общественных и религиозных объединений или иных организаций, соединенное с насилием либо угрозой его применения;

– совершение преступлений по мотивам, указанным в пункте «е» части первой статьи 63 Уголовного кодекса Российской Федерации:

– пропаганда и публичное демонстрирование нацистской атрибутики или символики либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо публичное демонстрирование атрибутики или символики экстремистских организаций;

– публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения;

– публичное заведомо ложное обвинение лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, в совершении им в период исполнения своих должностных обязанностей деяний, указанных в настоящей статье и являющихся преступлением;

– организация и подготовка указанных деяний, а также подстрекательство к их осуществлению;

– финансирование указанных деяний либо иное содействие в их организации, подготовке и осуществлении, в том числе путем предоставления учебной, полиграфической и материально-технической базы, телефонной и иных видов связи или оказания информационных услуг.

Перечень видов информации, распространение которой запрещено в Российской Федерации представлен в приложении 2.

4.6. К информации, не соответствующей задачам образования, относится:

– информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет») по тематике компьютерных игр, не соответствующая задачам образования, такая как порталы браузерных игр, массовые многопользовательские онлайн ролевые игры (ММОРИ), массовые многопользовательские игры, основанные на имитации боевых или противоправных действий, советы для игроков и ключи для установки и прохождения игр, игровые форумы и чаты;

– анонимные форумы, чаты, доски объявлений и гостевые книги, такие как: имиджборды, анонимайзеры, программы, обеспечивающие анонимизацию сетевого трафика в сети «Интернет»;

– информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), представляющая собой банки готовых рефератов, эссе, дипломных работ, за исключением печатных и электронных образовательных и информационных ресурсов, создаваемых в организациях, осуществляющих образовательную деятельность;

– информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая информацию об электронных казино, тотализаторах, играх на деньги;

– сайты, навязывающие платные услуги на базе СМС-платежей, сайты, обманным путем собирающие личную информацию (фишинг);

– информационная продукция, оказывающая психологическое воздействие на детей, при которой человек обращается к тайным силам с целью влияния на события, а также реального или кажущегося воздействия на состояние.

5. Меры, направленные на обеспечение защиты детей от информации, причиняющей вред их здоровью и (или) развитию, запрещенной к распространению в Российской Федерации, а также не соответствующей задачам образования

5.1. Институт обеспечивает выполнение административных и организационных мер, использование технических и программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию, запрещенной к распространению в Российской Федерации, а также не соответствующей задачам образования.

5.2. К административным мерам защиты несовершеннолетних обучающихся от информации, причиняющей вред их здоровью и (или) развитию, запрещенной к распространению в Российской Федерации, а также не соответствующей задачам образования, относятся:

5.2.1. Принятие настоящего Положения и иных локальных нормативных актов

института, направленных на повышение осведомленности лиц, находящихся в месте оборота информационной продукции, запрещенной для детей, о необходимости обеспечения информационной безопасности детей и защиты детей от информации, причиняющей вред их здоровью и (или) развитию, определяющих в частности:

– процедуры присвоения и размещения знака информационной продукции и (или) текстового предупреждения об информационной продукции, запрещенной для детей;

– условия присутствия в соответствии с законодательством Российской Федерации детей на публичном показе, при публичном исполнении, демонстрации посредством зрелищного мероприятия информационной продукции, запрещенной для детей, в случае их организации и (или) проведения;

– дополнительные требования к обороту информационной продукции, запрещенной для детей, и ее фрагментов, распространяемых посредством эфирного и кабельного, теле- и радиовещания, сети «Интернет» и сетей подвижной радиотелефонной связи, в местах, доступных для детей;

– меры защиты детей от информации, причиняющей вред их здоровью и (или) развитию, направленные на повышение осведомленности лиц, находящихся в месте оборота информационной продукции, запрещенной для детей, о необходимости обеспечения информационной безопасности детей и защиты детей от информации, причиняющей вред их здоровью и (или) развитию, нарушающей законодательство Российской Федерации, а также не соответствующей задачам образования;

– процедуры, направленные на предотвращение, выявление и устранение нарушений законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию.

5.2.2. Ознакомление работников Института, в трудовые обязанности которых входит организация и осуществление оборота информационной продукции для детей, работа с официальным сайтом Института в сети «Интернет», с положениями законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, а также не соответствующей задачам образования, настоящим Положением и иными локальными нормативными актами, регулирующими защиту детей от информации, причиняющей вред их здоровью и (или) развитию, запрещенной к распространению в Российской Федерации, а также не соответствующей задачам образования.

Обязанность по ознакомлению с вышеуказанными актами возлагается на руководителей структурных подразделений, в чьем подчинении находятся указанные работники.

5.2.3. Назначение работника, ответственного за обеспечение безопасного доступа и

использование сети «Интернет» в Институте в научно-образовательных целях, применение административных и организационных мер, технических и программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию, запрещенной к распространению в Российской Федерации, а также не соответствующей задачам образования, учитывающих специфику оборота информационной продукции, запрещенной для детей, и за проверку порядка их применения.

5.2.4. Осуществление внутреннего контроля за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, соответствием применяемых административных и организационных мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию, а также не соответствующей задачам образования.

5.2.5. Осуществление профилактики возможных нарушений законодательства в части защиты детей от информации, причиняющей вред их здоровью и (или) развитию, а не соответствующей задачам образования путем размещения соответствующих памяток (приложение 1 – 3).

5.3. К организационным мерам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, запрещенной к распространению в Российской Федерации, а также не соответствующей задачам образования, относятся:

5.3.1. Размещение в местах, доступных для детей, а также доведение иным доступным способом до третьих лиц настоящего Положения и иных локальных нормативных актов, направленных на защиту несовершеннолетних обучающихся от информации, причиняющей вред их здоровью и (или) развитию, запрещенной к распространению в Российской Федерации, а также не соответствующей задачам образования.

5.3.2. Размещение на официальном сайте в сети «Интернет» сведений о применении в Институте административных, организационных мер, а также технических и программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию, запрещенной к распространению в Российской Федерации, а также не соответствующей задачам образования, обеспечение свободного доступа к соответствующим локальным нормативным актам Института.

5.3.3. Применение технических и программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

5.3.4. К техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, запрещенной к распространению в Российской Федерации, а также не соответствующей задачам

образования, применяемым при предоставлении доступа к информации, распространяемой посредством сети «Интернет» в Институте, относятся:

– средства ограничения доступа к техническим средствам доступа к сети «Интернет»;

– средства ограничения доступа к сети «Интернет» с технических средств третьих лиц;

– средства ограничения доступа к запрещенной для распространения среди детей информации, размещенной на сайтах сети «Интернет», в частности, установка специального программного обеспечения;

– информационный контроль со стороны провайдера Интернет-связи;

– использование антивирусных программных комплексов.

5.3.5. Средства ограничения доступа к техническим средствам доступа к сети «Интернет»:

– доступ на управление к специализированному сетевому оборудованию, обеспечивающему доступ к сети «Интернет», регулируется методами авторизации (пароли, ключи авторизации и доступа);

– технические средства доступа в сеть «Интернет» устанавливаются в специальных помещениях с ограниченным доступом только для работников Института, имеющим соответствующий доступ, либо в помещениях, в которые не разрешен самостоятельный доступ несовершеннолетних обучающихся.

5.3.6. Средства ограничения доступа к сети «Интернет» с технических средств третьих лиц.

При доступе в сеть «Интернет» с технических средств третьих лиц в сети Института:

– подключение технических средств третьих лиц к сети Института по кабельной локальной сети запрещено;

– регистрация всех сетевых адресов, используемых при подключении по локальной сети к «Интернет», производится только работником Института, имеющим соответствующий допуск, использование незарегистрированных сетевых адресов запрещено;

– сетевое оборудование, через которое возможен выход в сеть «Интернет», устанавливается в помещениях, недоступных для обучающихся;

– подключение к сети «Интернет» через сеть Института по беспроводной технологии WiFi с технических средств третьих лиц возможно только при использовании авторизационных параметров (пароли доступа к сети WiFi).

5.3.7. Средства ограничения доступа к запрещенной для распространения среди детей информации, размещенной на сайтах в сети «Интернет», закреплены в разделе 7

настоящего Положения.

5.3.8. Обеспечение технических и программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию, в точках коллективного доступа к сети Интернет организуется работником Института в соответствии с его должностными обязанностями (системным администратором).

6. Организация доступа несовершеннолетних обучающихся к информационно-телекоммуникационной сети «Интернет»

6.1. Использование сети «Интернет» в Институте подчинено следующим принципам: соответствия образовательным целям, способствования гармоничному формированию и развитию личности, уважения закона, авторских и смежных прав, чести и достоинства граждан и пользователей сети «Интернет», приобретения новых знаний и навыков, расширения применяемого спектра учебных и наглядных пособий, социализации личности, введения в информационное общество.

Предоставление сеанса работы в сети «Интернет» осуществляется: обучающимся (в учебных аудиториях, компьютерных классах, помещениях для самостоятельной работы); работникам Института на их рабочих местах.

Обучающимся и работникам предоставляется доступ в сеть WiFi, при этом используется смешанная идентификация: для работников – индивидуальная, для обучающихся – групповая.

Использование сети «Интернет» разрешается только для работы и выполнения трудовых обязанностей, а также в научно-образовательных целях.

Использование сети «Интернет» в Институте в научно-образовательных целях направлено на решение задач учебно-воспитательного процесса и научно-исследовательской деятельности.

При использовании сети «Интернет» в Институте в научно-образовательных целях несовершеннолетним обучающимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношение к научно-образовательному процессу.

При использовании сети «Интернет» в Институте в научно-образовательных целях запрещено обращаться к ресурсам, содержащим информацию, причиняющую вред здоровью и (или) развитию обучающегося, распространение которой в Российской Федерации запрещено, не соответствующую целям образования.

6.2. Выполнение требований настоящего Положения осуществляется с помощью технических и программно-аппаратных средств контентной фильтрации, установленных в Институте или предоставленных оператором услуг связи.

К техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, нарушающей законодательство Российской Федерации, а также не соответствующей задачам образования, применяемым при предоставлении доступа к информации, распространяемой посредством сети «Интернет» относятся:

- средства контентной фильтрации;
- средства, ограничивающие доступ к сети «Интернет».

Отнесение определенных ресурсов и (или) категорий ресурсов в соответствующие группы, доступ к которым регулируется техническими и программно-аппаратными средствами контентной фильтрации, обеспечивается ответственным за защиту детей от негативной информации.

При принятии решения ответственный за защиту детей от негативной информации, руководствуется: законодательством Российской Федерации; специальными познаниями, в том числе полученными в результате профессиональной деятельности по рассматриваемой тематике; опытом целесообразной и эффективной организации учебного процесса с использованием информационных технологий и возможностей сети «Интернет»; интересами обучающихся, в том числе в части защиты детей от информации, причиняющей вред их здоровью и (или) развитию, целями образовательного процесса; рекомендациями профильных органов и организаций в сфере классификации ресурсов сети «Интернет».

Институт самостоятельно принимает решения о технологиях и формах организации системы ограничения, обучающихся к информации, причиняющей вред их здоровью и (или) развитию, а также не соответствующей задачам образования.

6.3. Соответствующие работники Института обеспечивают применение необходимых технических и программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию, нарушающей законодательство Российской Федерации, а также не соответствующей задачам образования, в том числе используя методы ограничения (запрета) доступа к ресурсам, потенциально способным причинить вред здоровью и (или) развитию детей.

Соответствующие работники Института, ответственные за использование технических средств и программного обеспечения, ограничения доступа к сети «Интернет» осуществляют:

- блокирование доступа к определенным ресурсам и (или) категориям;
- регулярное обновление антивирусного программного обеспечения;
- контроль состояния системы обеспечения информационной безопасности и интернет-канала Института.

6.4. Настройка технических и программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию, запрещенной к распространению в Российской Федерации, а также не соответствующей задачам образования, в том числе в точках доступа к сети «Интернет», осуществляется работниками Департамента информационных технологий.

Блокировка доступа к сайтам экстремистского характера осуществляется провайдером в соответствии с законодательством Российской Федерации и по договору оказания услуг связи в сети передачи данных.

Фильтрация к ресурсам, согласно норм законодательства в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию, а также, внесенным в «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащих информацию, распространение которой запрещено на территории РФ», осуществляется с помощью программных и аппаратных средств провайдером, предоставляющим услуги «Интернет».

Технические и программно-аппаратные средства, программное обеспечение не могут осуществлять полную фильтрацию ресурсов в сети «Интернет» в связи с частотой обновления ресурсов сети «Интернет». В связи с этим пользователи сети «Интернет» должны осознавать возможную опасность столкновения с ресурсом, содержание которого противоречит законодательству Российской Федерации и является несовместимым с целями и задачами образования, а также, что Институт не несет ответственности за случайный доступ к подобной информации, размещенной не на Интернет-ресурсах Института.

6.5. Самостоятельный доступ несовершеннолетних обучающихся в помещения Института, в которых установлены компьютеры, подключенные к сети «Интернет», не допускается.

Входные двери указанных помещений оборудуются запорными устройствами.

Ответственность за допуск несовершеннолетних обучающихся к компьютерам, не используемым в учебном процессе, несут работники, которым компьютер был предоставлен Институтом для осуществления их должностных обязанностей.

6.6. Работникам и совершеннолетним обучающимся Института запрещается передавать пароли доступа к сети WiFi Института несовершеннолетним обучающимся.

6.7. При проведении занятий в компьютерных классах фильтрация к ресурсам, согласно норм законодательства в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию, а также, внесенным в «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих

идентифицировать сайты в сети «Интернет», содержащих информацию, распространение которой запрещено на территории РФ», осуществляется с помощью программных и аппаратных средств провайдером, предоставляющим услуги «Интернет».

6.8. Во время доступа несовершеннолетних обучающихся к сети «Интернет» вне учебных занятий, в том числе при выполнении самостоятельной работы в помещениях, предназначенных для самостоятельной работы, контроль использования ресурсов сети «Интернет» осуществляют следующие работники Института: в аудиториях для самостоятельной работы, компьютерных классах – работник, отвечающий за эксплуатацию информационных систем, сетей и компьютерной техники.

6.9. Во время аудиторных занятий в соответствии с учебным планом контроль за использованием несовершеннолетними обучающимися компьютера, подключенного к сети «Интернет», осуществляют научные и педагогические работники, ведущие занятия.

Преподаватель осуществляет устный инструктаж обучающихся о правилах пользования информацией в сети «Интернет», визуальный контроль (наблюдает) за использованием компьютера и сети «Интернет» обучающимися; принимает меры для пресечения попыток доступа к ресурсу (группе ресурсов), несовместимых с задачами образования и не имеющим отношения к проводимому занятию, а также использования нештатных и непроверенных информационных носителей, копирования на компьютер информации, не относящейся к образовательному процессу.

6.10. Во время использования сети «Интернет» в образовательных или научных целях обучающемуся запрещается:

– обращаться к ресурсам, содержание и тематика которых недопустимы для несовершеннолетних и (или) нарушает законодательство Российской Федерации (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);

– осуществлять любые сделки через сеть «Интернет»;

– распространять в сети «Интернет» оскорбительную, не соответствующую действительности, порочащую честь и достоинство других лиц информацию, а также различного рода угрозы, иную информацию, распространение которой на территории Российской Федерации запрещено;

– использовать VPN-серверы, анонимайзеры и другие программные и облачные ресурсы для обхода блокировок и обеспечения анонимности при обращении к ресурсам сети «Интернет»;

– копировать на компьютер информацию, не относящуюся к образовательному процессу;

– загружать и распространять 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 сети «Интернет», а также размещения ссылок на вышеуказанную информацию;

– осуществлять загрузки файлов на компьютере без специального разрешения;

– изменять конфигурацию компьютеров, в том числе менять системные настройки компьютера и всех программ, установленных на нем (заставки, картинку рабочего стола, стартовой страницы браузера);

– осуществлять любые действия, направленные на вмешательство в функционирование технических средств контентной фильтрации доступа к сети «Интернет»;

– осуществлять действия, направленные на «взлом» любых компьютеров, находящихся как в «точке доступа к сети «Интернет» Института, так и за его пределами.

6.11. При случайном обнаружении доступа к ресурсу, содержащему информацию, которая причиняет вред здоровью и (или) развитию детей, не имеющую отношения к научно-образовательному процессу, не совместимую с задачами образования, иную информацию, распространение которой в Российской Федерации запрещено, обучающийся обязан незамедлительно сообщить об этом сотруднику Института.

6.12. При получении соответствующей информации от обучающегося или в случае самостоятельного выявления доступа к таким ресурсам сети «Интернет» работники обязаны зафиксировать доменный адрес ресурса и время его обнаружения и сообщить об этом ответственному за защиту детей от негативной информации.

6.13. Ответственный за защиту детей от негативной информации обязан:

– принять информацию и обеспечить меры к ограничению доступа к информации, причиняющей вред здоровью и (или) развитию детей;

– в случае явного нарушения обнаруженным ресурсом законодательства Российской Федерации сообщить о нем руководству Института для принятия мер в соответствии с законодательством Российской Федерации.

Лицо, назначенное ответственным за обеспечение безопасного доступа к сети «Интернет», проводит анализ обстоятельств, послуживших причиной доступа к ресурсам сети «Интернет», содержащим информацию, причиняющую вред здоровью и (или) развитию детей, запрещенную к распространению в Российской Федерации, информацию, не совместимую с задачами образования.

На основе проведенного анализа данное лицо обеспечивает совершенствование системы контентной фильтрации в целях минимизации доступа к ресурсам сети «Интернет», содержащим информацию, причиняющую вред здоровью и (или) развитию детей, запрещенную к распространению в Российской Федерации, информацию, не совместимую с задачами образования.

Приложение 1

Перечень видов информации, запрещенной к распространению посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования

№ п/п	Виды информации	Описание видов информации
Информация, запрещенная для распространения среди детей		
1	Побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая описания и (или) изображения способов причинения вреда своему здоровью, самоубийства; обсуждения таких способов и их последствий, мотивирующая на совершение таких действий
2	Способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая рекламу или объявления/предложения о продаже наркотических средств, психотропных и (или) одурманивающих веществ, табачных изделий, алкогольной и спиртосодержащей продукции, пива и напитков, изготавливаемых на его основе, участии в азартных играх, использовании или вовлечении в проституцию, бродяжничество или попрошайничество, содержащая обсуждение или организующую активность на данную тему
3	Обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных законом о Защите детей от информации	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая описания, фотографии, рисунки, аудио-, видеоматериалы актов насилия или жестокости, участников актов насилия и жестокости, обосновывающие или оправдывающие акты геноцида, военных преступлений, преступлений против человечности, террористических акций, массовых и серийных убийств, содержащие обсуждения участия или планирование совершающихся или будущих актов насилия

4	Отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), призывающая к отказу от семьи и детей («чайлдфри»), страницы клубов для лиц нетрадиционной сексуальной ориентации, сообщества и ресурсы знакомств людей нетрадиционной сексуальной ориентации
5	Оправдывающая противоправное поведение	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая описания, фотографии, рисунки, аудио- и видеоматериалы, содержащие призывы к противоправному поведению, одобрение противоправного поведения
6	Содержащая нецензурную брань	Информационная продукция (в том числе сайты, форумы, доски объявлений, сайты социальных сетей, чаты в сети «Интернет»), содержащая нецензурную брань
7	Содержащая информацию порнографического характера	Информационная продукция (в том числе сайты, форумы, доски объявлений, сайты социальных сетей, чаты в сети «Интернет»), содержащая описания, фотографии, рисунки, аудио- и видеоматериалы по данной теме
8	О несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего	Информационная продукция (в том числе сайты, форумы, доски объявлений, сайты социальных сетей, чаты в сети «Интернет»), содержащая описания, фотографии, рисунки, аудио- и видеоматериалы по данной теме, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего
Информация, распространение которой среди детей определенных возрастных категорий ограничено		
9	Представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия	Информационная продукция (в том числе сайты, форумы, доски объявлений, сайты социальных сетей, чаты в сети «Интернет»), содержащая описания, фотографии, рисунки, аудио- и видеоматериалы по данной теме

10	Вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий	Информационная продукция (в том числе сайты, форумы, доски объявлений, сайты социальных сетей, чаты в сети «Интернет»), содержащая описания, фотографии, рисунки, аудио- и видеоматериалы по данной теме
11	Представляемая в виде изображения или описания половых отношений между мужчиной и женщиной	Информационная продукция (в том числе сайты, форумы, доски объявлений, сайты социальных сетей, чаты в сети «Интернет»), содержащая описания, фотографии, рисунки, аудио- и видеоматериалы по данной теме
12	Содержащая бранные слова и выражения, не относящиеся к нецензурной брани	Информационная продукция (в том числе сайты, форумы, доски объявлений, сайты социальных сетей, чаты в сети «Интернет»), содержащая указанные виды информации
Информация, не соответствующая задачам образования и воспитания		
13	Компьютерные игры, за исключением соответствующих задачам образования	Информационная продукция (в том числе сайты, форумы, доски объявлений, сайты социальных сетей, чаты в сети «Интернет») по тематике компьютерных игр, не соответствующая задачам образования, такая как порталы браузерных игр, массовые многопользовательские онлайн ролевые игры (ММОРИ), массовые многопользовательские игры, основанные на имитации боевых или противоправных действий, советы для игроков и ключи для установки и прохождения игр, игровые форумы и чаты
14	Ресурсы, базирующиеся или ориентированные на обеспечении анонимности распространителей и потребителей информации	Анонимные форумы, чаты, доски объявлений и гостевые книги, такие как: имиджборды, анонимайзеры, программы, обеспечивающие анонимизацию сетевого трафика в сети «Интернет»
15	Банки рефератов, эссе, дипломных работ, за исключением соответствующих задачам образования	Информационная продукция (в том числе сайты, форумы, доски объявлений, сайты социальных сетей, чаты в сети «Интернет»), представляющая собой банки готовых рефератов, эссе, дипломных работ, за исключением печатных и электронных образовательных и информационных ресурсов, создаваемых в организациях, осуществляющих образовательную деятельность

16	Онлайн-казино и тотализаторы	Информационная продукция (в том числе сайты, форумы, доски объявлений, сайты социальных сетей, чаты в сети «Интернет»), содержащая информацию об электронных казино, тотализаторах, играх на деньги
17	Мошеннические сайты	Сайты, навязывающие платные услуги на базе СМС-платежей, сайты, обманным путем собирающие личную информацию (фишинг)
18	Магия, колдовство, чародейство, ясновидение, приворот по фото, теургия, волшебство, некромантия, тоталитарные секты	Информационная продукция, оказывающая психологическое воздействие на детей, при которой человек обращается к тайным силам с целью влияния на события, а также реального или кажущегося воздействия на состояние

Приложение 2

Виды информации, распространение которой запрещено в Российской Федерации

Наименование тематической категории	Содержание
Пропаганда войны, разжигание ненависти и вражды, пропаганда порнографии и антиобщественного поведения	Информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды. Информация, пропагандирующая порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение
Злоупотребление свободой СМИ/ экстремизм	Информация, содержащая публичные призывы к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы
Злоупотребление свободой СМИ/ наркотические средства	Сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров. Пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров
Злоупотребление свободой СМИ/ информация с ограниченным доступом	Сведения о специальных средствах, технических приемах и тактике проведения контртеррористической операции
Злоупотребление свободой СМИ / Скрытое воздействие	Информация, содержащая скрытые вставки и иные технические способы воздействия на подсознание людей и (или) оказывающая вредное влияние на их здоровье
Экстремистские материалы или Экстремистская деятельность (экстремизм)	Предназначенные для обнародования документы либо информация, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности (в т. ч. труды руководителей национал-социалистской рабочей партии Германии, фашистской партии Италии; публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой либо этнической, социальной, расовой, национальной или религиозной группы). Экстремистская деятельность (экстремизм) включает в себя деятельность по распространению материалов (произведений), содержащих хотя бы один из следующих признаков: насильственное изменение основ конституционного строя и нарушение целостности РФ;

	подрыв безопасности РФ; захват или присвоение властных полномочий; создание незаконных вооруженных формирований; осуществление террористической деятельности либо публичное оправдание терроризма; возбуждение расовой, национальной или религиозной розни, а также социальной розни, связанной с насилием или призывами к насилию; унижение национального достоинства; осуществление массовых беспорядков, хулиганских действий и актов вандализма по мотивам идеологической, политической, расовой, национальной или религиозной ненависти либо вражды, а равно по мотивам ненависти либо вражды в отношении какой-либо социальной группы; пропаганду исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, социальной, расовой, национальной, религиозной или языковой принадлежности; воспрепятствование законной деятельности органов государственной власти, избирательных комиссий, а также законной деятельности должностных лиц указанных органов, комиссий, соединенное с насилием или угрозой его применения; публичную клевету в отношении лица, замещающего государственную должность РФ или субъекта РФ, при исполнении им своих должностных обязанностей или в связи с их исполнением, соединенную с обвинением в совершении указанных в законодательстве РФ деяний, при условии, что факт клеветы установлен в судебном порядке; применение насилия в отношении представителя государственной власти либо угроза применения насилия в отношении представителя государственной власти или его близких в связи с исполнением им своих должностных обязанностей; посягательство на жизнь государственного или общественного деятеля, совершенное в целях прекращения его государственной или иной политической деятельности либо из мести за такую деятельность; нарушение прав и свобод человека и гражданина, причинение вреда здоровью и имуществу граждан в связи с их убеждениями, расовой или национальной принадлежностью, вероисповеданием, социальной принадлежностью или социальным происхождением
Вредоносные программы	Информация о программах для ЭВМ, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети

Преступления	Клевета (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию). Оскорбление (унижение чести и достоинства другого лица, выраженное в неприличной форме). Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма. Склонение к потреблению наркотических средств и психотропных веществ. Незаконное распространение или рекламирование порнографических материалов. Публичные призывы к осуществлению экстремистской деятельности. Информация, направленная на пропаганду национальной, классовой, социальной нетерпимости, а также пропаганду социального, расового, национального и религиозного неравенства. Публичные призывы к развязыванию агрессивной войны
Информация с ограниченным доступом	Информация, составляющая государственную, коммерческую, служебную или иную специально охраняемую законом тайну
Ненадлежащая реклама	Информация, содержащая рекламу алкогольной продукции и табачных изделий

Приложение 3

Форма акта проверки аудитории для самостоятельной работы обучающихся и компьютерных классов

АКТ № ____

проверки аудитории для самостоятельной работы обучающихся/компьютерных классов

от «_____»_____20__г.

Настоящим актом удостоверяем, что в аудитории для самостоятельной работы обучающихся №____/ компьютерных классах на момент составления акта обнаружена/ не обнаружена информация, недопустимая для несовершеннолетних обучающихся и (или) нарушающая законодательство Российской Федерации *(при обнаружении указать имя компьютера, тематику ресурса).*

Председатель комиссии		
Должность	подпись	И.О. Фамилия
Члены комиссии		
Должность	подпись	И.О. Фамилия
Должность	подпись	И.О. Фамилия
Должность	подпись	И.О. Фамилия

Приложение 4

Правила работы на компьютерах в сети «Интернет» в помещениях для самостоятельной работы обучающихся, компьютерных классах

1. При входе в аудитории для самостоятельной работы обучающихся, компьютерные классы с целью работы на компьютерах в сети «Интернет» необходимо обратиться к должностному лицу, ответственному за компьютерную технику.

2. При наличии свободных мест обучающемуся предоставляется рабочая станция (ПЭВМ).

3. При работе на компьютерах в сети «Интернет» пользователи обязаны выполнять все требования должностного лица, ответственного за компьютерную технику.

4. За одним рабочим столом должно находиться не более одного пользователя.

5. **Пользователю запрещено:**

– входить в систему более чем с одной рабочей станции без особого разрешения на то должностного лица;

– применять физические носители информации неизвестного происхождения;

– вносить какие-либо изменения в программное обеспечение, установленное как на рабочей станции, так и на серверах, а также хранить личную информацию на жестком диске рабочей станции;

– передавать информацию, представляющую государственную, коммерческую или иную охраняемую законом тайну, без соблюдения требований специальных нормативных правовых актов;

– распространять информацию, порочащую честь и достоинство граждан;

– работать с объемными ресурсами (видео-, аудио-, игры и др.) без согласования с работником Института, назначенным ответственным за использование сети «Интернет» в научно-образовательных целях, а также применение административных, организационных мер, технических и программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию, учитывающих специфику оборота информационной продукции, запрещенной для детей, и за проверку порядка их применения;

– использовать оборудование для работы с информационными ресурсами и электронной почтой в коммерческих и (или) личных целях, не связанных с образовательным процессом и (или) исследовательскими и научными изысканиями, либо выполнением гуманитарных и культурных проектов;

– осуществлять доступ к сайтам, содержащим информацию сомнительного содержания и противоречащую общепринятой этике.

6. **Пользователю разрешается:**

– записывать полученную информацию на личные носители информации, которые должны предварительно проверяться на наличие вирусов;

– использовать оборудование для работы с информационными ресурсами и электронной почтой исключительно в научно-образовательных целях или для осуществления исследовательских или научных изысканий, выполнения гуманитарных и культурных проектов.

7. Пользователь обязан сохранять оборудование в целости и сохранности.

8. При нанесении любого ущерба (порча имущества, вывод оборудования из рабочего состояния) пользователь несет ответственность в соответствии с действующим

законодательством Российской Федерации.

9. Контроль за соблюдением пользователями настоящих Правил осуществляет работник Института, назначенный ответственным за использование сети «Интернет» в научно-образовательных целях, а также применение административных, организационных мер, технических и программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию, учитывающих специфику оборота информационной продукции, запрещённой для детей, и за проверку порядка их применения.

Приложение N 5

Памятка для обучающихся об информационной безопасности детей

НЕЛЬЗЯ

1. Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей);
2. Открывать вложенные файлы электронной почты, когда не знаешь отправителя;
3. Грубить, придираться, оказывать давление - вести себя невежливо и агрессивно;
4. Не распоряжайся деньгами твоей семьи без разрешения старших - всегда спрашивай родителей;
5. Не встречайся с Интернет-знакомыми в реальной жизни - посоветуйся со взрослым, которому доверяешь.

ОСТОРОЖНО

1. Не все пишут правду. Читаешь о себе неправду в Интернете - сообщи об этом своим родителям или опекунам;
2. Приглашают переписываться, играть, обмениваться - проверь, нет ли подвоха;
3. Незаконное копирование файлов в Интернете - воровство;
4. Всегда рассказывай взрослым о проблемах в сети - они всегда помогут;
5. Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах.

МОЖНО

1. Уважай других пользователей;
2. Пользуешься Интернет-источником - делай ссылку на него;
3. Открывай только те ссылки, в которых уверен;
4. Общаться за помощью взрослым - родители, опекуны и администрация сайтов всегда помогут;
5. Пройди обучение на сайте "Сетевичок" и получи паспорт цифрового гражданина!

Приложение N 6

Информационная памятка для обучающихся для размещения на официальных интернет-ресурсах

С каждым годом молодежи в интернете становится больше, а школьники одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в сети.

Компьютерные вирусы

Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ;
2. Постоянно устанавливай пачти (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;
4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
5. Ограничь физический доступ к компьютеру для посторонних лиц;
6. Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд "WECA", что обозначало словосочетание "Wireless Fidelity", который переводится как "беспроводная точность".

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура "Wi-Fi". Такое название было дано с намеком на стандарт высшей звуковой техники Hi-Fi, что в переводе означает "высокая точность".

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работы в общедоступных сетях Wi-fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
3. При использовании Wi-Fi отключи функцию "Общий доступ к файлам и принтерам". Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе;
4. Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;
5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно "https://";
6. В мобильном телефоне отключи функцию "Подключение к Wi-Fi автоматически". Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Социальные сети

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;

7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронные деньги

Электронные деньги - это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов - анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;
2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли - это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;;
4. Не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта

Электронная почта - это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
2. Не указывай в личной почте личную информацию. Например, лучше выбрать "музыкальный_фанат@" или "рок2013" вместо "тема13";
3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;
5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;
6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;
7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;
8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на "Выйти".

Кибербуллинг или виртуальное издевательство

Кибербуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.
Основные советы по борьбе с кибербуллингом:
1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;
2. Управляй своей киберрепутацией;
3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;
5. Соблюдай свою виртуальную честь смолоду;
6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и

теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;

Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?

Необходимо обновлять операционную систему твоего смартфона;

Используй антивирусные программы для мобильных телефонов;

Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;

После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;

Периодически проверяй, какие платные услуги активированы на твоем номере;

Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;

Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Online игры

Современные онлайн-игры - это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для

программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности твоего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;

2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;

3. Не указывай личную информацию в профайле игры;

4. Уважай других участников по игре;

5. Не устанавливай неофициальные патчи и моды;

6. Используй сложные и разные пароли;

7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься "любимым" делом.

Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей - логинов и паролей. На английском языке phishing читается как фишинг (от fishing - рыбная ловля, password - пароль).

Основные советы по борьбе с фишингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;

2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;

3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;

4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;

5. Установи надежный пароль (PIN) на мобильный телефон;

6. Отключи сохранение пароля в браузере;

7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Цифровая репутация

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на твоей реальной жизни. "Цифровая репутация" - это твой имидж, который формируется из информации о тебе в интернете.

Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких - все это накапливается в сети.

Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.

Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только "для друзей";
3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

Авторское право

Современные школьники - активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира

требует соблюдения прав на интеллектуальную собственность.

Термин "интеллектуальная собственность" относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Авторские права - это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.

Использование "пиратского" программного обеспечения может привести к многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в сети.

Приложение N 3

Памятка для родителей об информационной безопасности детей

Определение термина "информационная безопасность детей" содержится в Федеральном законе N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", регулирующим отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию. Согласно данному закону "информационная безопасность детей" - это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

В силу Федерального закона N 436-ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:

1. информация, запрещенная для распространения среди детей;

2. информация, распространение которой ограничено среди детей определенных возрастных категорий.

3. К информации, запрещенной для распространения среди детей, относится:

4. информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству;

5. способность вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе; принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

6. обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;

7. отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

8. оправдывающая противоправное поведение;

9. содержащая нецензурную брань;

10. содержащая информацию порнографического характера.

К информации, распространение которой ограничено среди детей определенного возраста, относится:

1. информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;

2. вызывающая у детей страх, ужас или панику, в т.ч. представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;

3. представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

4. содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

С учетом этого Вам предлагаются правила работы в сети Интернет для различных возрастных категорий, соблюдение которых позволит обеспечить информационную безопасность ваших детей.

Общие правила для родителей

1. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку - главный метод защиты.

2. Если Ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.

3. Проверьте, с какими другими сайтами связан социальный сервис Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт, или сайт, на котором друг упоминает номер сотового телефона Вашего ребенка или Ваш домашний адрес).

4. Поощряйте Ваших детей сообщать обо всем странном или отталкивающем и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).

5. Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями.

Возраст от 7 до 8 лет

В Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям особенно полезны будут те отчеты, которые предоставляются программами по ограничению

использования Интернета, т.е. Родительский контроль или то, что вы сможете увидеть во временных файлах. В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернету, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

Советы по безопасности в сети Интернет для детей 7-8 лет

1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.

2. Требуйте от Вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что Вы наблюдаете за ним не потому что Вам это хочется, а потому что Вы беспокоитесь о его безопасности и всегда готовы ему помочь.

3. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.

4. Используйте специальные детские поисковые машины.

5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

6. Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.

7. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.

8. Приучите детей советоваться с Вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.

9. Научите детей не загружать файлы, программы или музыку без вашего согласия.

10. Не разрешайте детям использовать службы мгновенного обмена сообщениями.

11. В "белый" список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.

12. Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.

13. Не делайте "табу" из вопросов половой жизни, так как в Интернете дети могут легко

наткнуться на порнографию или сайты "для взрослых".

14. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Возраст детей от 9 до 12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности для детей от 9 до 12 лет

1. Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

2. Требуйте от Вашего ребенка соблюдения норм нахождения за компьютером.

3. Наблюдайте за ребенком при работе за компьютером, покажите ему, что Вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.

4. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

6. Не забывайте принимать непосредственное участие в жизни ребенка, беседовать с детьми об их друзьях в Интернете.

7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.

8. Позволяйте детям заходить только на сайты из "белого" списка, который создайте вместе с ними.

9. Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

10. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

11. Создайте Вашему ребенку ограниченную учетную запись для работы на компьютере.

12. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах и опасениях.

13. Расскажите детям о порнографии в Интернете.

14. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.

15. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Возраст детей от 13 до 17 лет

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок "для взрослых". Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернете.

Зачастую в данном возрасте родителям уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, не отпускайте детей в "свободное плавание" по Интернету. Старайтесь активно участвовать в общении ребенка в Интернете.

Важно по-прежнему строго соблюдать правила Интернет-безопасности - соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте от 13 до 17 лет

1. Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов ("черный список"), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).

2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.

3. Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким

образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.

4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

5. Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.

7. Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

8. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

9. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам, о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

10. Расскажите детям о порнографии в Интернете. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

11. Приучите себя знакомиться с сайтами, которые посещают подростки.

12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде - даже в виртуальном мире.

13. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

14. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

Постоянно контролируйте использование Интернета Вашим ребенком! Это не нарушение его личного пространства, а мера предосторожности и проявление Вашей родительской ответственности и заботы.