Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ДЕТЕЙ ОТ НЕГАТИВНОЙ ИНФОРМАЦИИ В СЕТИ INTERNET

Выпускная квалификационная работа
по направлению подготовки 44.03.04 Профессиональное обучение
(по отраслям)
профилю подготовки «Энергетика»
профилизации «Компьютерные технологии автоматизации и управления»

Идентификационный код ВКР: 118

Екатеринбург 2017

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

К ЗАЩИТЕ ДОПУСКАЮ
Заведующий кафедрой ИС
_____Н. С. Толстова
«____»_____2017г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ДЕТЕЙ ОТ НЕГАТИВНОЙ ИНФОРМАЦИИ В СЕТИ INTERNET

Исполнитель:
обучающийся группы № КТэ -402 С. А. Корнев
Руководитель:
ст.преподаватель Г. Л. Нечаева
Нормоконтролер:
ст.преподаватель Т. В. Рыжкова

Екатеринбург 2017

АННОТАЦИЯ

Выпускная квалификационная работа состоит из лабораторного практикума и пояснительной записки на 64 страницах, содержащей 15 рисунков, 1 таблицу, 24 источника литературы, а также 4 приложения на 4 страницах.

Ключевые слова: РОДИТЕЛЬСКИЙ КОНТРОЛЬ, INTERNET, ИНФОРМАЦИЯ.

Корнев, С.А. Обеспечение защиты детей от негативной информации в сети Internet: выпускная квалификационная работа / С. А. Корнев; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. – Екатеринбург, 2017 – 64 с.

В работе рассмотрены вопросы обеспечения защиты детей от негативной информации в сети Internet.

Целью работы является разработка комплекса мероприятий по обеспечению защиты детей в сети Internet. Для достижения цели были проанализированы основные теоретические материалы по способам защиты детей от негативной информации в сети Internet, выполнен обзор программно-аппаратного обеспечения, разработана структура и содержание лабораторного практикума, предложена система мероприятий по организации защиты детей от негативной информации в сети Internet. Комплекс мероприятий включает в себя анкетирование, обзор основных Федеральных законов по защите детей от негативной информации, способной нанести им вред, лабораторный практикум, свод правил по работе в сети Internet.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном обществе огромную роль занимают компьютер и интернет. Они помогают нам в учёбе, в работе и просто используются для развлекательных целей.

Ещё в далёком 1964 году с созданием интегральной схемы случился глобальный скачок от крупных и массивных электронно-вычислительных машин, которые находили своё применение в научных лабораториях, к персональному компьютеру. Это привело к уменьшению габаритов, стоимости и упрощению устройства больших ЭВМ. Позже, в начале 2000-х, к компьютеру присоединился Интернет. И сейчас эти два научных чуда, зачастую, неразрывно связаны друг с другом.

При нынешнем уровне развития глобальных коммуникаций и информационных технологий, родители и педагоги нередко не имеют возможности защитить детей от негативных и вредоносных для них сведений. Избыток жестокости и насилия в общедоступных средствах массовой информации способен создать у ребёнка искаженную картину общества и ошибочные, а иногда даже небезопасные жизненные ситуации.

В ходе изучения вопроса об обеспечении безопасности детей в сети Internet обучающимся будет предложено пройти анкетирование, познакомиться с основными Федеральными законами, касающимися этой темы, а так же выполнить лабораторный практикум. Данный практикум содержит 5 лабораторных работ по настройке аппаратно-программного обеспечения компьютера, вопросы для самопроверки, задания для самостоятельного выполнения, ссылки на полезную литературу, а так же глоссарий.

Обучающиеся, успешно прошедшие предложенные мероприятия, получат особые знания и умения, которые помогут им в дальнейшем организовать детям безопасный поиск в сети Internet.

Обучающиеся, прошедшие лабораторный практикум по теме «Обеспечение защиты детей от негативной информации в сети Internet», будут знать основные способы защиты, базовые и понятные программы по ограничению доступа к сети Internet. Также знать необходимые параметры для настройки роутера.

Объект работы – процесс обеспечения защиты детей от негативной информации в сети Internet.

Предмет работы – система мероприятий для самостоятельного изучения по теме «Обеспечение защиты детей от негативной информации в сети Internet».

Для достижения цели необходимо решить следующие задачи:

1. Рассмотреть теоретический материал по основным способам защиты детей от негативной информации в сети Internet.
2. Изучить интерфейс программ по ограничению доступа в сеть Internet.
3. Разработать структуру и содержание лабораторного практикума.
4. Составить список мероприятий по теме «Обеспечение защиты детей от негативной информации в сети Internet».

Разработанная система мероприятий предназначена для самостоятельного обучения в системе дополнительного образования учащимися учебно-технического центра «Омега – 1».

1 ЗАЩИТА ДЕТЕЙ ОТ НЕГАТИВНОЙ ИНФОРМАЦИИ В СЕТИ INTERNET

1.1 Виды информации, способной нанести вред детям

Основываясь на формулировки закона, упомянутые виды информации можно объединить так:

1. **Пропаганда.** Информация, побуждающая или рекламирующая детям различные социально неоднозначные действия – вред здоровью или самоубийства, употребление алкоголя, табака и прочих наркотических веществ, карточные и азартные игры, проституцию, насилие над людьми и животными, неуважение к семье и нетрадиционные сексуальные отношения, правонарушения.
2. **Нецензурная речь** и другие бранные выражения.
3. **Порнографическая информация** и половые отношения в виде изображения или описания.
4. **Насилие и пугающий контент**. Изображение или описание (не реклама) насилия, преступлений, жестокости, болезней, совершения суицида, трагедий, аварии или катастрофы и (или) их последствий.
5. **Личная информация о ребёнке**, которая дает возможность установить его личность и местоположение.

Что же говорит о потребности защиты такого рода материала? Пройдёмся по пунктам.

1.1.1 Пропаганда и реклама

По данным исследования Американской ассоциации психологов (АСА): дети возрастом до 8 лет не умеют критически производить оценку те-

левизионных рекламных сообщений и склонны думать, что они полезные, точные, объективные.

По данным российского исследования становится понятно, что 55% дошкольников доверяют рекламе. Отношение к рекламе школьников младших классов более осознано и критично, верят рекламе только 23-30% детей, больше половины – не доверяют вовсе. Подростки в основном не доверяют рекламным сообщениям.

Согласно еще одному исследованию, опубликованному более десяти лет назад в журнале Tobacco Control (Великобритания), подростки, которые постоянно подвергаются влиянию большого числа рекламы табака, закурят с вероятностью 70%, в то время как люди, которые имеют низкий уровень воздействия, закурят с вероятностью 11%.

Вот рекомендации, данные Центром по предотвращению самоубийств (США) для СМИ. Подобные сведения могут подтолкнуть к этому шагу или попытке его имитации. Например, навредить может детальное описание суицида, романтизация погибшего, идеализация известных личностей, реакция близких людей погибшего, завышение информации о частоте самоубийств. Полезными же могут стать сведения об оказываемой помощи, рассказы людей, которые смогли справиться с ситуациями, не прибегая к самоубийству, контакты специалистов и горячей линии.

Также имеется множество исследований, подтверждающих, что рекламные компании влияют на пищевые привычки детей:

1. Дети потребляют на 45% больше под влиянием рекламы продуктов питания.

2. Дети предпочитают рекламируемые продукты, вопреки запретам родителей.

3. Реклама продуктов питания и напитков, которая направленна на детей и молодёжь, идёт вразрез со здоровым питанием и подвергает риску их здоровье.

1.1.2 Нецензурная речь

Существует достаточно много исследований о влиянии на детей нецензурной лексики в средствах массовой информации. Одно из них, опубликованное в официальном журнале Американской академии педиатров Pediatrics, утверждает, что дети, которые слышат бранные слова на телевидении, более агрессивны, а агрессивные дети, в свою очередь, более склонны к насмешкам. Причем речь идёт не только о матерной лексике.

1.1.3 Порнография

Согласно отчёту RAND (некоммерческая организация в США, которая занимается исследованиями и аналитикой), постоянный просмотр контента с сексуальной тематикой приближает начало подростковой сексуальной активности, причём влияют как демонстрирование сексуального поведения, так и его обсуждение. При этом данные о последствиях и всевозможных рисках, методах контрацепции могут способствовать установлению диалога между ребенком и его родителями.

Статья на сайте BBC говорит о том, что подростки могут копировать сексуальное поведение, демонстрируемое в порнографии, думая, что это нормальные действия в сексуальной жизни всех людей.

В докладе министерства внутренних дел Великобритании от 2010 года содержалось предупреждение о том, что «ползучее проникновение» эротики и откровенной порнографии в жизнь подростков искажает их самовоспитание: мальчики начинают зацикливаться на мачизме и доминировании, а девочки чувствуют себя обязанными быть сексуально доступными.

1.1.4 Насилие и жестокость

Проблеме влияния на детей насилия печатные издания посвящали уже долгие годы исследований. В одной из статей на сайте Американской ассоциации психологов приведены выводы из отчёта Национального института психического здоровья, где перечислены основные эффекты от частого просмотра сцен насилия. Вот они:

- дети могут становиться менее чувствительными к боли и страданиям других;
- дети могут начать больше бояться мира вокруг них;
- дети могут с большей вероятностью вести себя агрессивно, враждебно или причиняя вред другим людям.

Исследования психологов Л. Хьюсман, Л. Эрон (США), начиная с 1980-х годов показали, что дети, которые часами смотрели на насилие по телевидению, когда были в начальной школе, обычно показывают более высокий уровень агрессивного поведения, став подростками. Наблюдая за этими участниками в зрелом возрасте, Хьюсман и Эронустановили, что те, кто бы смотрел много сцен насилия по ТВ, когда они были в возрасте восьми лет, вероятнее всего, будут арестованы или привлечены к ответственности за преступные действия, будучи взрослыми.

Но в более поздних исследованиях психологов Д. Джентайл, Б. Бушмен (США), среди прочего, предполагалось, что воздействие насилия в СМИ является только одним из множества факторов, которые могут способствовать агрессивному поведению.

1.1.5 Персональная информация

Существуют следующие риски, связанные с раскрытием персональной информации:

- персональные данные могут быть использованы для мошенничества, спама, взлома аккаунтов, подбора паролей, мошенники могут выдавать себя за человека, чьи данные они используют;
- используя информацию о местоположениях, где обычно находится ребёнок, преступники могут нанести вред ребенку, похитить его проникнуть в дом;
- персональные данные могут также быть использованы для кибериздевательств;
- информация о человеке, который пострадал от правонарушения, может составлять его личную или семейную тайну, использоваться для угроз со стороны пособников правонарушителя.

1.2 Классификация интернет – угроз

Во всемирной паутине есть определённая классификация Интернет – угроз. Юных пользователей сети интернет могут подстерегать опасности. Условно их можно поделить на интернет – угрозы, связанные с безопасностью компьютера, с которого выполняется выход в Internet, и интернет – угрозы психологического характера для детей и молодёжи.

Во всемирной паутине можно встретить следующие виды угрозы для несовершеннолетних пользователей:

- сайты, призывающие к самоубийству;
- сайты-форумы потенциальных самоубийц;
- наркосайты (интернет пестрит статьями о «пользе» употребления марихуаны, рецептами и рекомендациями по приготовлению «зелья»);

- сайты, разжигающие национальную рознь и расовое неприятие (экстремизм, национализм, фашизм);
- сайты безнравственной направленности;
- сайты знакомств (виртуальное общение приводит к тому, что подростки теряют способности к реальному общению, у них исчезают коммуникативные навыки);
- сайты, пропагандирующие экстремизм, насилие и девиантные формы поведения, непосредственные угрозы жизни и здоровью детей от незнакомцев, которые предлагают личные встречи, а кроме того разнообразные виды аферы;
- секты (виртуальный собеседник способен оказать влияние на мировоззрение ребенка).

1.3 Международный опыт защиты детей от негативной информации. Решение данного вопроса в разных странах

Проблема защиты детей от негативной информации заключается в невозможности регулирования Интернета национальным законодательством. Международное сообщество, осознавая нравственную ответственность за детские жизни, реализует её через международные стандарты и обязанности государств.

Международные стандарты защиты детей от негативной информации – это утвержденные на международном уровне правила, требования и принципиальные положения, обращенные на координацию деятельности государств по обеспечению прав ребёнка на информацию и защиты его от негативной информации. Международные стандарты фиксируются в соглашениях, декларациях, пактах, конвенциях, правилах и других документах в виде норм, принципов и рекомендаций. Документы не равнозначны по юридическому статусу, но едины в выражении стремления мирового сообщества по макси-

муму скоординировать политику, методы и средства защиты детей от негативной информации.

Большая часть международных стандартов и общепринятых принципов и нормы о защите детей от негативной информации разработаны в рамках ООН. Кроме того, защита прав детей от негативной информации является внутренним делом каждого государства, и оно само определяет, в каких договорах следует принимать участие, к делам каких международных организаций присоединиться и в каком объёме. Здесь невозможно вмешательство во внутренние дела государств. Этим можно объяснить тот факт, что почти все решения и резолюции ООН носят характер рекомендаций. Все же, многие государства признают их приоритет над своим внутренним законодательством.

1.3.1 Опыт США

Ещё в 90-е годы в США активно рассматривался вопрос о защите детей в глобальной информационной системе. Таким образом, в 1996 году Конгресс одобрил Communication Decency Act, признавший противозаконным размещать в сети Интернет заведомо оскорбительные материалы, согласно общественным нормам. Но верховный суд отклонил статьи этого закона как неконституционные. Представленный позже в 1998 году Children`s Online Privacy Protection Act был опять же почти сразу заблокирован решением федерального апелляционного суда, а после и ликвидирован.

В октябре 2000 года Конгресс США принял закон «О защите детского Интернета» (CIPA), оберегающий детей от сексуальных и иных нежелательных материалов, которые размещены в Интернете. Закон предписывает школам и библиотекам, принимающим участие в федеральной программе доступа к сети Интернет (в качестве условия получения федерального финансирования E –Rate), устанавливать программные фильтры, которые мешают просмотру материалов порнографического и другого нежелательного содержа-

ния. Библиотекам позволяется открывать доступ к конкретным сайтам по просьбам взрослых интернет-пользователей для научных и иных законных целей.

Так же в США действует закон «о защите конфиденциальности детей в Интернете» (COPPA). Закон применяется к собиранию персональной информации от детей младше 13 лет лицами или организациями под юрисдикцией США.

Согласно закону, администрация сайта обязана включить в политику конфиденциальности варианты получения согласия родителей или опекунов, и ответственности администрации за сохранение конфиденциальности и безопасности детей в глобальной информационной системе, включая ограничения в маркетинге. Хотя, не смотря на то, что дети имеют возможность публиковать личные данные легально с согласия родителей, большая часть сайтов всё же блокируют детей из-за количества работы, связанной с этим.

Так же с 2000 года в США нельзя продавать телевизоры, которые не имеют специального кодирующего устройства, позволяющего родителям программировать телевизор на приём передач с учётом их возрастной классификации.

Со временем акцент сместился с вопросов противодействия распространению порнографии на борьбу с сексуальными преследованиями детей онлайн. С 2009 года был поставлен вопрос об обучении подростков навыкам интернет-грамотности. Появился проект Online Safety 3.0, ставший заниматься исследованиями данной области.

Кроме всех этих законов также в некоторых штатах действуют свои локальные законы, которые касаются киберпреследования и издевательств.

1.3.2 Опыт Канады

Сейчас в Канаде нет отдельных законов, которые бы регулировали интернет – контент. К сайтам, размещённым в Канаде и к её резидентам, чьи

сайты размещены на серверах, что находится под иной юрисдикцией, применяются требования общих законов.

В ноябре 2006 года ряд основных канадских Интернет – провайдеров анонсировали проект «Cleanfeed Канада»; добровольное блокирование доступа к сотням предлагаемых сайтов с детской порнографией. Список заблокированных сайтов формируется из отчётов пользователей Интернета и исследуется независимой организацией Cybertip.ca. Хоть это и добровольный шаг без участия со стороны властей, канадское правительство выразило своё одобрение.

1.3.3 Опыт Великобритании

В данной стране ведущие интернет – провайдеры предлагают включённую фильтрацию контента по умолчанию, с возможностью отказа от её использования. Фильтры не пропускают многие категории содержимого: сайты знакомств, табак, алкоголь, наркотики, файлообмен, азартные и онлайн-игры, социальные сети и форумы, самоубийство и вред здоровью, оружие и насилие, нецензурные выражения, ненависть, криминальные навыки, анонимайзеры и прочее.

Мобильные операторы стали добровольно фильтровать информацию с 2004 года. При попадании на сайт с запрещённым содержимым появляется страница с предупреждением. Взрослые пользователи имеют возможность отключить эту функцию.

Шесть главных провайдеров общественного Wi-Fi, суммарно ответственных за его долю в 90%, тоже выполняют добровольную фильтрацию.

Есть проблемы с попаданием разрешённых сайтов под действие фильтров. Так, около половины общественных Wi-Fi фильтров блокирует религиозные сайты, треть – сайты с сексуальным образованием. Также ошибочно блокируются службы поддержки людей с проблемами, которые связанны с вышеперечисленной тематикой, библиотеки и политические сайты.

Также в Великобритании действует система Cleanfeed, проверяющая URL на наличие в конфиденциальном «черном списке URL» и отдаёт «Страница не найдена» в случае совпадения. Из этого следует, что пользователь не может без сомнения определить, была ли запрашиваемая страница заблокированной или по каким-то причинам просто отсутствовала на сайте. Введением запрещённых URL занимается неправительственная организация IWF.

1.3.4 Опыт Китайской Народной Республики

В Китайской Народной Республике огромное количество законов регулирующих Интернет. Так для защиты детей от негативной информации Китай разработал концепцию «большого китайского брандмауэра», закрепленного в законе о защите несовершеннолетних(1992). Основными субъектами, ответственными за исполнение закона определены родители и государство. Родители обязаны профилактировать Интернет зависимость детей. Государство обязано развивать технологии защиты несовершеннолетних от ненужных материалов. Под ними понимаются данные включающие порно, насилие, акты терроризма, расовой ненависти и азартные игры, а кроме того предусматривает уголовную ответственность за торговлю, аренду либо продвижение среди несовершеннолетних аналогичных материалов.

По согласованию с властью в июне 2004 организовали Центр жалоб в целях контроля за соблюдением закона. Одной из целей Центра считается «защита общества, в частности, несовершеннолетних, от влияния незаконной и вредной информации». В основном Центр занимается противодействием популяризации материалов, которые считаются губительными для здорового становления несовершеннолетних, такие как непристойные и порнографические материалы, игры частью которых является насилие, терроризм, пособничество в совершении преступлений, а кроме того данных, распространяющих расовую ненависть и т.д. За минувшие года Центр принял свыше 30 тысяч жалоб о несоблюдении закона.

Также с 2003 года на территории Китайской Народной Республики начал функционировать проект «Золотой щит», создание которого началось с 1998 года. «Золотой щит» представляет собой организацию серверов на интернет-канале среди провайдеров и международных сетей передачи данных, которая фильтрует информацию.

1.3.5 Опыт Австралии

Правительственный регулятор Австралийские коммуникации и средства массовой информации занимаются лимитированием интернет-контента, расположенного в Австралии и ведением «черного списка» сайтов, размещенных в других странах. Данный список после применяется системами фильтрации, какие предлагаются абсолютно всем потребителям провайдерами и властью Австралии.

1.3.6 Опыт Сингапура

В Сингапуре тоже работает общегосударственный регулятор The Media Development Authority, который контролирует интернет-обслуживание трех главных провайдеров. Блокируется определенное число страниц, включающих в себя «неприемлемые» материалы, в их числе Playboy, YouPorn и сайт знакомств Ashley Madison.

Кроме этого, Министерство образования Сингапура перекрывает доступ к порнографическому и некоторому «неугодному» интернет-контенту, к отдельным торрент-сайтам. При попытке заполучить доступ к заблокированному веб-сайту, гости страницы, обычно, видят сообщение The Media Development Authority, хотя определенные страницы отображаются с ошибкой 404.

Список блокируемых веб-сайтов конфиденциален, кроме того в него входят сайты, которые связанны с гомосексуализмом, новостные сайты Малайзии, сайты с антиисламскими настроениями.

1.3.7 Опыт Швеции

В Швеции основные поставщики интернет-услуг используют DNS-фильтр, блокирующий «очевидно» нелегальный контент, к коему относятся: призывы к бунту, расовая агитация, детская порнография, незаконное описание насилия.

Шведская полиция ответственна за ведение и обновление списка запрещенных сайтов.

Также в Швеции запрещена реклама для детей младше 12 лет.

1.3.8 Опыт Германии

Требования об удалении и ограничении доступа накладываются на немецких интернет-провайдеров, как правило, для защиты несовершеннолетних или для подавления пропаганды ненависти и экстремизма.

В 2009 году был принят закон о блокировке сайтов с детской порнографией, но в 2011 году он был отвергнут по причине того, что провайдеры и так быстро удаляют детскую порнографию, когда получают информацию о ней.

1.3.9 Опыт России

В России совершенно недавно были внесены важные изменения в законодательстве, которые ужесточили контроль над негативной информацией. Так 28 июля 2012 года был принят Федеральный закон №139-Ф317 «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети Интернет». Данный закон внёс поправки в ряде

положений и в иных федеральных законах, которые предполагают фильтрацию негативной информации:

1. Поправки были внесены в принятый 29 декабря 2010 года №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Изменения вносят множество новых уточнений и подробнее регламентируют способы маркировки информации. Текущим законом вносится положение о том, что доступ к сети Интернет в «местах доступных для детей» должен быть ограничен.

2. В Кодексе Российской Федерации об административных правонарушениях от 30.12.2001 №195-ФЗ были внесены положения об ответственности за неприменение в местах, доступных для детей, операторами связи, оказывающими услуги связи, либо администрацией таких мест при осуществлении доступа к информации, распространяемой через Интернет, административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью или развитию.

3. В Федеральный закон от 7 июля 2003 года №126-ФЗ «О связи» внесено изменение об ограничении и восстановлении доступа к материалам, распространяемым через Интернет, и регулирующимися Федеральным законом №149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации».

4. Большие поправки были внесены в Федеральный закон от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации». В этом федеральном законе даются формулировки интернет-сайта, интернет-страницы, сетевого адреса, доменного имени, хостинг-провайдера, владельца интернет-сайта. Здесь же возникает новая статья, в соответствии с которой образуется некая информационная система «Единый реестр доменных имён и универсальных указателей страниц сайтов в сети Интернет и сетевых адресов сайтов сети Интернет, содержащих ин-

формацию, запрещённую к распространению на территории Российской Федерации».

Реестр – это автоматизированная информационная система ведения и использования базы данных о сайтах, содержащих незаконную к распространению в России информацию.

Реестр находится в ведении Роскомнадзора в соответствии с постановлением Правительства Российской Федерации от 26 октября 2012 года №1101 «О единой автоматизированной информационной системе «Единый реестр доменных имён, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, которые позволяют идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», включающей в себя информацию, которая запрещена к распространению на территории Российской Федерации».

Реестр нацелен на предупреждение распространения через сайты негативной информации, в частности туда вносятся ссылки на интернет-страницы или доменные имена, которые содержат материалы с порнографическими изображениями несовершеннолетних и публикации о привлечении детей в роли исполнителей для участия в зрелищных мероприятиях порнографического характера; пропаганду употребления наркотиков и психотропных веществ, сведения о способах их производства и точках потребления; информацию о путях совершения самоубийства, а также призывов к совершению самоубийства; любую другую информацию, не допускаемую к распространению в России решениями судов.

Исходя из вышеизложенного, можно сделать вывод, что проблемы, касающиеся защиты несовершеннолетних от негативной информации, в самом деле, актуальны в наше время. Это подтверждает тенденция ужесточения контроля и ответственности за распространение такого рода материалов. Актуальность вопроса будет расти по мере развития информационных технологий в будущем и иных факторов, которые влияют на распространение негативной информации, угрожающей здоровью и развитию детей.

Уже на современном этапе Интернетом и другими видами коммуникаций становится невозможно управлять только на уровне национального законодательства, и для достижения определённых успехов в этом вопросе необходимо обсуждать данную задачу на международном уровне. Только общими усилиями международного сообщества, а не отдельных государств можно свести распространение негативной информации к минимуму. Необходимо разработать единые стандарты, в которых будет установлено, что считать вредной информацией для ребёнка, наладить определённую систему санкций за распространение негативной информации и общий подход для решения этой задачи.

Все основные способы защиты детей от негативного контента в разных странах можно занести в таблицу 1.

Таблица 1 – Мировой опыт по обеспечению защиты детей в сети Internet

Название страны	Меры по обеспечению защиты
США	Установка программных фильтров в учебных заведениях Установка кодирующего устройства на телевизоры Обучение подростков интернет-грамотности
Канада	Создание добровольного проекта «Cleenfeed Канада» Использование требований общих законов
Великобритания	Использование интернет-провайдерами фильтрации контента по умолчанию Использование фильтров в мобильной сети Фильтрация провайдерами общественных сетей Wi-Fi Система «Cleenfeed», работающая на основе «чёрных списков»
Китайская Народная Республика	Использование технологий защиты несовершеннолетних от негативной информации Организация Центра жалоб Создание проекта «Золотой щит»
Сингапур	Работает общегосударственный регулятор The Media Development Authority Министерство образования ограничивает доступ к «неугодному» контенту
Швеция	Использование DNS-фильтра интернет-провайдерами Ведение списка запрещённых сайтов полицией Швеции Запрет рекламы для детей младше 12 лет
Германия	Удаление нежелательного контента самими провайдерами
Россия	Ограничение доступа в Интернет для детей в общедоступных местах Использование системы «Единый реестр доменных имён»

Исходя из данных таблицы, можно сделать вывод о том, что помимо действующих законодательных актов и законов, в разных странах используются дополнительные меры обеспечения защиты детей от информации, способной нанести вред их физическому и психическому здоровью. В основном

это использование интернет-фильтров и «черных списков» нежелательных для просмотра сайтов.

1.4 Рекомендации по защите детей различных возрастных категорий от негативного контента

Таким образом, в мире придается большое значение защите малолетних детей и подростков от вредной для них информации в целях обеспечения их нормального физического и психологического развития, которое может быть нарушено или даже существенно повреждено неподходящим аудиовизуальным контентом.

На государство и общество должна быть возложена обязанность по выстраиванию четкой системы предупреждения получения детьми потенциально опасной для них информации. Конституцией России установлены обязанности государства защищать детей и родителей - заботиться о детях и воспитывать их (ч. ч. 1, 2 ст. 38). Конституцией также предусмотрена возможность ограничивать права и свободы человека и гражданина федеральным законом в той мере, в какой это необходимо для защиты нравственности, прав и свобод других лиц (ч. 3 ст. 55). В Федеральном законе от 27 июля 2012 года описаны основные правила о защите детей от информации, причиняющей вред их здоровью и развитию.

В рамках государственной программы в целях обеспечения необходимой защиты родители и лица, на которых возложена забота о детях, также должны иметь возможность получить информацию о том, может ли нанести вред доступная детям информационная продукция. Программой предусмотрено, как защитить детей от отрицательного воздействия СМИ, Интернета, телевидения, каким образом родители могут оградить детей и научить их правильно воспринимать информационные сообщения.

Родителям обычно выгодно, чтобы дети сидели у себя дома около компьютера, телевизора, чем идти с ними в кафе, кинозалы или кружки. Им не

стоит полагаться на защиту только на федеральном или местном уровнях. Часть ответственности лежит и на родителях.

Одним из главных течений в борьбе за информационную безопасность детей является просвещение родителей. По данным статистики, половина русских подростков знает о Всемирной паутине и может работать в ней гораздо лучше своих родителей. Уровень знаний родителей о программах и модулях по охране детей от вредной информации также чрезвычайно низкий. Сегодня почти все из них встают перед проблемой – как же ограничить доступ ребёнка к компьютеру, как ограничить время присутствия в Интернете и защитить от порно, наркотиков и матов? Присмотр за детьми в глобальной информационной сети именуется как «Родительский контроль».

Так какими способами можно защитить детей от нежелательной информации? Для этого существует определённый свод правил, который различается для каждой возрастной группы детей.

1.4.1 Дети возрастной группы от 6 до 11 лет

В сети Интернет ребёнок старается побывать на тех или иных сайтах, а может быть и чатах, на посещение которых он не получил бы позволения от мамы и папы. Потому родителям могут быть полезны те отчёты, которые даются программами по ограничению пользования Интернетом, то есть «Родительский контроль». В итоге у ребёнка не останется ощущения, что за ним ведётся постоянный контроль, но, родители будут всё еще знать, на какие сайты заходит их ребёнок. Дети в таком возрасте владеют большим чувством семьи, они часто бывают наивны и не сомневаются в авторитетах. Они обожают проводить время в сетевых играх и чатах, запрещенных родителями.

Программой предусмотрены советы по безопасности в сети Интернет:

1. Создайте перечень семейных правил посещения Интернета при участии детей и просите его соблюдения.

2. Обязывайте ребёнка придерживаться временных норм нахождения за компьютером. Покажите ребёнку, что вы следите за ним не от того, что вам этого хочется, а только потому, что вы переживаете об его сохранности и всегда готовы прийти к нему на помощь.

3. Компьютер с выходом в Интернет находится в общей комнате под наблюдением родителей.

4. Используйте средства блокировки ненужного контента как добавление к «Родительскому контролю».

5. Создайте семейный электронный ящик для того, чтобы дети не могли иметь собственные адреса.

6. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с поддержкой соответствующего программного обеспечения.

7. Приучите детей консультироваться с вами перед публикацией каких-либо материалов средствами электронной почты, регистрационных форм, чатов и профилей.

8. Дайте детям понять, что не нужно загружать различные файлы, программы или звуковые аудиодорожки без вашего ведома.

9. Не разрешайте детям пользоваться службами мгновенного обмена сообщениями.

10. В «белый» перечень интернет-страниц, которые разрешены для посещения, вносите лишь сайты с высокой репутацией.

11. Не забывайте разговаривать с детьми об их интернет-друзьях, как если бы речь зашла о друзьях в реальной жизни.

12. Приучите ребёнка объявлять вам обо всех опасностях или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами поведали вам о своих угрозах или тревогах. Похвалите их и предложите подойти ещё раз в похожих ситуациях.

1.4.2 Дети возрастной группы от 12 до 15 лет

В представленном возрасте дети, как правило, уже наслышаны о том, какая информация есть в Интернете. Абсолютно естественно то, что они желают это увидеть, прочитать, узнать. При этом не стоит забывать, что доступ к ненужным материалам можно просто блокировать с помощью средств «Родительского контроля».

Программой предусмотрены советы по безопасности в сети Интернет:

1. Создайте перечень домашних законов посещения Интернета при участии детей и просите его исполнения.
2. Просите своего ребёнка соблюдать принятые временные рамки нахождения за компьютером. Продемонстрируйте ребёнку, что вы следите за ним не потому, что хотите этого, а потому, что вы тревожитесь об его защищенности и в любой ситуации готовы ему помочь.
3. Компьютер с выходом в сеть полагается ставить в общей комнате под надзором родителей.
4. Используйте средства блокировки ненужного контента ровно как дополнение к «Родительскому контролю».
5. Не забывайте общаться с ребенком об их интернет-товарищах.
6. Настаивайте на том, чтобы дети ни в коем случае не принимали предложения на личные встречи с товарищами по Интернету.
7. Разрешайте детям заходить на сайты только из «белого списка», который составите совместно с ними.
8. Дайте понять ребенку, что не нужно никогда выдавать собственную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в сети Интернет.
9. Приучите детей не скачивать программы без вашего одобрения. Поясните им, что они имеют все шансы случайно загрузить вирусы или другое ненужное программное обеспечение.

10. Создайте для вашего ребёнка ограниченную учётную запись для работы на компьютере.

11. Приучите детей ставить вас в известность при любых тревогах или опасностях, которые могут настигнуть их в сети Интернет. Будьте спокойными и напомните детям, что они в безопасности, если сами сообщили вам о тревогах или опасностях. Похвалите их и порекомендуйте подойти снова в аналогичных случаях.

12. Проинформируйте детей о порнографии в Интернете.

13. Настаивайте на том, чтобы ребенок доверил вам доступ к своей электронной почте, чтобы вы убедились, что они не имеют переписок с незнакомцами.

14. Донесите до детей, что запрещено пользоваться сетью с целью хулиганства, распространения сплетен или угроз.

1.4.3 Дети возрастной группы от 16 до 17 лет

В данном возрасте школьники в полном объеме применяют поисковые машины, используют электронную почту, пользуются службами мгновенного обмена сообщениями, закачивают аудио- и видеофайлы. Юношам в данном возрасте больше нравится сметать все возможные ограничения, они хотят резкого юмора, увлекающих игр, иллюстраций «для взрослых». Девочки выбирают беседовать в чатах, при этом они наиболее восприимчивы к сексуальным домогательствам в сети Интернет. В рассматриваемом возрасте Отцу с матерью зачастую уже крайне трудно осуществлять контроль за своими детьми, так как об Интернете они уже понимают существенно больше собственных родителей. Тем не менее, в особенности немаловажно точно придерживаться принципов Интернет безопасности – договор между отцом с матерью и детьми. Помимо этого, следует как можно чаще смотреть отчёты о работе ребенка во Всемирной паутине. Необходимо сконцентрировать внимание в надобности содержания родительских паролей (паролей администра-

торов) в серьезной тайне и сосредоточить внимание на строгость данных паролей.

Программой предусмотрены советы по безопасности в сети Интернет:

1. Создайте перечень домашних законов посещения сети Интернет при участии школьников и попросите абсолютного его исполнения. Укажите список воспрещённых веб-сайтов («чёрный список»), время работы в Интернете, руководство по общению в сети Интернет (а также в чатах).

2. Компьютер с подсоединением к Интернету обязан стоять в общей комнате.

3. Не забывайте пообщаться с ребенком об его приятелях в Интернете, о том, чем они занимаются так, будто бы вы говорите о приятелях в реальной жизни. Узнавайте о людях, с которыми ребенок контактирует с помощью служб мгновенного обмена сообщениями, для того, чтобы удостовериться, что они знакомы с этими людьми.

4. Используйте ресурсы блокировки ненужного контента ровно как дополнение к обычному «Родительскому контролю».

5. Необходимо понимать, что за чаты пользуют ваши дети. Поощряйте применение модерируемых чатов и требуйте того, чтобы школьники никак не общались в приватном чате.

6. Настаивайте на том, чтобы дети ни в коем случае не соглашались на личные встречи с людьми из интернета.

7. Приучите ребенка никогда не предоставлять собственные данные средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

8. Приучите детей не скачивать на компьютер программы без вашего согласия. Дайте понять то, что есть риск нечаянно загрузить вирусные файлы или иное ненужное программное обеспечение.

9. Научите себя просматривать сайты, на которых бывают ваши дети.

10. Обсудите с ребенком проблемы, которые могут возникать с сетевыми азартными играми и их возможные риски. Напомните, что школьники не имеют права играть в подобные игры в соответствии с законом.

11. Научите ребенка не предоставлять в сети Интернет личного электронного адреса, не отвечать на подозрительные послания и применять особые почтовые фильтры.

12. Помогите уберечься от спама.

Государство в своей образовательной программе в основном обучает настройке защиты доступа в сеть Internet педагогов в школах и иных сотрудников образовательных учреждений. Но мало кто обучает этому самих детей, которые в будущем будут родителями, а также самих родителей.

Таким образом, изучив предметную область этого вопроса, международный опыт по защите детей, содержание государственных программ, выделив возможные виды негативной информации, был разработана система проведения мероприятий по теме «Обеспечение защиты детей от негативной информации в сети Internet». Список мероприятий состоит из:

1. Анкетирование.
2. Обсуждение основных вопросов интернет-безопасности.
3. Ознакомление с Федеральными законами и нормативными актами.
4. Ознакомить с правилами работы в сети Internet.
5. Выдать материал для самостоятельного выполнения лабораторного практикума.

2 ОРГАНИЗАЦИЯ ЗАЩИТЫ ДЕТЕЙ ОТ НЕГАТИВНОЙ ИНФОРМАЦИИ В СЕТИ INTERNET

2.1 Методические рекомендации по обеспечению защиты детей

В качестве методических рекомендаций по защите детей мною были разработана система мероприятий, которые будут проводиться в форме обмена мнениями между обучающимися учебно-технического центра «Омега - 1».

Задачи проводимых мероприятий:

- повысить уровень осведомлённости в вопросах интернет-безопасности;
- повысить уровень осведомлённости учащихся о нормах Федерального закона и других правовых нормативных актов.

Перечень мероприятий по организации защиты детей:

- провести анкетирование обучающихся;
- проинформировать обучающихся о правилах работы в сети Интернет;
- проинформировать обучающихся о Федеральных законах и нормативных актах;
- организовать обучение обучающихся по настройке программно-аппаратного обеспечения;
- проведение круглого стола по выполненному лабораторному практикуму.

Перед началом обмена мнениями необходимо провести анкетирование, которое выявит уровень осведомлённости обучающихся об угрозах, которые подстерегают детей в сети Internet (приложение Д).

Повышение уровня осведомлённости будет происходить в виде обсуждения наиболее важных вопросов, которые затрагивают информационную безопасность и защищённость ребёнка (приложение Б).

В качестве основных правовых и нормативных актов будет приведён список основных Федеральных законов Российской Федерации по защите детей от информации, которая может нанести вред их здоровью и развитию (приложение В).

Также был разработан список основных правил по безопасной работе в сети Internet (приложение Г).

Основным мероприятием является обучение настройке оборудования и программного обеспечения в рамках лабораторного практикума, который обучающиеся будут выполнить самостоятельно.

Задачи практикума:

- дать знания о способах ограничения доступа к сети Internet;
- повысить навыки самообучения;
- увеличить запас теоретических и практических знаний, повысить мотивацию к углублению полученных знаний, использования знаний, приобретенных во всевозможных образовательных сферах;
- развить творческие способности учащихся.

Работа в практикуме рассматривается на трёх уровнях:

- первый уровень – «репродуктивный» (обучающийся осознает, способен повторить без погрешностей);
- второй уровень – «интерпретация» (обучающийся осознает, способен использовать с изменениями в похожих условиях);
- третий уровень – «изобретение» (обучающийся способен без чужой помощи решить поставленную перед ним практическую задачу).

При проведении лабораторного практикума обучающиеся без помощи других проделывают лабораторные работы.

Лабораторные практикумы важны для обучения. Обучающиеся приобретают опыт работы с определёнными типами оборудования, который будет

полезен им в жизни. В отсутствии практикумов обучение не может считаться полным. По итогам самостоятельного изучения лабораторного практикума предлагается организовать обмен мнениями.

2.2 Лабораторный практикум, как компонент профессиональной подготовки

Лабораторный практикум это потенциально наиболее значимый и результативный компонент естественнонаучной, общей профессиональной и специальной подготовки в области техники и технологий, предназначенный для приобретения навыков работы на реальном оборудовании, с аналогами которого будущему специалисту, возможно, придется иметь дело в своей практической деятельности [2].

Лабораторный практикум «Обеспечение защиты детей от негативной информации в сети Internet» разработан для самостоятельного изучения в системе дополнительного образования обучающихся в учебно-технологическом центре «Омега – 1». Данный лабораторный практикум содержит 5 лабораторных работ. В конце каждой лабораторной работы есть вопросы для самопроверки, а также задание для самостоятельного выполнения.

Лабораторный практикум может быть выполнен в компьютерном классе центра «Омега – 1». Данный вид занятий эффективен тем, что:

- компьютерные классы центра «Омега – 1» оснащены всем необходимым техническим оборудованием;
- учащиеся могут выполнять практикум, советуясь друг с другом.

Лабораторный практикум также можно выполнить в домашних условиях, имея базовый набор оборудования: компьютер, выход в сеть Internet, роутер.

Лабораторный практикум «Обеспечение защиты детей от нежелательной информации в сети Internet» содержит в себе вопросы для самоконтроля после каждой лабораторной.

Благодаря детальному объяснению и максимальной наглядности, обучающиеся должны овладеть умением создавать правила защиты от нежелательного контента на оборудовании, а также применять это умение в своей практической деятельности.

Лабораторный практикум «Обеспечение защиты детей от нежелательной информации в сети Internet» осуществляется в рамках самостоятельного изучения в сфере дополнительного образования.

К электронным учебным практикумам предъявляется целый ряд требований. Выделяют дидактические и технологические требования [2].

К дидактическим требованиям относят:

1. Требование научности обозначает необходимость обеспечения необходимой глубины, корректности и научной достоверности изложения содержания учебного материала с учетом последних научных достижений.

2. Требование доступности обозначает потребность установления степени теоретической сложности и глубины изучения учебного материала согласно возрастным и личным отличительным чертам обучающихся.

3. Требование обеспечения проблемности обучения обуславливается самой сущностью и характером учебно-познавательной работы. Когда обучающийся встречается с проблемной ситуацией, которая требует разрешения, его мыслительная активность увеличивается.

4. Требование обеспечения наглядности означает потребность учета эмоционального восприятия исследуемых объектов, их макетов либо моделей и их личное наблюдение за обучающимися. Применение мультимедиа составляющих гарантирует полисенсорность обучения с задействованием почти всех каналов восприятия информации человеком.

5. Требование систематичности и последовательности означает обеспечение последовательного усвоения обучающимися определенной системы знаний в изучаемой предметной области. Необходимо, чтобы знания, умения и навыки формировались в определенной системе, в строго логическом порядке и находили применение в практической жизнедеятельности. При этом

системообразующее значение имеет не только «логика предмета», но и в первую очередь «логика деятельности» [2].

Для этого нужно:

- предъявлять учебный материал в систематизированном и структурированном виде;
- принимать во внимание не только ретроспективы, но и возможности формируемых знаний, умений и способностей при организации каждой порции учебной информации;
- иметь в виду межпредметные взаимосвязи исследуемого материала, соответствующие отличительным чертам вида деятельности;
- основательно обдумывать порядок подачи учебного материала и обучающих воздействий, аргументировать каждый этап по отношению к обучающемуся;
- выстраивать процесс получения знаний в очередности, определяемой логикой преподавания, в свою очередь характеризуемой логикой предстоящей (нынешней) профессиональной работы;
- обеспечивать связь информации с практикой путем увязывания содержания и методики обучения с личным опытом обучающегося, подбором примеров, создания содержательных игровых моментов, предъявления заданий практического характера, экспериментов, моделей реальных процессов и явлений [3].

Требование прочности усвоения знаний: с целью прочного усвоения учебного материала максимальное значение имеют полное осознание данного материала, его усвоение.

Требование единства образовательных, развивающих и воспитательных функций обучения. Электронные издания, применяемые на практических занятиях, должны предоставлять обучаемому все имеющиеся сведения о теме, цели и порядке проведения занятий, контролировать знания каждого обучаемого, выдавать обучаемому информация о правильности ответа; предъявлять необходимый теоретический материал или методику решения

задач; осуществлять обратную связь в режиме «педагог – электронное издание – обучаемый» [3].

Преподаватель считается одной из важнейших составляющих обучения. От его мастерства поднести свою информацию и провести занятия будет зависеть то, как обучающиеся усвоят материал.

К технологическим требованиям относятся:

- открытость – право, в какое угодно время внести изменения в практикум;
- наличие развитой организации поддержки (с её помощью обучающийся сможет разрешить задачу и установить образовавшиеся затруднения);
- многоуровневая систематизация учебного материала (наличие банка заданий);
- обеспечение двухстороннего диалога;
- шанс вернуться обратно;
- интуитивный доступный интерфейс;
- надёжность работы, системная целостность.

Лабораторный практикум призван разрешить следующие проблемы:

Практическое фиксирование приобретенных теоретических знаний.

Приобретение навыков самостоятельной работы с настоящим оборудованием.

Планирование и постановка целей для настройки оборудования и аппаратно-программного обеспечения.

Выбор оборудования с целью выполнения поставленных целей.

Обработка и объяснение итогов настройки оборудования и софта.

Сопоставление результатов теоретического материала с данными настройки.

В идеальной постановке образовательного процесса для повышения эффективности усвоения учебного материала, каждый объект изучения в рамках учебной темы в обязательном порядке должен снабжаться всеми не-

обходимыми компонентами теоретического, практического, модельного и экспериментального изучения [3].

Лабораторный практикум – важное звено учебного процесса. В процессе лабораторного практикума обучающиеся встречаются с самостоятельной практической работой в определенной сфере. Лабораторные занятия, ровно, как и прочие разновидности практических занятий, считаются средним звеном между углубленным теоретическим трудом обучающихся на лекциях, семинарах и использованием знаний на практике. Данные занятия успешно совмещают части теоретического исследования и практической деятельности.

В процессе выполнения лабораторных работ, обучающиеся, лучше всего понимают программный материал, потому что почти все определения и формулировки, которые казались отвлеченными, становятся достаточно ясными, совершается соприкосновение теоретических знаний с практикой, что в целом способствует уяснению трудных вопросов науки и становлению обучающихся как будущих профессионалов.

Я многому научился благодаря лабораторным практикумам. За период обучения на различных дисциплинах было большое количество разных практикумов, которые развивают, формируют, закрепляют различные знания, умения и навыки.

2.3 Требования к организации лабораторных практикумов

Современный ФГОС ВО никак не регламентирует содержательную часть лабораторного практикума, оговаривая, в лучшем случае, его объем в часах по сравнению с теоретической частью темы. Отсутствует и сколько-нибудь серьезный государственный контроль и аттестация используемого в различных учебных заведениях лабораторного оборудования. Необходимо повышать статус лабораторных практикумов. Поэтому выбор объектов лабо-

раторного практикума и определение его содержания часто происходят без учета реальных потребностей учебного процесса [3].

Главным условием проведения лабораторных практикумов является обеспечение техническим и методическим материалом. К этим материалам относятся:

1. Специально оборудованное помещение, оснащённое необходимым техническим оборудованием.
2. Наличие методических пособий по выполнению лабораторных работ, а так же список дополнительной полезной литературы.

Лабораторный практикум разработан студентом, обучающимся по специальности «Компьютерные технологии автоматизации и управления». Практикум будет применяться в системе дополнительного образования.

Лабораторный практикум «Обеспечение защиты детей от негативной информации в сети Internet» разработан для выполнения не только в учебных лабораториях, но и в домашних условиях. Для хорошей организации практикума необходимо современное оборудование, которое не является труднодоступным.

В настоящий момент оборудование компьютерного класса учебно-технического центра «Омега – 1» отвечает всем современным требованиям. Оно в полной мере может быть использовано для выполнения задания лабораторного практикума.

2.4 Структура лабораторного практикума

Лабораторный практикум содержит в себе: аннотацию, практический блок, средства контроля знаний (вопросы для самопроверки, задания для самостоятельного выполнения), список рекомендованной литературы и глоссарий.

Аннотация включает в себя: предназначение электронного лабораторного практикума, педагогический адрес, цель и задачи.

Практический блок лабораторного практикума складывается из пяти лабораторных работ.

Лабораторная работа – одна из главных форм организации учебного процесса. Её смысл состоит в выполнении обучающимися учебных заданий под наставлением педагога для усвоения научно-теоретических базы, получения навыков, опыта творческой и самостоятельной работы.

В описании лабораторной деятельности формируется содержание, объем и последовательность ее исполнения. Оно включает заголовочную и основную части.

Заголовочная часть содержит в себе:

1. Номер лабораторной работы в изучаемом курсе;
2. Формулировку проблемы и целей лабораторных работ.

Тема работы должна ясно указывать на предмет и аспекты практического изучения.

Структура лабораторного практикума такова: аннотация, содержание, пять лабораторных работ, вопросы для самопроверки, задания для самостоятельного выполнения, список полезной литературы, глоссарий. Лабораторные работы включают в себя цель работы, длительность, оборудование, порядок выполнения работы, последовательность выполнения действий с подробным объяснением, практическую часть, контроль знаний в виде вопросов для самопроверки и задания для самостоятельного выполнения.

Цель работы должна полностью отражать её познавательную и практическую адресность. Основная часть практической (лабораторной) работы включает:

- технологию выполнения работы;
- выполнение заданий по инструкции;
- задания для самостоятельного выполнения;
- вопросы для самопроверки.

Задания для лабораторной работы представлены в виде списка последовательных операций, которые необходимо выполнять для более полной реализации целей и задач.

Технология выполнения работы содержит в себе последовательность действий и способов, обеспечивающих более точное и правильное выполнение лабораторной работы.

Вопросы для самопроверки предназначены для самостоятельной проверки надёжности усвоения знаний и умений, полученных в процессе выполнения лабораторного практикума.

В заданиях для самостоятельного выполнения указано задание, которое будет отражать в себе весь материал, описанный в лабораторной работе.

В полезных ссылках указаны электронные ресурсы и учебники, необходимые к прочтению для более полного усвоения предложенного материала.

Одно из наиболее распространенных средств для просмотра файлов в формате PDF считается Adobe Acrobat. Формат файлов PDF (Portable Document Format) был создан с целью сохранения и распространения отпечатанной продукции. Разработала такой формат фирма Adobe Systems Incorporated, которая через некоторое время, представила его в публичном доступе.

Сегодня формат PDF является самым простым и популярным форматом для полиграфической продукции, огромное количество книг и документов хранится и распространяется именно в этом формате. Файлы PDF занимают мало места и очень удобны в использовании [3].

Adobe Acrobat – полнофункциональный издательский проект для публикации документов, распространяемых как в отпечатанном, так и в электронном виде в формате PDF. Проектом разрешено пользоваться для публикации в формате PDF практически любого формата документов (Word, Excel, PageMaker, InDesign, Illustrator, CorelDraw, Photoshop и т.д.), сохраняя при этом нужный вид и содержание начального файла.

PDF файлы можно прочесть на каждом персональном компьютере в какой угодно операционной системе, в том случае, если на нем установлено бесплатно распространяемое программное обеспечение AdobeReader.

При просмотре PDF документа применяются следующие ключевые функции:

Открытие PDF документа:

- команда меню File – Open (Файл – Открыть), использование кнопки на панели «Файл», двойной щелчок по иконке PDF файла;
- можно открыть одновременно несколько файлов, выделяя их при нажатых клавишах CTRL или SHIFT;
- имена пяти недавно просматривавшихся файлов отображаются в нижней части меню File;
- при открытии одновременно нескольких документов удобно разместить их окна каскадом (команда Window – Cascade) или мозаикой (команда Window – Tile).

Навигация по документу:

- макеты страниц, позволяющих за очень короткий срок переходить на необходимую страницу публикации;
- список закладок, сделанных в тексте, дает возможность моментально переключаться на необходимую часть текста;
- активные области, применяемые подобно web-ссылкам, дают возможность сформировать активное содержание публикации.

Кнопка «Создать PDF» (Create PDF) вызывает меню, содержащее последующие команды:

- From File (Из файла). Щелкните по представленной кнопке, выберите документ на вашем компьютере, который необходимо превратить в PDF файл;
- From Multiple Files (Из нескольких файлов). Щелкните по данной кнопке и подберите ряд файлов для того, чтобы преобразовать их в PDF документ. Файлы могут оказаться разного формата – дополнения Microsoft

Word, Post Script файлы, графические файлы. Из всех этих файлов можно сформировать единый многостраничный PDF документ;

- From WebPage (Из Web-страницы). Щелкните по представленной кнопке, а далее введите URL в диалоговом окне этой веб-страницы, которую нужно преобразовать в PDF документ. Уже после преобразования страницу допускается изменять, выполнив команды меню Advanced –Web Capture (Дополнительные возможности – Захват Web-страницы);
- FromScanner (Со сканера). Дает возможность формировать PDF документ из изображения, полученного со сканера;
- FromClipboardImage (Из буфера обмена). Эта кнопка нужна для получения файла из буфера обмена, куда ранее были скопированы материалы, созданные в другом приложении.

Создание закладок:

Закладка предполагает текстовую ссылку на вкладке Закладки (Bookmarks) и применяется с целью перемещения в определенный участок файла. Для того, чтобы создать закладку в документе, проделайте последующие действия:

Откройте окно навигации и переключитесь на вкладку Закладки.

Выделите закладку, под которой вы хотите разместить новую. В случае если вы не определите место для будущей закладки, то она окажется последней в списке.

При помощи инструмента Hand (Рука) либо команд меню View (Вид) перенеситесь в ту часть файла, на которую станет ссылаться новая закладка.

Щелкните по кнопке Create New Bookmark (Создать новую закладку) либо щелкните по кнопке Options (Опции) и выберите команду New Book mark (Новая закладка) из выпадающего меню.

Введите название новой закладки и нажмите клавишу Enter.

Интерфейс электронного практикума должен быть интуитивно понятным. Такие объекты, как панель навигации, основной текст с иллюстрациями

сгруппированы в определенных зонах и пропорционально размещены на экране.

Лабораторный практикум «Обеспечение защиты детей от негативной информации в сети Internet», сделанный в рамках выпускной квалификационной работы по специальности «Компьютерные технологии автоматизации и управления в электроэнергетике (по отраслям)» является структурированный документ в формате PDF.

Согласно принципу размеренного распределения по экрану оптической тяжести изображения, любые структурные элементы страницы расположены так, что в результате уравновешивают друг друга.

Согласно принципу целостности, все составляющие смотрятся взаимосвязано, верно соотносятся согласно размеру, форме и цвету. Для достижения целостности использовались поля (для заголовков, важных замечаний и т.п.).

Так как этот электронный практикум по большей части нацелен на самостоятельную работу, в нем организована довольно удобная навигация. Описанная выше типовая структура реализована в лабораторном практикуме по теме «Обеспечение защиты детей от негативной информации в сети Internet».

2.5 Наполнение содержания лабораторного практикума

Данный лабораторный практикум содержит цикл из пяти лабораторных работ.

Каждая работа включает в себя:

- описание задания;
- пошаговые инструкции по выполнению;
- контроль усвоения знаний (вопросы для самопроверки);
- задание для самостоятельного выполнения.

В качестве контроля после выполнения лабораторных работ необходимо ответить на вопросы для самоконтроля. Обучающийся сам решает может ли он приступать к следующей лабораторной работе или нет.

Ниже представлено подробное описание первой лабораторной работы. Последующие лабораторные работы сделаны по такой же структуре. Далее приводится краткое описание всех лабораторных работ.

Данная лабораторная работа посвящена созданию учётной записи «ребёнок» и настройке «Родительского контроля» на операционной системе Windows 8.1. После её выполнения обучающийся будет знать основные функции «Родительского контроля», будет уметь создавать новые учётные записи, устанавливать параметры.

Лабораторная работа № 1

Тема: «Создание учётной записи «Ребёнок». Установка параметров родительского контроля».

Цель:

- научиться создавать учётную запись «Ребёнок»;
- изучить возможности родительского контроля на Windows 8.1;
- установить параметры ограничений для учётной записи учащегося.

Длительность: 180 минут

Оборудование: Компьютер с операционной системой Windows 8.1, доступ к сети Internet

Порядок выполнения работы: работа содержит описательную часть и задания для самостоятельного выполнения. Задания выполняются непосредственно в ходе прочтения содержания.

1. Создание учётной записи

В первую очередь, «Родительский контроль» на Windows представляет собой создание учётной записи ребёнка, которая будет работать по установленным администратором правилам. Чтобы «Родительский контроль» был надёжным, необходимо на все учётные записи установить пароль. В противном случае учащийся может войти через учётную запись администратора и

снять все установленные запреты в «Родительском контроле». На учётную запись учащегося пароль ставить не обязательно.

Задание 1

Для того чтобы создать новую учётную запись, выполните следующие действия:

1. Зайдите в «Панель управления». Для того чтобы туда зайти, нажмите WIN() + X (английская буква) и выберите пункт «Панель управления» (рисунок 1). Данная комбинация работает как на русской раскладке клавиатуры, так и на английской.

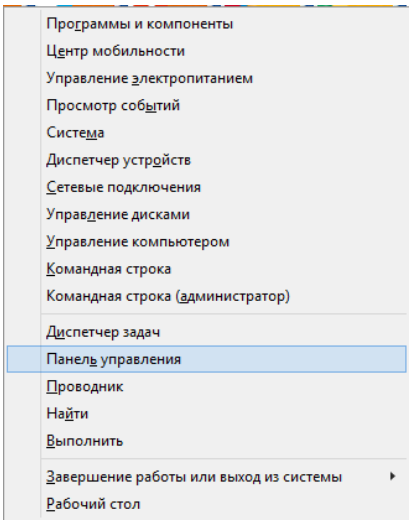


Рисунок 1 – Всплывающее меню свойств

.

2. Выберите раздел «Учётные записи и семейная безопасность». Щёлкните левой кнопкой мыши по «Учётные записи пользователей». В появившемся окне выберите «Управление другой учётной записью» и в последнем окне выберите пункт «Добавить нового пользователя в окне ”Параметры компьютера”» (рисунок 2).

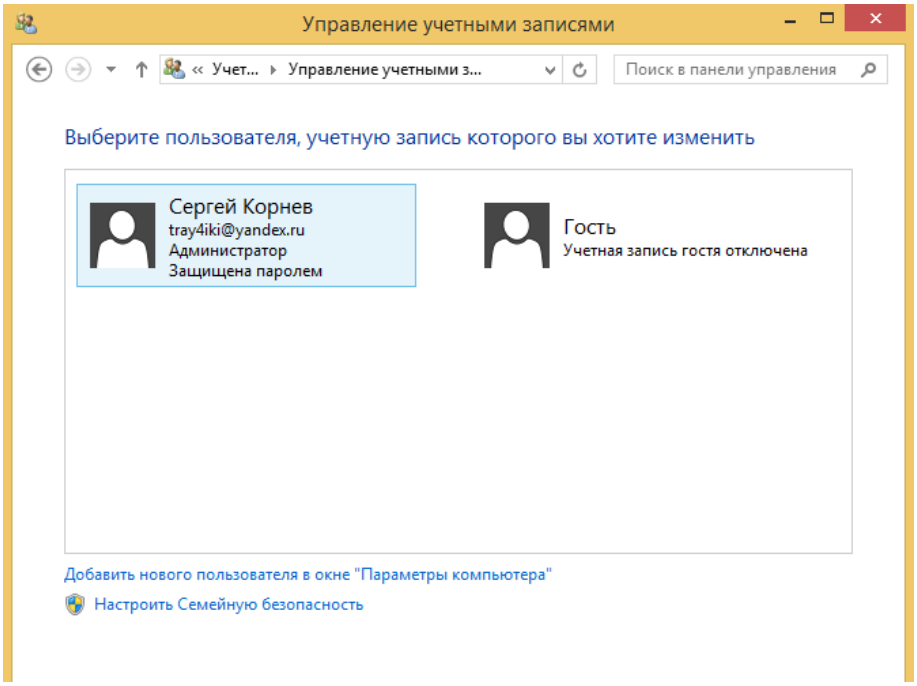
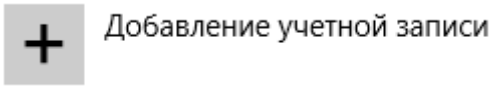


Рисунок 2 – Окно «Управление учётными записями»

3. В открывшемся окне выберите пункт «Добавление учётной записи».



4. Следующим действием система предложит вам вписать адрес электронной почты. Нам это не нужно, и мы выбираем «Добавить учётную запись ребёнка» – «Добавить учётную запись ребёнка без адреса электронной почты».

5. Далее вписываем имя учётной записи и, если возникает такая необходимость, устанавливаем пароль (рисунок 3). Как говорилось ранее, пароль на учётную запись ребёнка устанавливать не обязательно.

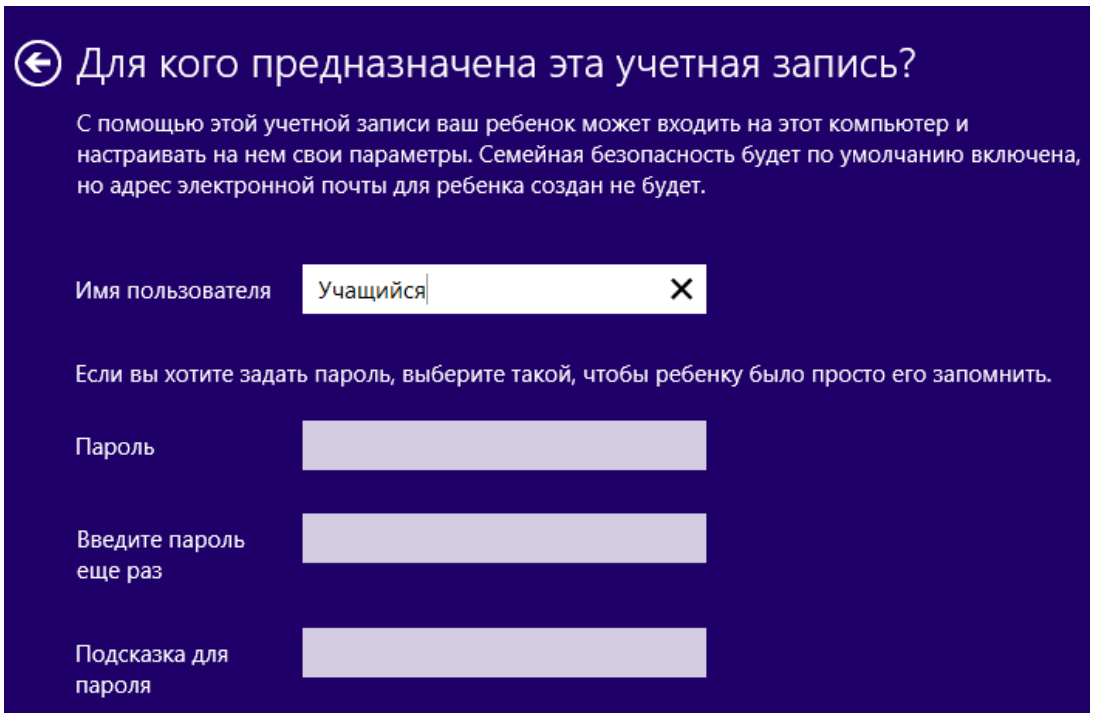
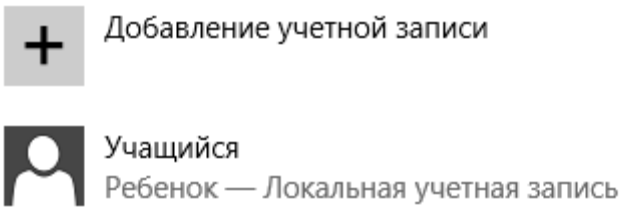


Рисунок 3 – Создание новой учётной записи ребёнка

6. После того, как имя пользователя было введено, нажимаем «Далее». В появившемся окне нажимаем «Готово». После происходит завершение создания учётной записи.



2. Установка параметров родительского контроля

Создав учётную запись ребёнка, мы можем приступать к настройке параметров доступа. Родительский контроль Windows обладает следующими параметрами:

- веб-фильтр – ограничение просмотра веб-сайтов в интернете пользователем;
- ограничение по времени – ограничение времени, когда пользователь может пользоваться компьютером;

- ограничение на игры и приложения из Магазина Windows– управление доступом по категории или названию;
- ограничения на классические приложения – управление приложениями, разрешенными на компьютере.

Задание 2

1. Для того чтобы перейти в окно выбора действий, разрешённых пользователю, необходимо зайти в «Панель управления» – «Учётные записи и семейная безопасность» – «Семейная безопасность».

2. Вы попадаете в окно, в котором вам будут показаны все учётные записи, созданные на этом компьютере. Выберите ту учётную запись, к которой вы хотите применить семейную безопасность. В нашем случае это запись «Учащийся» (рисунок 4).

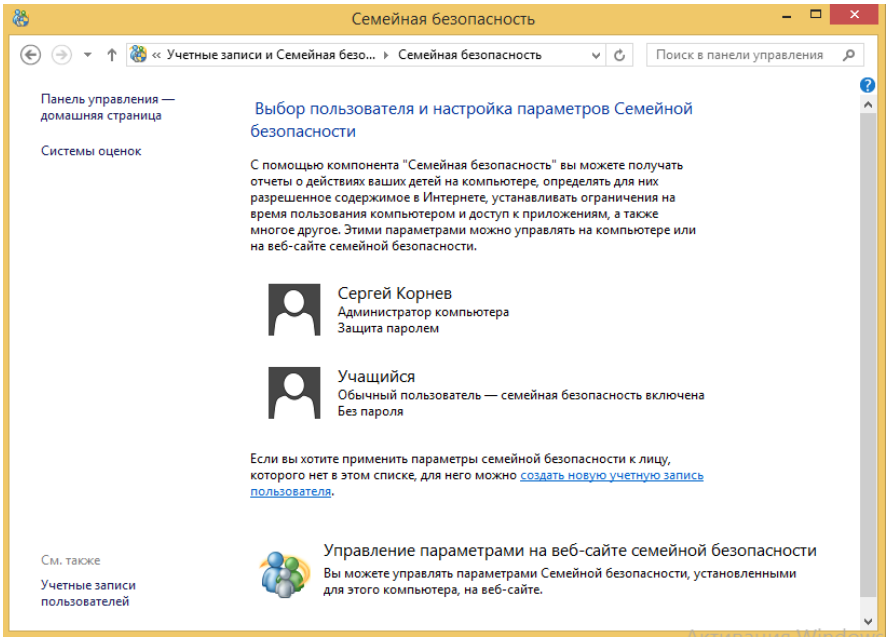


Рисунок 4 – Выбор учётной записи в окне «Семейная безопасность»

3. Выбрав пользователя, мы попадаем в окно параметров пользователя. Именно в этом окне находятся все те функции, которые описывались выше (рисунок 5).

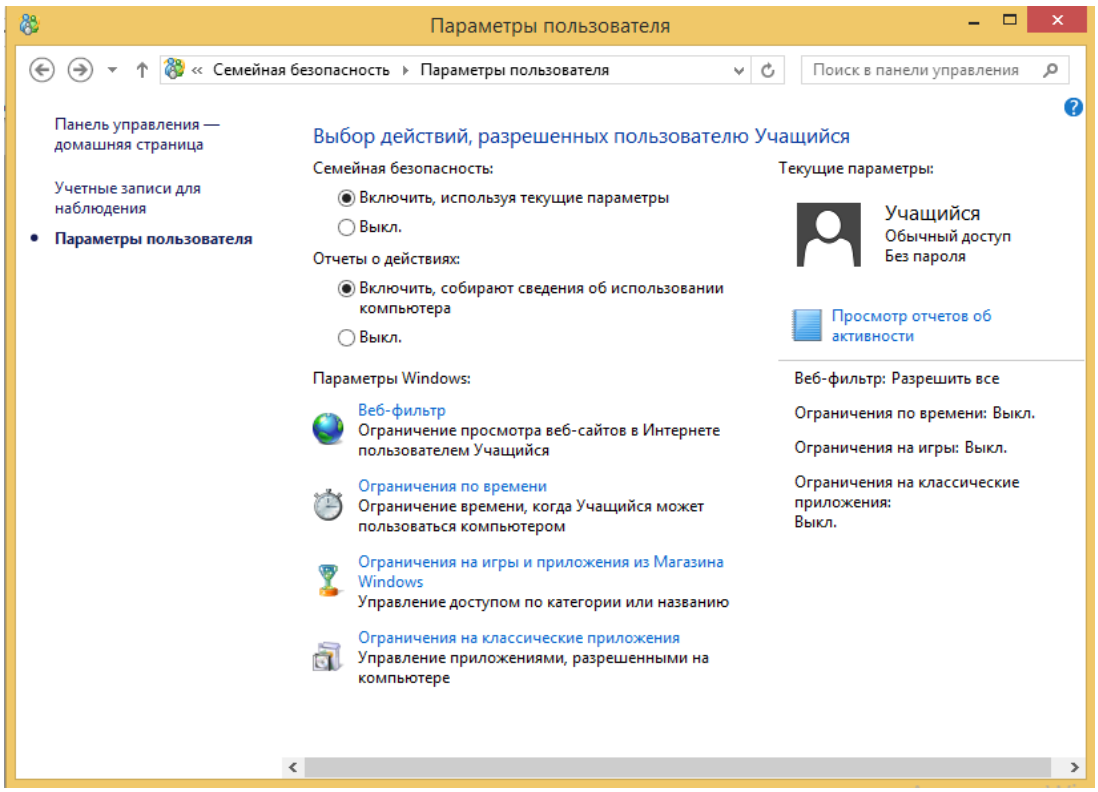


Рисунок 5 – Окно «Параметры пользователя»

Задание 3

Начнём с установки параметров веб-фильтра.

1. Левой кнопкой мыши выберите «Веб-фильтр» из списка «Параметры Windows».

2. Веб-фильтр нам предложит просмотр любых веб-страниц или же только те страницы, которые будут разрешены администратором. Так как мы создаем ограничение для учащихся, то нам следует выбрать второй пункт (рисунок 6).

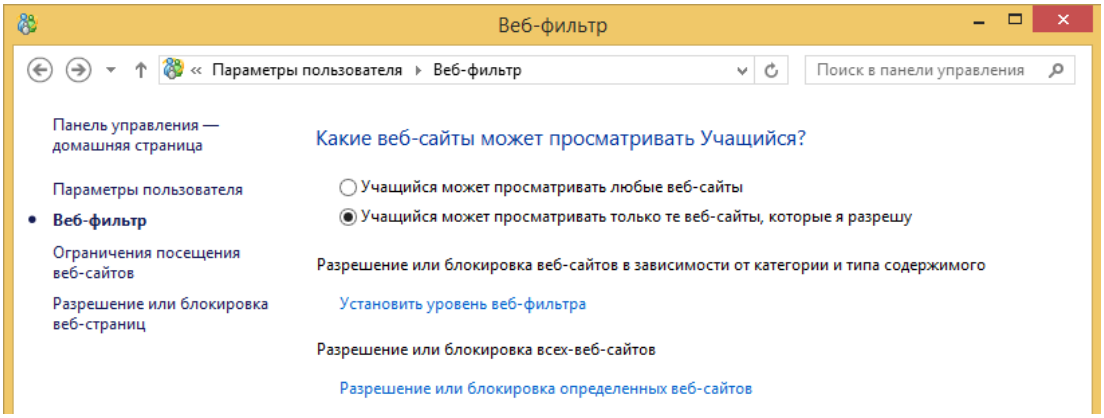


Рисунок 6 – Функции «Веб-фильтра»

3. После этого мы можем установить уровень веб-фильтра. Перейдя туда, мы видим различные уровни ограничения. Устанавливая уровень для учащегося, мы понимаем, что доступ в интернет ему будет разрешён только на конкретные сайты, которые администратор впишет в список. Поэтому установим уровень «Только из списка разрешений». Стоит отметить тот факт, что после выбора этого пункта при пустом списке разрешённых сайтов, пользователю будет запрещён просмотр каких-либо веб-страниц. После этого нажимаем стрелочку назад, чтобы вернуться в меню веб-фильтра (рисунок 7).

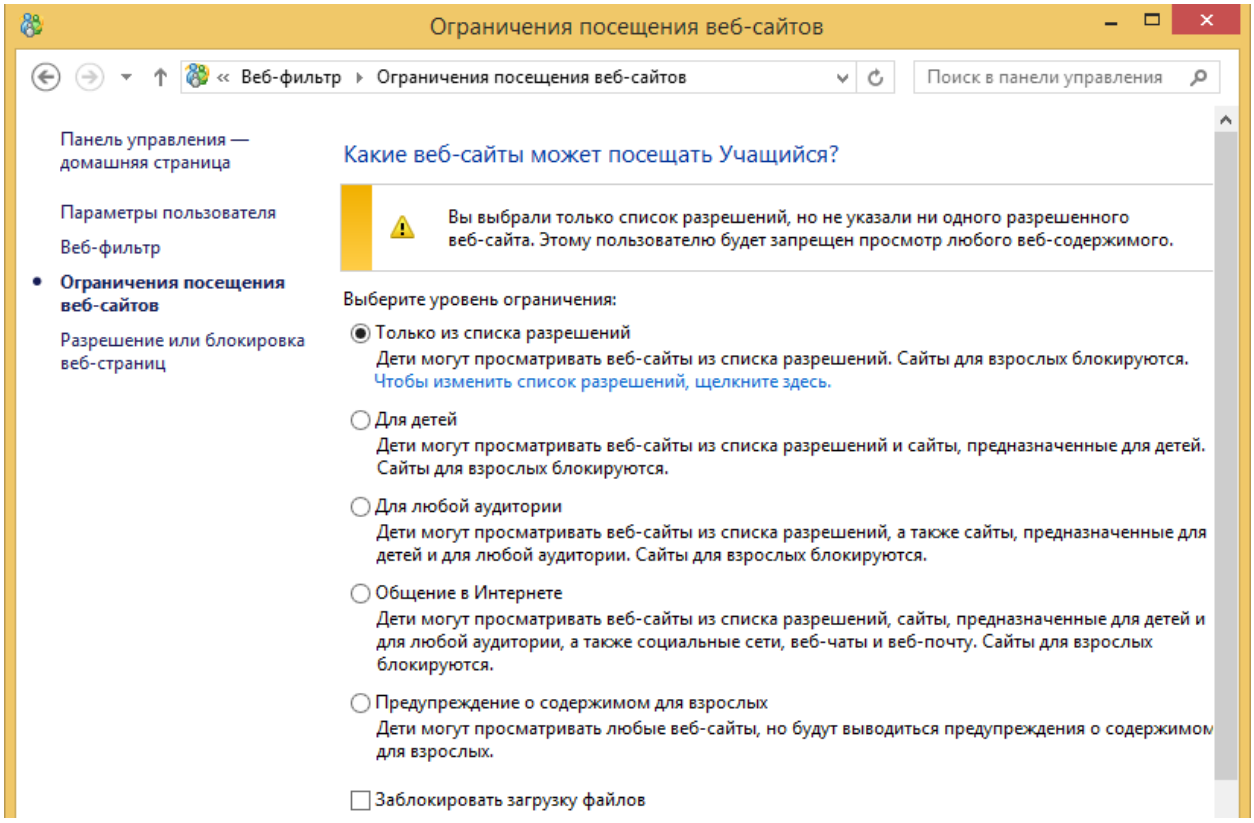


Рисунок 7 – Окно «ограничения посещения веб-сайтов»

4. Далее создадим список тех сайтов, которые будут доступны для просмотра с учётной записи учащегося. Для этого перейдём в пункт «Разрешение или блокировка веб-страниц». В этом окне (рисунок 8) нам предлагают ввести веб-сайт и определить, будет ли он заблокирован или наоборот – разрешён.

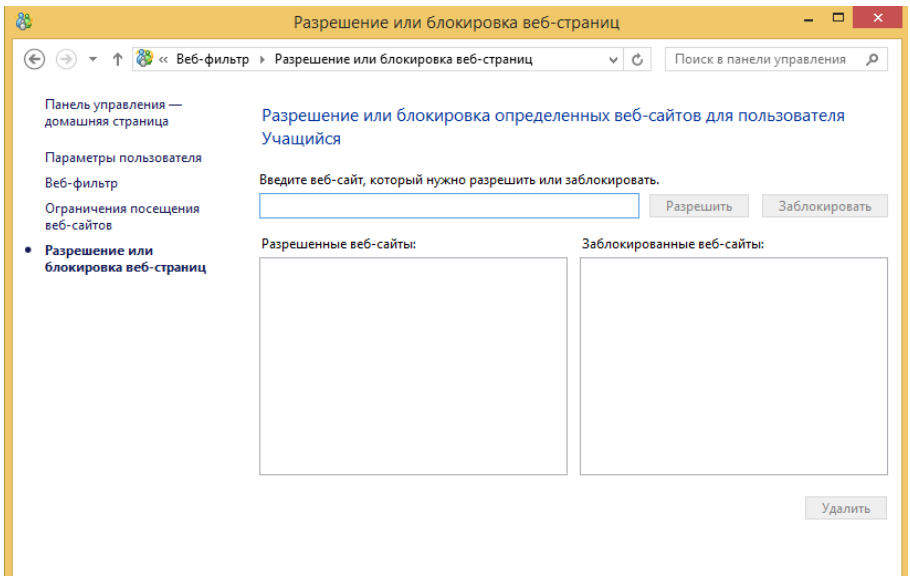


Рисунок 8 – Окно «Разрешение или блокировка веб-страниц»

Задание 4

Далее разберём функцию «Ограничения времени».

1. Нажимаем левой кнопкой мыши по «Ограничения времени».
2. Выберите раздел «Установить лимит времени».
3. На выбор вам будет предоставлено пользование компьютером весь день, либо пользование компьютером столько времени, сколько вы разрешите. Так как нам необходимо поставить ограничение, выбираем второй пункт (рисунок 9).

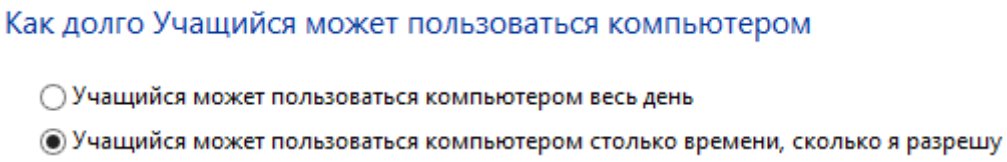


Рисунок 9 – Выбор ограничения по времени

4. Далее выберем лимит времени в рабочие дни и в выходные. Можно выставить лимит, применимый ко всем дням, а можно раскрыть список и поставить разное значение лимита в определённые дни (рисунок 10).

Рисунок 10 – Настройка лимита времени

5. Кроме задания лимита времени, можно установить «Запретное время». Чтобы перейти к его установке, нажмите левой кнопкой мыши на список функций, который находится в левом верхнем углу (рисунок 11).

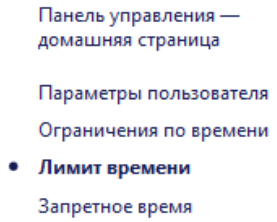


Рисунок 11 – Список функций окна «Ограничение по времени»

6. Войдя в настройки запретного времени, выберите пункт «учащийся может пользоваться компьютером только в промежутки времени, которые я разрешу». Перед вами появится поле с днями недели, временем суток и ограничительным полем. Для того чтобы ограничить пользование, компьютером в определённое время, необходимо установить курсор мыши в нужном вам квадрате на поле и, зажав левую кнопку мыши, потянуть. Например, вам необходимо ограничить пользование компьютером в среду во временной промежуток с 9-00 утра до 13-00 дня. Это будет выглядеть следующим образом (рисунок 12).

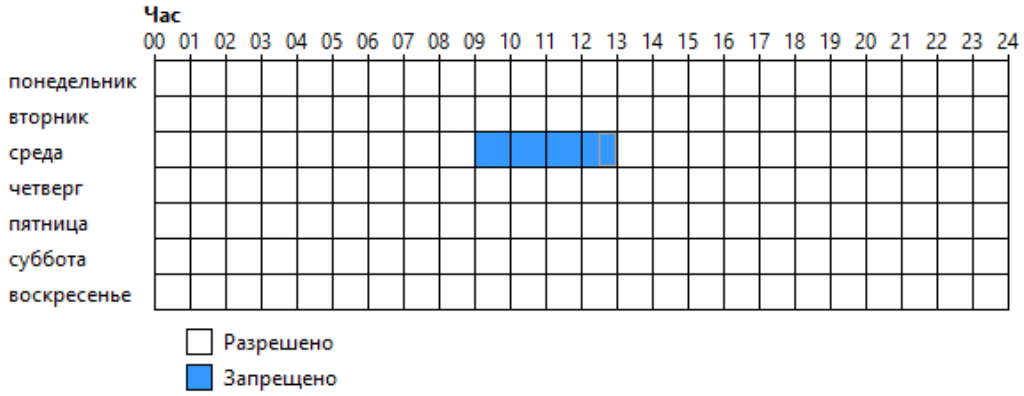


Рисунок 12 – Ограничительное поле с днями недели и временем суток

Задание 5

Перейдём к установке параметров «Ограничения на классические приложения». Под этими приложениями понимаются все приложения, установленные вами на компьютер.

1. Из списка предложенных параметров выбираем «Ограничения на классические приложения».

2. По аналогии со всеми другими параметрами, Windows нам предложит пользование всеми приложениями, либо теми, которые разрешит администратор. Выбираем второй пункт (рисунок 13).

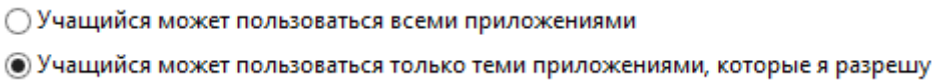


Рисунок 13 – Выбор ограничения приложений

3. После того, как вы выбрали этот пункт, компьютер начнёт сбор информации об установленных вами приложениях. После чего он выдаст вам список всех этих приложений (рисунок 14).

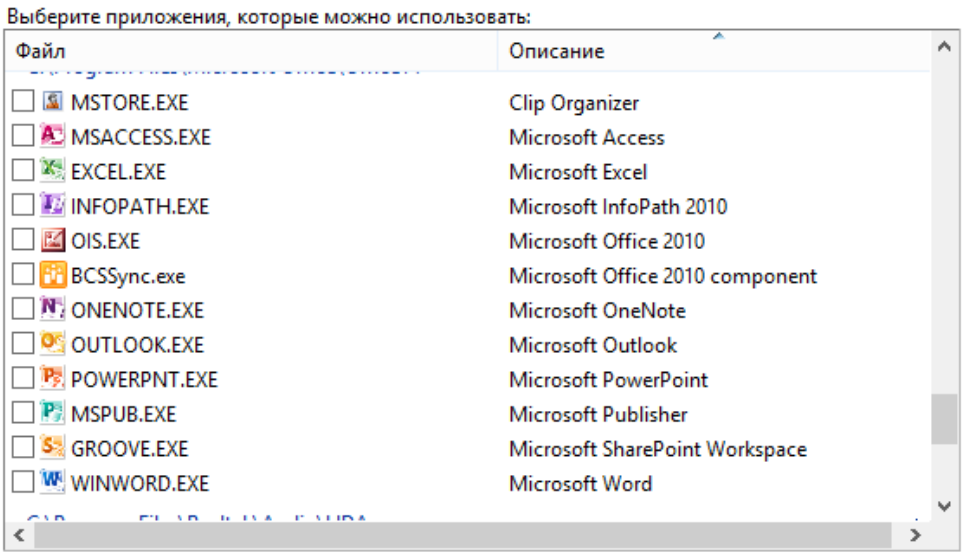
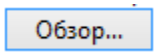


Рисунок 14 – Список приложений компьютера

4. Для того чтобы выбрать те приложения, которыми можно будет пользоваться учащемуся, необходимо поставить галочку рядом с нужными приложениями.

5. Если приложение не было найдено, его можно добавить самому. Для этого необходимо нажать на кнопку «Обзор»  и вручную указать путь к приложению.

Задание 6

Помимо всех этих параметров, Windows предусматривает просмотр отчёта активности пользователя (рисунок 15).

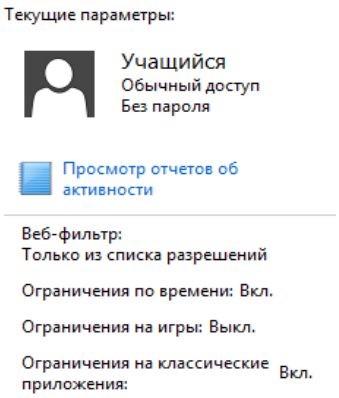


Рисунок 15 – Список текущих параметров пользователя

1. Зайдите в «Просмотр отчётов об активности» и проанализируйте, что можно увидеть в этих отчётах.

Вопросы для самоконтроля

1. Комбинация клавиш, с помощью которых можно открыть «Панель управления»?
2. Обязателен ли пароль на учетной записи «Учащийся» и почему?
3. Перечислите, какими основными параметрами обладает «Родительский контроль» в Windows 8.1?
4. Настройки «Родительского контроля» применяются на все учётные записи компьютера или только на выбранную учётную запись?
5. Какую информацию можно увидеть в «Просмотре отчётов об активности»?

Задание для самостоятельного выполнения

Создайте отдельную учётную запись ребёнка. Настройте «родительский контроль»:

1. Пользование компьютером только во вторник в период с 13-00 до 17-00.
2. Установить уровень веб-фильтра «Для детей».
3. Установить ограничение на пользование 3-мя установленными на компьютере приложениями.

Лабораторная работа № 2

Тема: «Ограничение доступа к сайтам с помощью файла hosts»

Цель:

- научиться работать с системными файлами;
- научиться блокировать доступ к сайтам через файл hosts.

Длительность: 90 минут

Оборудование: Компьютер, доступ к сети Internet

Порядок выполнения работы: работа содержит описательную часть и задания для самостоятельного выполнения. Задания выполняются непосредственно в ходе прочтения содержания.

Лабораторная работа № 3

Тема: «Настройка родительского контроля на роутере TP-link»

Цели работы:

- научить пользователя входить в настройки роутера;
- установить родительский контроль на Wi-Fi роутере;
- установить доступ к определённым сайтам через Wi-Fi роутер;

Длительность:90 минут

Оборудование: Компьютер, роутер TP-link серии N, доступ к сети Internet.

Порядок выполнения работы: работа содержит описательную часть и задания для самостоятельного выполнения. Задания выполняются непосредственно в ходе прочтения содержания.

Лабораторная работа № 4

Тема: «Создание правил контроля доступа для роутера tp-link».

Цель: Научиться создавать правила по ограничению доступа к определённым веб-сайтам.

Длительность: 90 минут.

Оборудование: Компьютер, роутер tp-link серии N.

Порядок выполнения: Работа содержит описательную часть и задания для самостоятельного выполнения. Задания выполняются непосредственно в ходе прочтения содержания.

Лабораторная работа № 5

Тема: «Настройка интернет-фильтра «Интернет Цензор» для ограничения доступа к сети Internet».

Цель: Научиться настраивать правила ограничения доступа к информации глобальной сети на интернет-фильтре.

Длительность: 90 минут.

Оборудование: Компьютер, подключение к сети Internet, ISO –образ (инсталлятор) «Интернет цензора».

Порядок выполнения: Работа содержит описательную часть и задания для самостоятельного выполнения. Задания выполняются непосредственно в ходе прочтения содержания.

ЗАКЛЮЧЕНИЕ

В период выполнения выпускной квалификационной работы была проделана следующая работа:

1. Описаны способы, использующиеся для защиты доступа к информации в сети Internet (встроенная в операционную систему функция «Родительский контроль», функция «Родительский контроль» на роутере, функция «Ограничение доступа» на роутере», интернет-фильтр «Интернет цензор», системный файл hosts).
2. Изучены технологии составления правил ограничения.
3. Выделены основные требования лабораторного практикума по защите доступа к сети Internet.
4. Разработана структура и содержание лабораторного практикума, состоящая из 5 лабораторных работ, в которые входят последовательное объяснение заданий, практическое задание, контроль знаний в виде вопросов для самопроверки и задания для самостоятельного выполнения.
5. Предложена система мероприятий по организации защиты детей от негативной информации в сети Internet.

По завершению предложенной системы мероприятий, обучающиеся будут знать основные виды опасностей, подстерегающие их в глобальной информационной сети, а также основные средства защиты детей от негативной информации в сети Internet.

Цель достигнута, задачи выполнены. Данный комплекс мероприятий может быть использован в системе дополнительного образования.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Алханова А.Б. К вопросу о защите детей от информации, причиняющей вред их развитию в сети Интернет: Аналитический отчет, пособие для педагогов, психологов, родителей и всех заинтересованных сторон [Текст] / А.Б. Алханова – Астана, Каз. Нац. ун-т им. Аль-Фараби, респ. Казахстан, 2010. – 10 с.

2. Грошев А.С. Информатика. Учебник для ВУЗов [Текст] / А. С. Грошев. – Архангельск, Арханг. гос. техн. ун-т, 2010.– 470 с.

3. Информация инженерного образования [Электронный ресурс]. – Режим доступа: http://www.studfiles.ru/preview/1496714/page:42/ (дата обращения: 9.05.2017).

4. Как защитить ребенка от негативного контента [Электронный ресурс]. – Режим доступа http://libr-sch-2.moy.su/publ/iz_opyta_raboty_bibliotekarja/v_pomoshh_uchitelju/kak_zashhitit_rebenka_ot_negativnogo_konteнta/33-1-0-814 (дата обращения: 28.04.2017).

5. Маслов С.И. Информация образования. Направления, среда, технологии [Текст] / М.: Издательство МЭИ, 2004.– 865 с.

6. Международный опыт в области защиты детей от нежелательной информации в интернете [Электронный ресурс]. – Режим доступа: http://www.cossa.ru/152/23475/ (дата обращения: 3.05.2017).

7. Обеспечение защиты детей от негативной информации в сети [Электронный ресурс]. – Режим доступа: http://slidegur.com/doc/1624163/obespechenie-zashhity-detej-ot-negativnoj-informacii-v-seti (дата обращения: 28.04.2017).

8. Обзор решений для ограничения доступа к компьютеру и хранящимся на нем данным [Электронный ресурс]. – Режим доступа http://compress.ru/article.aspx?id=19859 (дата обращения: 01.05.2017).

9. Общие вопросы технической защиты информации [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/studies/courses/2291/591/lecture/12689?page=3 (дата обращения: 23.04.2017).

10. Обучение и техническая поддержка для Adobe Acrobat [Электронный ресурс]. – Режим доступа: https://helpx.adobe.com/ru/support/acrobat.html (дата обращения: 28.05.2017).

11. Ограничение Интернета для детей [Электронный ресурс]. – Режим доступа https://xserver.a-real.ru/support/useful/ogranichenie-interneta-dlya-detey/ (дата обращения: 27.04.2017).

12. О защите детей от информации, причиняющих вред их здоровью и развитию [Электронный ресурс]. – Режим доступа: http://xn--b1afa5ahn1h.xn--80asehdb/(дата обращения: (13.05.2017).

13. О защите детей от опасной информации [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/post/208510/ (дата обращения: 9.05.2017)

14. Петренко В.И. Защита персональных данных в информационных системах: учебное пособие [Текст] / В.И. Петренко. – Ставрополь, уч. высш. обр. «Сев. Кав. ун-т», 2016 год. – 65 с.

15. Безопасность детей в сети Интернет. Правила поведения и родительский контроль [Электронный ресурс]. – Режим доступа: http://www.sovets.ru/safe/7383.htm (дата обращения: 13.05.2017).

16. Родительский контроль в Windows 8 [Электронный ресурс]. – Режим доступа http://remontka.pro/raoditelskiy-kontrol-windows-8/ (дата обращения: 10.05.2017).

17. Родительский контроль. Как ограничить ребенку доступ к Интернет, по времени [Электронный ресурс]. – Режим доступа: https://mhelp.kz/ogranichenie-vremeni-internet/ (дата обращения: 27.04.2017).

18. Симулятор TP-link [Электронный ресурс]. – Режим доступа: http://www.tp-linkru.com/emulators.html (дата обращения: 07.06.2017).

19. Утилиты для родительского контроля за посещаемыми детьми сайтами [Электронный ресурс]. – Режим доступа: http://www.ixbt.com/soft/parentalcontrol.shtml (дата обращения: 30.04.2017).

20. Федеральный закон от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [Электронный ресурс]. – Режим доступа: https://rg.ru/2010/12/31/deti-inform-dok.html?utm_source=rg.ru&utm_medium=offline&utm_campaign=back_to_online (дата обращения: 14.05.2017).

21. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 N 436-ФЗ (последняя редакция) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_ LAW_ 108808/ (дата обращения: 14.05.2017).

22. Хлестова Д.Р., Попов К.Г. Защита детей от интернет-угроз [Текст] / М.: Омега Сайнс, 2016. – 90-92 с.

23. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие [Текст] / В.Ф. Шаньгин. – М.: Форум, 2014. – 702 с.

24. Эрганова Н.Е. Методика профессионального обучения [Текст]: учебное пособие / Н.Е. Эрганова. – 3-е изд., испр. и доп. – М.: Академия, 2007. – 160с.

ПРИЛОЖЕНИЕ А Лист задания на подготовку выпускной квалификационной работы

Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Российский государственный профессионально-педагогический университет»

Институт инженерно-педагогического образования
Кафедра информационных систем и технологий
направление 44.03.04 Профессиональное обучение (по отраслям)
профиль «Энергетика»
профилизация «Компьютерные технологии автоматизации и управления»

УТВЕРЖДАЮ

Заведующий кафедрой
_____Н. С. Толстова

«_____»_____2017 г.

ЗАДАНИЕ

на подготовку выпускной квалификационной работы

Обучающегося (ейся) группы КТэ-402

Фамилия Корнева Имя Сергея Отчество Андреевича

1. Тема Обеспечение защиты детей от негативной информации в сети Internet утверждена распоряжением по институту от 16.06.2017 г. №.

2. Руководитель Г. Л. Нечаева

3. Место преддипломной практики Учебно-технологический центр «Омега – 1»
4. Исходные данные к ВКР
Эрганова Н.Е. Методика профессионального обучения [Текст]: учебное пособие / Н.Е. Эрганова. – 3-е изд., испр. и доп. – М.: Академия, 2007. – 160с.
5. Содержание текстовой части ВКР (перечень подлежащих разработке вопросов)
Изучение литературы по теме способы защиты детей в сети Internet
Разработка электронных средств обучения
Разработка методического указания к лабораторному практикуму
Разработка плана мероприятия по защите детей от негативной информации в сети Internet
6. Перечень демонстрационных материалов
Презентация
Защитное слово
Пояснительная записка
Лабораторный практикум

7. Календарный план выполнения выпускной квалификационной работы

№ п/п	Наименование этапа дипломной работы	Срок выполнения этапа	Процент выполнения ВКР	Отметка руководителя о выполнении
1	Сбор информации по выпускной работе и сдача зачета по преддипломной практике	25.05.2017	10	
2	Выполнение работ по разрабатываемым вопросам, их изложение в выпускной работе:			
	Изучение литературы по теме способы защиты детей в сети Internet	20.04.2017	10	
	Разработка электронных средств обучения	12.05.2017	30	
	Разработка методического указания к лабораторному практикуму	30.06.2017	30	
3	Оформление текстовой части ВКР		5	
4	Выполнение демонстрационных материалов к ВКР		5	
5	Нормоконтроль		5	
6	Подготовка доклада к защите в ГЭК		5	

8. Консультанты по разделам выпускной квалификационной работы

Наименование раздела	Консультант	Задание выдал		Задание принял	
		подпись	дата	подпись	дата

Руководитель _____ *Задание получил* _____
подпись дата подпись студента дата

9. Выпускная квалификационная работа и все материалы проанализированы.
Считаю возможным допустить Корнева Сергея Андреевича к защите выпускной квалификационной работы в государственной экзаменационной комиссии.

Руководитель _____ _____
подпись дата

10. Допустить Корнева Сергея Андреевича к защите выпускной квалификационной работы в государственной экзаменационной комиссии (протокол заседания кафедры от)

Заведующий кафедрой _____ _____
подпись дата

Приложение Б Вопросы для обсуждения

Перечень вопросов, которые следует вынести на рассмотрение среди обучающихся на мероприятии по обмену мнениями:

1. В каком возрасте стоит позволять детям выходить в глобальную сеть Интернет?
2. Следует ли позволять школьникам иметь личные учётные записи электронной почты?
3. Каких внутрисемейных правил необходимо придерживаться при использовании сети Интернет?
4. Как подростки могут защитить себя при использовании служб мгновенной отправки сообщений?
5. Могут ли несовершеннолетние оказаться зависимыми от интернета?
6. Как проконтролировать какие веб-сайты посещают дети в сети Интернет?
7. Какие угрозы глобальной сети встречаются чаще всего?
8. Как обучить ребенка различать правду и ложь в Интернете?

ПРИЛОЖЕНИЕ В Список Федеральных актов и законов Российской Федерации, касающихся ограничения детей от негативной информации в сети Internet

1. Указ президента Российской Федерации от 01 июня 2012 года № 761 «О национальной стратегии действий в интересах детей на 2012-2017 годы».
2. Федеральный закон Российской Федерации от 28 июля 2012 года № 139-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
3. Концепция Всероссийской информационной компании против насилия и жестокости в средствах массовой информации и других средствах массовой коммуникации (Решение Общественного совета при Уполномоченном при президенте Российской Федерации по правам ребёнка от 18.09.2012 года).
4. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

ПРИЛОЖЕНИЕ Г Правила работы в сети Internet

1. Не посещайте незнакомые вам сайты.
2. Если на вашу электронную почту пришёл документ Word или Excel, даже от знакомого лица, перед тем, как открыть, в обязательном порядке проверьте его на вирусы.
3. Если вы получили незнакомое вложение, не открывайте его, а лучше незамедлительно удалите и очистите корзину.
4. Никогда и никому не отправляйте свой пароль.
5. Старайтесь использовать для паролей тяжело запоминающийся набор из цифр и букв.
6. При общении в сети Интернет не указывайте собственные данные, а пользуйтесь псевдонимом (никнеймом).
7. Без контроля старших никогда не встречайтесь с людьми, с которыми познакомились в сети Интернет.
8. Если в сети следует пройти регистрацию, то проходите её таким образом, чтобы в ней не было указано личных данных.
9. Далеко не всей информации, которая размещена в глобальной сети, следует верить.
10. Ни в коем случае не оставляйте компьютер с важными сведениями на экране без присмотра.
11. Не сохраняйте важные данные на компьютере, который находится в свободном доступе.

ПРИЛОЖЕНИЕ Д Вопросы для анкетирования

Анкетирование обучающихся.

Уважаемые обучающиеся. Вопрос обеспечения информационной безопасности детей в информационно-телекоммуникационных сетях становится всё более актуальным. Просим вас ответить на ряд вопросов.

1. Есть ли в вашем доме компьютер?

- да (один);
- да (несколько);
- нет.

2. Кто пользуется компьютером в вашей семье?

- только родители;
- только ребёнок;
- все члены семьи (родители и дети).

3. Пользуетесь ли вы средствами блокировки на компьютере или телевизоре?

- да;
- нет.

4. Имеет ли ваш ребенок личный адрес электронной почты?

- да;
- нет.

5. Существуют ли в вашей семье правила посещения детьми сети Интернет?

- да;
- нет.

6. Пользуетесь ли вы поисковыми браузерами для детей?

- да;
- нет.

7. Следите ли вы за тем, какую информацию загружает ваш ребёнок?

- да;
- нет.

8. Контролируете ли вы, в какие игры играет ваш ребёнок?

- да;
- нет.

9. Проверяете ли вы, с кем общается ваш ребёнок в сети Интернет?

- да;
- нет.

10. С какими законодательными актами Российской Федерации по информационной безопасности детей вы знакомы (перечислить).