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

ЭКСПЕРТНАЯ СИСТЕМА «ИНФОМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ»

Выпускная квалификационная работа
по направлению подготовки 44.03.04 Профессиональное обучение
(по отраслям)
профилю подготовки «Информатика и вычислительная техника»
профилизации «Информационная безопасность»

Идентификационный номер ВКР: 136

Екатеринбург 2019

Министерство науки и высшего образования 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
И.о. заведующего кафедрой ИС
_____ И. А. Суслова
«____» _____ 2019 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

ЭКСПЕРТНАЯ СИСТЕМА «ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ»

Исполнитель:
обучающийся группы ЗИБ-401С А. А. Килин
Руководитель:
канд. пед наук, доцент И. А. Суслова

Нормоконтролер: Н. В. Хохлова

Екатеринбург 2019

АННОТАЦИЯ

Выпускная квалификационная работа состоит из экспертной системы «Информационно-психологическая безопасность» и пояснительной записки на 56 страницах, содержащей 34 рисунка, 2 таблицы, 33 источника литературы, а также 1 приложение на 2 страницах.

Ключевые слова: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ, ЭКСПЕРТНАЯ СИСТЕМА

Килин А. А., экспертная система: выпускная квалификационная работа / А. А. Килин; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. — Екатеринбург, 2019. — 56 с.

Цель работы — разработать экспертную систему «Информационно-психологическая безопасность».

В соответствии с поставленной целью в работе определены следующие задачи: анализ литературы и интернет-источников по теме «Информационно-психологическая безопасность», с целью формирования круга печатных и электронных изданий, рассматривающих данную область; выделить теоретические блоки по теме «Информационно-психологическая безопасность», с целью формирования тематических рекомендаций по рассматриваемой теме; смоделировать процесс принятия решений экспертной системой; реализовать экспертную систему «Информационно-психологическая безопасность». В ходе работы была создана база знаний, включающая также информационные статьи и видеофайлы.

Так же с помощью конструктора экспертных систем «Миварный» были проработаны вопросы и выстроено дерево ответов.

Система реализована на языке гипертекстовой разметки HTML с поддержкой каскадной таблицы стилей CSS.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Благодаря обширной информатизации основных аспектов жизни информационное поле стало важной частью общественной жизни, которая во многом определяет направление национальной социальной политики и экономического развития. Информационное поле. Сфера деятельности субъектов общественной жизни, связанная с созданием, сбором, преобразованием, хранением, распространением и использованием информации, можно разделить на две области: информационно-техническую и информационно-психологическую.

Информационно-техническая область связана с информационным обеспечением всех сторон жизнедеятельности личности, общества и государства посредством использования информационных и телекоммуникационных систем. **Информационно-психологическая область** образуется совокупностью людей и информации, которой они обмениваются и которую воспринимают, общественных отношений, возникающих в связи с информационным обменом информационно-психологическими воздействиями на человека. Этим двум составляющим информационной сферы соответствуют два вида информационной безопасности: информационно-техническая и информационно-психологическая. В настоящее время в Российской Федерации основным документом, содержащим совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности является **доктрина информационной безопасности Российской Федерации** [14].

Вопросы информационно-психологической безопасности в Доктрине затронуты в общих чертах. При этом анализ состояния информационно-психологической безопасности Российской Федерации показывает, что её уровень не в полной мере соответствует потребностям граждан, общества и государства.

Пересмотр приоритетов и акцентов в интерпретации проблемы национальной безопасности и перенос их с интересов государства, которые воспринимались в отрыве от нужд и потребностей человека, на интересы самого человека поставили науку и практику перед необходимостью разработки совершенно нового аспекта этой проблемы — информационно-психологической безопасности, являющейся составной частью информационной безопасности, специфика которой состоит в том, что выступая в качестве объектов, подлежащих защите, отдельные граждане, общество и государство рассматриваются как социальные субъекты.

Под информационно-психологической безопасностью Российской Федерации будем понимать защищённость граждан, отдельных групп и социальных слоёв, массовых объединений людей и населения страны в целом от негативных информационно-психологических воздействий.

Объектом выпускной квалификационной работы является деятельность по выявлению защищенности отдельных лиц от негативных информационно-психологических воздействий.

Предметом выпускной квалификационной работы является диагностирование информационно-психологической безопасности детей.

Цель работы — разработать экспертную систему «Информационно-психологическая безопасность».

В соответствии с поставленной целью в работе определены следующие задачи:

1. Проанализировать литературу и интернет-источники по теме «Информационно-психологическая безопасность», с целью формирования круга печатных и электронных изданий, рассматривающих данную область.

2. Выделить теоретические блоки по теме «Информационно-психологическая безопасность», с целью формирования тематических рекомендаций по рассматриваемой теме.

3. Смоделировать процесс принятия решений экспертной системой.

4. Реализовать экспертную систему «Информационно-психологическая безопасность».

1 АНАЛИЗ ЛИТЕРАТУРЫ ПО ТЕМЕ «ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ»

1.1 Анализ рабочей программы по дисциплине «Основы информационной безопасности»

Анализ рабочей программы [24] показал место учебной дисциплины в структуре основной профессиональной образовательной программы.

Дисциплина «Основы информационной безопасности» относится к базовым дисциплинам программы подготовки специалистов среднего звена, изучается в 3–4 семестрах. Изучение данной дисциплины базируется на освоении студентами дисциплин «Информатика», «Обществознание (включая экономику и право)» и предшествует изучению дисциплин, связанных с профессиональной деятельностью, таких как «Методология защиты информации», «Ведение конфиденциального делопроизводства» и тому подобное.

Целями изучения дисциплины являются:

- формирование стройной системы знаний об основных понятиях, концепциях и ключевых проблемах современной информационной безопасности (ИБ);
- формирование представлений об источниках, рисках и формах атак на информацию;
- классификация угроз, которым подвергается информация; вредоносных программам;
- приобретение практических навыков в работе с защитой от компьютерных вирусов;
- воспитание культуры эффективного использования основных методов и средств защиты информации.

Распределение времени на освоение программы учебной дисциплины «Основы информационной безопасности» представлено в таблице 1.

Таблица 1 — Количество часов, отведённых на изучение дисциплины «Основы информационной безопасности»

Вид учебной работы	**Объем часов**
Общая трудоёмкость (всего)	150
Занятия лекционного типа	48
Практические занятия	44
Консультации	8
в том числе:	
групповые	6
индивидуальные	2
Самостоятельная работа	50

В таблице 2 представлено, что студент должен знать и уметь после изучения дисциплины «Основы информационной безопасности».

Таблица 2 — Что студент должен знать и уметь по окончании изучения курса

Знать	**Уметь**
сущность и понятие информационной безопасности, характеристику ее составляющих	классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности
место информационной безопасности в системе национальной безопасности страны	применять основные правила и документы системы сертификации Российской Федерации
источники угроз информационной безопасности и меры по их предотвращению;	классифицировать основные угрозы безопасности информации
жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;	
современные средства и способы обеспечения информационной безопасности.	

Обладать следующими компетенциями:

1. Общие компетенции (ОК) [30]:

- ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности;

- ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество;
- ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность;
- ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития;
- ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности;
- ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации;
- ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

2. Профессиональные компетенции (ПК):

- ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий;
- ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах;
- ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов;
- ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты;
- ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.

Тематический план дисциплины «Основы информационной безопасности» предусматривает изучение следующих тем:

1. Сущность и понятие информационной безопасности.

2. Значение информационной безопасности для субъектов информационных отношений.

3. Понятие и сущность защиты информации, её место в системе информационной безопасности.

4. Цели и концептуальные основы защиты информации.

5. Защищаемая информация.

6. Понятие и структура угроз защищаемой информации.

7. Каналы и методы несанкционированного доступа к конфиденциальной информации.

8. Методологические подходы к защите информации и принципы её организации.

9. Объекты и методы защиты. Классификация методов защиты информации.

10. Классификация средств защиты информации.

11. Системы защиты информации.

12. Типизация и стандартизация систем защиты.

Для проверки знаний, составляющих компетенции, формируемые в рамках дисциплины «Основы информационной безопасности» в фонде оценочных средств предусмотрены:

- тестовые задания;
- вопросы для устного собеседования (опроса).

Для проверки практической составляющей компетенции, формируемые в рамках дисциплины «Основы информационной безопасности» в фонде оценочных средств размещены профессионально-ориентированные проектные задания.

Формой текущего контроля по данной дисциплине является устный опрос по результатам изучения отдельных тем учебного курса.

Формой промежуточного контроля по данной дисциплине является экзамен (2 семестр).

1.2 Анализ литературы

Особую роль в сфере социальной информации занимает индивидуальное, групповое и массовое сознание, на которое все больше влияет агрессивная информация, которая подрывает психологическое и моральное здоровье граждан и в некоторых случаях разрушает их. Моральные нормы общества привели к стабилизации общественных и политических условий.

Состояние защищённости отдельных лиц и (или) групп лиц от негативных информационно-психологических воздействий и связанных с этим иных жизненно важных интересов личности, общества и государства в информационной сфере — это информационно-психологическая безопасность [21].

В статье Н. В. Старикова «Западная пропаганда, как она работает и форматирует мозги всем народам мира» [28] описаны несколько принципов работы пропагандисткой машины:

- фрагментарность;
- воспитание детей;
- живи в своё удовольствие.

Фрагментарность — это воспитание узкоспециализированых работников со школьной скамьи. Фрагментарность может нести как пользу для общества, можно получить высококлассного профессионала в одном направлении, так и вред, специалист дальше своей области ничего не знает. Её можно применять в профессиональных направлениях подготовки, но перед этим человеку надо сформировать максимально широкий базис знаний, что бы он понимал причинно-следственные связи.

Воспитание детей. «Взрослыми» в такой системе становятся только единицы, и как правило это выпускники элитных школ и академий, которым преподают широкий базис, всем остальным дают лишь минимальный набор общих знаний. Следовательно, такие люди очень наивны и могут поверить в любую глупость, а что бы у них не возникало противоположного мнений, во

всех средствах массовой информации говорят одно и тоже, с поправкой на местность.

Так же что бы у такого общества не появлялись «не правильные» мысли, им говорят, что надо жить в своё удовольствие, и для этого сделаны целые комплексы развлечений: фильмы, книги, все возможные игры. Все это не несёт практической пользы для развития личности, а вот как средство для манипулирования и переключения внимания имеет практическую пользу. Все это приводит к инфантильности людей. Следовательно, они не хотят заводить семьи и иметь детей.

Сохранение индивидуальной компетентности граждан от не достоверной информации является основной деятельностью [11], обеспечивающей национальную информационную и психологическую безопасность. Конечно, все это может снизить устойчивость психики личности на различную информацию. Человек считается устойчивым, если может провести критический анализ, оценить воспринимаемую информацию и принять объективное решение на основе этих данных.

Сейчас наблюдается рост эффективности средств информационного воздействия на психику людей и общественное сознание. Современные информационные технологии и средства массовой информации позволяют практически полностью контролировать и управлять информационным воздействием на коллективный разум [31].

Орудиями информационной пропаганды являются: средства массовой информации, средства массового воздействия, технические средства коммуникации. Одним из самых успешных средств на данный момент являются компьютерные игры, потому что через них можно навязать гражданину ценности и идеалы. Например, в игре «Metro: Last Light» есть 4 стороны конфликта: Фашисты, Бандиты, Наёмники и Коммунисты, и все сделано так что самой большой угрозой для главного героя и всего мира игры, являются коммунисты, и на протяжении большей части игры мы будем с ними воевать, а их буду показывать, как очень жутких людей. В другой серии игр «Call of

Duty: Modern Warfare» есть с цена с аэропортом где по сюжету требуется устроить теракт в московском аэропорту и все преподносится так будто только русские плохие, а все остальные хорошие. В ещё одной серии игр «Rise of the Tomb Raider» игрокам предлагают устроить революцию на Алтае и сжигать портреты Юрия Гагарина и плакаты космических кораблей, якобы это все русская пропаганда. Вот три примера пропаганды в играх, и люди которые играют в подобные игры начинают верить в эти мифы и выдумки.

Вопросы связанные с информационно-психологической безопасностью российские учёные стали изучать совсем недавно — в начале 21 века. В. Я. Асанович и Г. Г. Маньшин [1]. Они изучили как информация влияет на психологическое состояние людей, и на динамику рассогласованности.

Проблемы информационной и психологической безопасности лежат в междисциплинарной области взаимодействия: право, психология и информационные технологии. Так, например, Л. А. Михайлов [22] и Р. М. Юсупов [31] рассмотрели вопросы личной безопасности в информационном обществе в рамках национальной безопасности всей страны. Ю. С. Уфимцев, Е. А. Ерофеев и другие авторы посвятили свою работу современным аспектам информационной безопасности России, нормативно-правовым, психологическим и технологическим приёмам её обеспечения. Две главы посвящены негативному психологическому воздействию сообщений на народы [29].

Цифровые продукты представляют угрозу для информационно-психологической безопасности людей. Данной проблеме посвящено исследование Ю. М. Кузнецовой и Н. В. Чудовой [20]. В данной работе рассматриваются личные изменения, возникающие в новой социальной ситуации личностного развития, определяемой формированием интернет-культуры. — Ю. С. Рысин [25]. Он обобщил научные и практические достижения в области современных информационных систем вещания и технологий, и обосновал серьёзность влияния на индивида.

В настоящее время выросло число исследований, посвящённых вопросам информационной безопасности и влияния информационных технологий на мышление народов.

Цифровые технологии — определяют будущее общества. Но в то же время в руках злоумышленников это страшное оружие. Основная опасность — несанкционированный доступ к источнику или потребителю.

Сейчас они оказывают информационное воздействие на толпы и общество. Развитие информации и технологий оказали значительное влияние на внутренний и внешний мир человека, что, в свою очередь, отражается на уровне информационной безопасности. Психологическое, социальное и культурное составляющие человека содержит в себе информационные технологии, и люди зачастую не в состоянии следить за процессом своего развития. В условиях социальной информатизации цифровые технологии стали одним из важнейших инструментов формирования потребностей, интересов, взглядов и ценностей, и в конечном счёте, стали инструментом, влияющим на механизмы идеологии, грамотности и занятий [22].

При поддержке нынешних средств массовой информации появляется множество возможностей влиять на информацию получаемую человеком. По сути, сегодняшние средства массовой информации являются фактически единственной структурой, в которой население каждый час получает информацию о различных процессах в стране, регионе и мире, и благодаря этой структуре различные идеологические взгляды применяются дословно. Поэтому люди должны согласиться с тем, что сегодняшние российские средства массовой информации могут быть силой для стабилизации социальной ситуации, а также могут служить поводом для общественных разногласий.

Телекоммуникационные продукты предназначены для предоставления информации, образования и развлечений. Непосредственно обращаясь к людям и обществу, они оказывают на людей огромное информационное влияние. С момента своего создания телекоммуникационные технологии также стали инструментом для агитаторов и пропагандистов.

Из-за коммерциализации средств массовой информации, со стороны телевидения на общество обрушились потоки рекламы, фильмов и передач, связанных с насилием, унижением личности человека. Все это можно отнести к категории вредоносной информации.

Реклама непосредственно связана с вопросом дезинформации вкладчиков. В девяностые года прошлого века, много россиян стали жертвами финансовых пирамид. В основном это люди, пожилого возраста, которые поверили в громкую рекламную компанию в средствах массовой информации: со страниц газет, журналов и с экранов телевизора [31].

Нынешние программы могут не только влиять на людей, сообщая неточную информацию, но и на их психическое и физическое состояние.

Общество много времени тратит в средствах массовой информации. В среднем жители крупных городов проводят по три часа в день за просмотром телевизора. Эта ситуация оказывает негативное влияние на психическое здоровье людей, потому что хорошо известно, что цветовые эффекты телевидения оказывают прямое физиологическое воздействие и двадцать пятый кадр. Специалисты сосредоточены на изучении синего, красного и белого ритмических вспышек. Эти вспышки могут нарушить нормальное функционирование мозга. Поэтому, изменяя цветовую схему, можно использовать различные способы манипуляции, чтобы вызвать стресс, усталость, депрессию, торможение сексуальной функции и тому подобное. Психологи обнаружили, что после долгого просмотра телевизора человеческий мозг впадает в состояние лёгкого гипноза т.к. 9% сознательно воспринимаемой человеком информации, а 93% — на подсознательном уровне [25]. Следовательно, в дополнение к основной информации, предназначенной для понимания людьми, эксперты могут также передавать бессознательную информацию в виде низкочастотных изменений яркости света, что влияет на подсознание и психофизиологию человека.

Один из случаев произошёл в Японии, когда у 700 детей обнаружили припадки во время просмотра мультфильма «Карманные монстры». 208 че-

ловек пришлось госпитализировать. Причиной этого явления являются синие, красные и белые ритмичные мерцания тонов [25].

Орудия массовой информации, которые управляют, трансформируют и распространяют информацию, стали основным инструментом современного социального влияния. Для повышения эффективности исполнения диктаторских планов используются интеллектуальные технологии, которые помогают обратить аудиторию в предмет манипуляции. Люди, с повышенной внушаемостью становятся этим искомым предметом. Сознание народных масс редко бывает тщательно структурировано, но оно продолжает внушать идеи, они бесконечно распространяется средствами массовой информации и представляют собой невидимую основу для контроля мнений, институтов и ограничений, и регулировать реакцию общественности, оценку и поведение [26].

Интернет так же является одним из средств массовой информации. Сегодня есть онлайн-новости, публикуются онлайн-журналы и онлайн-газеты, но Интернет так же более универсален и имеет более глобальное влияние, чем традиционные медиа. Сегодняшний Интернет стал очень доступным и популярным. Согласно статистике, в 2018 году во всем мире насчитывалось около 4.021 млрд. пользователей Интернета, а для России этот показатель составляет 91.4 миллиона пользователей только мобильного Интернета [32].

Интернет-сектор России характеризуется постоянно растущим числом пользователей. В 2018 году Интернетом в России пользуются 99% людей в возрасте от 16 до 29 лет, 88% людей в возрасте от 30 до 54 лет, а так же 36% людей в возрасте от 55 лет и старше [19]. Интернет оказывает самое серьёзное влияние на сознание, которое ещё не сформировалось до конца [16].

Увлечение играми на компьютерах, сегодня широко распространено среди молодёжи, вызывает особую тревогу. Дети и подростки могут свободно играть в игрушки с сетевых ресурсов и играть в игры через Интернет в сетевом режиме. Молодые люди со слабой психикой особенно уязвимы для виртуальной реальности, создаваемой такими играми. Благодаря игре подростки и дети могут проводить много времени сидя за компьютером. Поэто-

му они «отрываются» от общества, становятся равнодушными и пассивными к жизни в реальности, и для них человеческая жизнь ничего не стоит [17].

Написание и популяризация онлайн-игр является одним из наиболее прибыльных и активных направлений бизнеса, поэтому не следует ожидать, что развитие этой области будет сокращено или ограничено. Общество и государство должны принять все возможные меры, в том числе этические, для защиты молодого поколения от негативных последствий этого хобби. Некоторые государства начали двигаться в этом направлении. Например, Министерство здравоохранения Таиланда сочло необходимым предупредить родителей о том, что им следует тщательно выбирать видеоигры и учитывать возраст и эмоциональное состояние своего ребёнка [31].

Технические средства коммуникации — могут привести к психическим расстройствам у детей, а также к психологическим и эмоциональным проблемам, связанным с влиянием информации на людей: у ребёнка ухудшается память, сон, он хуже учится в школе, не может сосредоточиться, становится взволнованным, раздражённым, чувствительным [6].

Особенно значимым является исследования учёных, которые раскрывают влияние Интернета на условия жизни людей и, следовательно, информационную локализацию от него.

Народ, подчинённый средствам телекоммуникации, в основном использует сетевые сервисы, которые позволяют им накапливать информацию и поддерживать связь с ранее установленными знакомыми, позволяют им знакомиться с новыми людьми в виртуальном пространстве, общаться и обмениваться идеями. Большинство людей, использующих Интернет, пользуются услугами связи. К. Янг выделил две группы людей, которые зависят от сети: «висящие» ради информации (91%) и «висящие» на общении ради общения. Люди, зависимые от сети, используют Интернет для получения социальной поддержки (поскольку они являются членами определённой социальной группы: участвуют в чатах или конференц-звонках), могут создавать

виртуальных героев (создавать новое «Я»), порождая какую-то реакцию со стороны прочих индивидов [22].

Зависимость от сети можно сравнить с другими типами зависимостей, например, от психотропных веществ. Зависимые люди, в том числе информационно, характеризуются крайним отсутствием самостоятельности, неспособностью отказать, критиковать или противостоять уязвимости, нежеланием брать на себя ответственность и принимать решения, и, следовательно подчинение авторитетам. Опасность этого зависимого общества состоит в том, что оно может заменить чьё-то реальное общение с жизни людьми. Рост количества подобных индивидов возможно приведёт к общественному разложению.

Свойства Интернета имеют решающее значение при рассмотрении вопросов информационной и психологической безопасности человека. Это связано с отсутствием какого-либо органа управления или контроля в сети. Ответственность за информацию в сети фактически никто не несёт [27].

Взлом, который проявляется в интернет-преступности. Крупные компании и частные лица подвергаются атакам хакеров. Девиантное поведение в сети может быть объяснено тем фактом, что люди здесь показывают свою склонность к агрессии, но в реальной жизни они ограничены страхом перед законом, а характеристиками виртуальной реальности является: анонимность и физическая недоступность. Это позволяет людям показать худшие стороны личности [23]. По словам К. Касперски, компьютерный мир из доброго сообщества быстро превратился в подобие социума, где нельзя оставлять ворота незапертыми, а за каждым углом может стоять человек с ножом [18].

Поскольку ещё никто и не что не отвечает за достоверность размещённой в сети Интернет информации, показывает худшую особенность людей и вредит людям через виртуальное пространство.

Как показывают опросы общественного мнения хакеров, первое — это их мотивация, они называют это познанием (работать на более мощном компьютере, узнать, как работает та или иная программа); кроме того, ими ещё

движут корыстные мотивы, отомстить работодателю, желанию быть признанным, самовыражение, даже во вред окружающим [3].

Информационные сети типа Интернет служат весьма удобной площадкой для подготовки и осуществления информационно-террористических и информационно-криминальных действий. В нем могут распространяться пропагандистские материалы преступных организаций, рецепты изготовления взрывчатых веществ, оружия, в том числе ядерного, наркотических и психотропных средств, наконец, изощрённых алгоритмов вскрытия шифров. Такая информация маскируется под научно-техническую информацию [15].

Интернет, как любое крупное изобретение человечества, предлагает возможности для личного развития, застоя и деградации. Использование первой или второй из этих возможностей или отказ от сетевой активности в качестве средства изменения своей жизни зависит от желаний субъекта. Можно лишь констатировать, что человек меняется под влиянием деятельности, опосредованной Интернетом, причём меняется закономерно, в соответствии с внутренними и внешними условиями этой деятельности. Внутренние условия зависят от того, какой этап в развитии идентичности и развитии высших психических функций человек проходит с опорой на возможности данной среды; внешние — от форм психической активности, которые поддерживаются этой средой [12].

Ещё одной опасностью для человека в информационном обществе становится терроризм. Террористические организации активно и эффективно используют достижения научно-технической и информационной революции — от средств массового уничтожения, транспорта и связи до новейших медийных и психологических технологий, регулярно опережая в этом государственные службы, противодействующие терроризму. Поэтому террористические угрозы в информационной сфере представляют очень серьёзную проблему, актуальность которой будет только возрастать по мере развития и распространения информационно-коммуникационных технологий.

Использование террористами нестандартных средств нападения и сценариев повышает эффективность психологического воздействия на население за счёт «новизны» и увеличивает вероятность успешной реализации за счёт неготовности государственных антитеррористических структур и систем к их выявлению и отражению. Перспективной террористической технологией является осуществление компьютерных атак на критически важные информационно-управляющие системы с учётом их повсеместного распространения, а также объективных возможностей нанесения скрытого и удалённого воздействия [11].

В конце 90-х гг. были сообщения о том, что члены некоторых исламских экстремистских организаций пытаются развить хакерские сети для оказания компьютерной поддержки и организации информационных войн в будущем [5].

В основе современных технологий пропаганды терроризма лежит прямое или опосредованное использование средств массовой информации. Подавляющее большинство средств массовой информации в настоящее время не предоставляет свои страницы или эфир террористам с учётом общественного мнения и законодательства своих стран. Однако в государствах с фундаменталистскими, левыми и гипертрофированно либеральными режимами такие средства массовой информации всегда находятся («Аль-Джазира» и т.д.), а остальные их в обязательном порядке цитируют. Здесь наблюдается объективное совпадение интересов террористов и средств массовой информации: террористам нужно максимально широкое освещение их деятельности (вне зависимости от контекста), а средствам массовой информации нужны сенсации [10].

Технологии воздействия на сознание личности в информационном обществе террористическими организациями различны. Так, прямое использование средств массовой информации в настоящее время реализуется, как правило, в глобальной сети Интернет, где в качестве инструмента воздействия выступают сайты террористических структур. Интернет является иде-

альной средой для деятельности террористов, поскольку доступ к ней крайне лёгок, потенциальная аудитория огромна, там легко обеспечить анонимность пользователей, эта среда никем не управляется и не контролируется [4].

Террористы адресуют свои сайты активным участникам, потенциальным членам, международной общественности (для формирования соответствующих настроений в обществе) и противникам (с целью их деморализации). Особое внимание уделяется журналистам: на террористических сайтах постоянно публикуются пресс-релизы, а журналистам предлагается контактная информация для связи. Сейчас в Интернете представлены все известные террористические группы, которые публикуют свои материалы более чем на 40 различных языках. Типичный террористический интернет-сайт, как правило, содержит историю организации, обзор политических, экономических и социальных предпосылок возникновения организации, биографии лидеров, обоснование применения насилия, программу действий, хронику деятельности. На террористических сайтах часто организована торговля флагами, футболками, плакатами, значками, аудио- и видеозаписями по соответствующей тематике [7].

К обсуждаемым в последнее время возможным террористическим технологиям относятся акции по непосредственному оказанию устрашающего воздействия на массовое сознание (без реализации классического теракта) с помощью информационного оружия и социальных технологий. Одним из наиболее успешных инструментов ведения психологической войны стали сами террористические сайты. На них публикуются дезинформационные сообщения, новости, вызывающие панику и ощущение безнадёжности у населения, фотографии и видеоматериалы, внушающие ужас, например казни заложников. «Аль-Каида» периодически публикует на своих сайтах угрозы и предупреждения о готовящихся террористических актах. Технологии планирования сценариев терактов направлены на достижение максимального информационно-психологического эффекта и базируются на хорошем знании социальной психологии и массовых коммуникаций.

Террористы, пытаясь показать незащищённость граждан в государстве, вызывая страх и сея панику в обществе, влияют на сознание людей и манипулируют ими. Так, за период с 2014 по 2018 гг. тысячи граждан Российской Федерации получали письма от представителей террористов с призывами присоединиться к джихаду против Российской Федерации, ссылками на сайты с детальными инструкциями о путях присоединения к террористам. После начала спец. операции в Сирии многие граждане Европы также получили послания, призывающие их приехать в Сирию и принять участие в освободительной войне против Российской Федерации и её союзников [5].

В настоящее время информационное общество характеризуется все возрастающей скоростью прохождения различных информационных потоков, и соответственно клиповостью мышления во взаимодействие с которыми вступает человеческая психика, являющаяся одним из звеньев коммуникационных сетей [2]. Клиповость мышления выражается в восприятии информации через заголовок, на усвоение всего текста у многих людей не хватает времени.

Благодаря достижениям двадцатого века в технологиях появились качественно новые возможности для средств массовой информации, являющихся в руках ограниченной части населения мощным инструментом информационного воздействия в информационной войне. Общество сегодня стоит на пороге очередной технической революции в информационной области, благодаря распространяющимся всемирным сетям кабельного и спутникового вещания, а они, в свою очередь, способствуют появлению новых технологий информационно-психологического воздействия, которое не всегда положительно влияет на психологию людей.

В связи с этим в качестве одной из первоочередных практических задач становится подготовка людей к глобальным информационным переменам, событиям, участниками которых они являются или могут явиться. В результате исследований доказано, что назрела необходимость разработки теории информационных нововведений, поскольку население часто оказывается

психологически не подготовленным к новшествам при формировании информационного общества, изучения психологических аспектов принятия решений в условиях информационного общества, а также разработки и создания эффективно функционирующих систем стратегического планирования в условиях современной информационно-технической среды.

1.3 Обзор специфических возможностей экспертных систем

1.3.1 Общие сведенья об экспертных системах

Экспертная система (ЭС, англ. expert system) — компьютерная система, способная частично заменить специалиста — эксперта в разрешении проблемной ситуации. Современные ЭС начали разрабатываться исследователями искусственного интеллекта в 1970-х годах, а в 1980-х получили коммерческое подкрепление. Предтечи экспертных систем были предложены в 1832 году С. Н. Корсаковым, создавшим механические устройства, так называемые «интеллектуальные машины», позволявшие находить решения по заданным условиям, например, определять наиболее подходящие лекарства по наблюдаемым у пациента симптомам заболевания.

В области компьютерных наук экспертная система рассматривается вместе с базой знаний как модель поведения эксперта в области знаний с использованием процессов вывода и принятия решений, а база знаний служит набором фактов и правил вывода в выбранных предметных областях.

Аналогичные действия выполняются программными средствами, такими как «Мастер» (англ. Wizard). Мастера используются как в системных программах, так и в приложениях для упрощения интерактивного общения с пользователями (например, при установке программного обеспечения). Основным отличием мастера от ЭС является отсутствие базы знаний — все операции строго запрограммированы. Это просто набор форм, заполненных пользователем.

Другими подобными программами являются поисковые или справочные (энциклопедические) системы. По запросу пользователя они предоставляют наиболее подходящую (релевантную) часть базы данных статей (объекты предметной области, их идеи виртуальной модели).

В настоящее время «классическая» концепция экспертных систем, разработанная в 1970-х и 1980-х годах, переживает серьёзный кризис, в основном связанный с оригинальностью формальной логики, особенно для разработчиков и пользователей информационных систем. На самом деле, начиная с эпохи Аристотеля, формальная логика ещё не развилась, и её древняя форма не соответствует требованиям современных технологий. Интерфейс человек-машина, используемый сегодня, далёк от оптимального. Кроме того, «классический» подход к созданию экспертных систем несовместим с ведущими современными реляционными моделями данных в области компьютерных наук, что делает невозможным эффективное использование современных промышленных систем управления базами данных для организации базы знаний этих систем. Все примеры «известных» или «широких» экспертных систем, приведённые в литературе и онлайн-ресурсах, можно проследить до 1980-х годов, они больше не существуют или устарели, и лишь немногие энтузиасты поддерживают это. С другой стороны, современные программные продукты часто объявляются как экспертные системы, не имеющие «классического» значения (например, компьютерные справочные и правовые системы). Поклонники, сочетающие «классический» подход с современным подходом к разработке экспертной системы и созданию пользовательского интерфейса (проект CLIPS Java Native Interface, CLIPS.NET и т. д.). Не могут найти поддержку в крупных компаниях-разработчиках программного обеспечения, поэтому они остаются в экспериментальной фазе.

Некоторый оптимизм вселяет современное развитие OLAP-систем и систем поддержки принятия решений, которые пока и дороги, и далеки от оптимальности.

Структуру экспертной системы обычно представляют из следующих элементов:

- интерфейс эксперта;
- интерфейс пользователя;
- интеллектуальный редактор базы знаний;
- база знаний;
- решатель (механизм вывода);
- подсистема объяснений.

База знаний включает в себя правила анализа информации от пользователя о конкретной проблеме. ЭС анализирует ситуацию и предлагает решения проблемы.

Как правило, база знаний экспертной системы содержит факты (данные, отношения на синтаксическом уровне), знания (семантические, семантические отношения между данными) и правила — набор инструкций, которые можно применять к известным фактам и значениям.

Как часть логической модели базы данных и базы знаний, они написаны на компьютерных языках с продвинутой логикой, таких как, например, Prolog или Smalltalk, с использованием языков предикатов для описания фактов и правил вывода, которые выражают правила определения концепции для описания обобщённых сумм. Конкретная информация, а также конкретные и обобщённые запросы для баз данных и баз знаний.

Конкретные и обобщённые запросы к базе знаний на языке Prolog пишутся с использованием языков предикатов, которые представляют правила вывода и определения процессов вывода, доступных в базе знаний, которые представляют широкие и конкретные аспекты выбранной предметной области и знаний.

Зачастую факты в базе знаний описывают те явления, которые являются постоянными для данной предметной области. Признаки, значения которых зависят от условий конкретной задачи, принимаются от пользователя во время работы и сохраняются в рабочей модели. Например, в медицинской ЭС

тот факт, что «у здоровых людей две ноги» хранится в базе знаний, а тот факт, что «у пациента одна нога» — в рабочей модели конкретного пациента.

База знаний ЭС создаётся при помощи трёх групп людей:

- эксперты той проблемной области, к которой относятся задачи, решаемые ЭС;
- инженеры по знаниям, являющиеся специалистами по разработке;
- программисты, осуществляющие реализацию ЭС.

1.3.2 Режимы функционирования экспертной системы

ЭС может работать в двух режимах [13]:

- схема ввода знаний — в этом режиме эксперт вводит информацию о своей известной предметной области в базу знаний ЭС с помощью редактора базы знаний с помощью инженера знаний;
- консультационный режим — пользователь ведёт разговор с ЭС, уведомляя её о текущей задаче и получая рекомендации ЭС. Например, на основании информации о физическом состоянии пациента ЭС диагностируется в виде списка заболеваний, наиболее вероятно имеющих эти симптомы.

1.3.3 Классификация экспертных систем

Экспертные системы в зависимости от решаемой задачи подразделяются (специализируются) в следующих направлениях деятельности [8]:

- интерпретация данных;
- диагностирование систем;
- мониторинг проблемной области;
- проектирование систем;
- прогнозирование процессов;
- планирование производства;
- оптимизация процессов и систем;

- обучение знаниям и умениям (технологиям);
- управление процессами и системами;
- ремонт технических систем и лечение организмов;
- отладка и тестирование систем и их элементов.

В зависимости от условий экспертные системы делятся на:

- статические ЭС — это ЭС, решающие задачи в условиях не изменяющихся во времени исходных данных и знаний;
- квазидинамические ЭС интерпретируют ситуацию, которая меняется с некоторым фиксированным интервалом времени;
- динамические ЭС — это ЭС, решающие задачи в условиях изменяющихся во времени исходных данных и знаний.

2 ХАРАКТЕРИСТИКА ПРОГРАММНОГО ПРОДУКТА

2.1 Общие сведения

Данная экспертная система реализована в формате HyperText Markup Language (HTML) с использованием таблицы стилей Cascading Style Sheets (CSS). Для автоматизации набора HTML-кода был использован Website X5, в конструктор экспертных систем «Миварный» (КЭСМИ «Миварный») были проработаны вопросы и выстроено дерево ответов.

Объём электронного учебного пособия составляет 153 Мб.

2.2 Требуемое программное и аппаратное обеспечение

Для использования экспертной системы потребуется персональный компьютер с установленной операционной системой MS Windows 7 или выше и следующей аппаратной конфигурацией:

- объем оперативной памяти не менее 4Гб;
- процессор с частотой не менее 2 ГГц;
- браузер Firefox, либо любой другой браузер;
- наличие необходимого оборудования.

2.3 Структура экспертной системы

Структуру ЭС можно разделить на 2 блока (рисунок 1):

1. Блок вопросов.
2. Блок ответов.

Экспертная система предназначена для:

- родителей, желающих оградить своего ребёнка от вредной информации;

- интересующихся разделом «Информационно-психологическая безопасность».

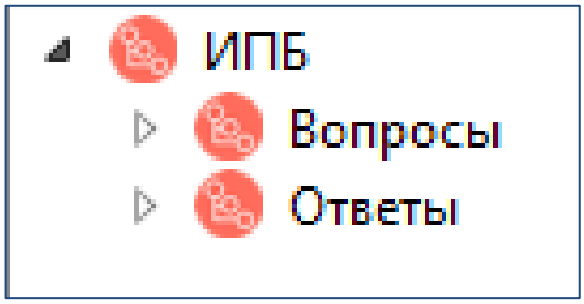

Рисунок 1 — Структура системы

Блок 1. Блок вопросов.

Блок вопросов содержит следующие вопросы (рисунок 2).

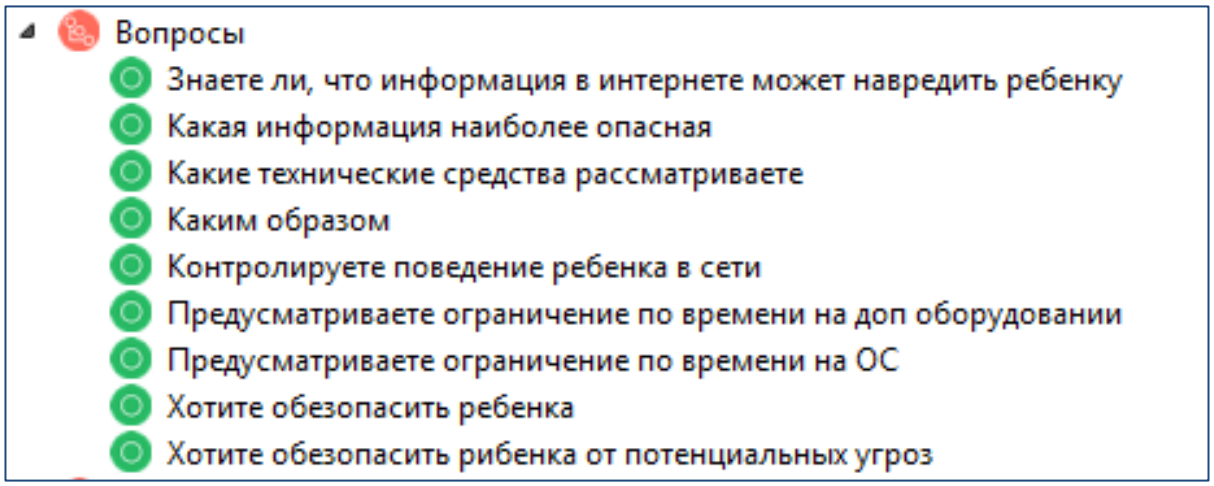

Рисунок 2 — Блок вопросов

Блок 2. Блок решений.

Блок решений содержит следующий ответы:

1. Человек как социально-биологическая ценность. Раздел содержит информацию о социальной и индивидуальной составляющей человека, о групповой системе мировоззрения, об основе поведенческого акта.

2. Информация и её восприятие человеком. Раздел содержит описание видов информации и её восприятие человеком.

3. Психика и психические процессы. Раздел содержит информацию о психических процессах, психических свойствах и состояниях, коллективное бессознательное и надсознательное.

4. Групповое, массовое и общественное сознание. Раздел содержит информацию о видах сознания и их отличия, способах манипуляции им.

5. Воздействие на психику и сознание человека. Раздел содержит информацию об информационно-психологическом воздействии, о методах и средствах информационно-психологического воздействия, о последствиях информационно-психологического воздействия.

6. Родительский контроль. Раздел содержит информацию о программах родительского контроля, способах ограничения вредной информации.

Раздел посвящён настройке родительского контроля средствами Windows, на примере Windows 7.

«Ограничение по времени» (рисунок 3) компьютер будет выключен в то время, которое не разрешено правилами, установленными администратором, и включить его можно только в указанное время и дни. С точки зрения семейной психологии — это очень ценно — родителям не нужно ругать ребёнка и отнимать у него компьютер, потому что он сам себя выключит. Тогда ребёнок не считает, что родители являются злодеями, которые забирают его любимую игрушку.

Рисунок 3 — Ограничение по времени

«Ограничение запуска игр» (рисунок 4) — ценность семейной психологии очевидна — иногда даже взрослым становится не по себе от компьютерных игр.

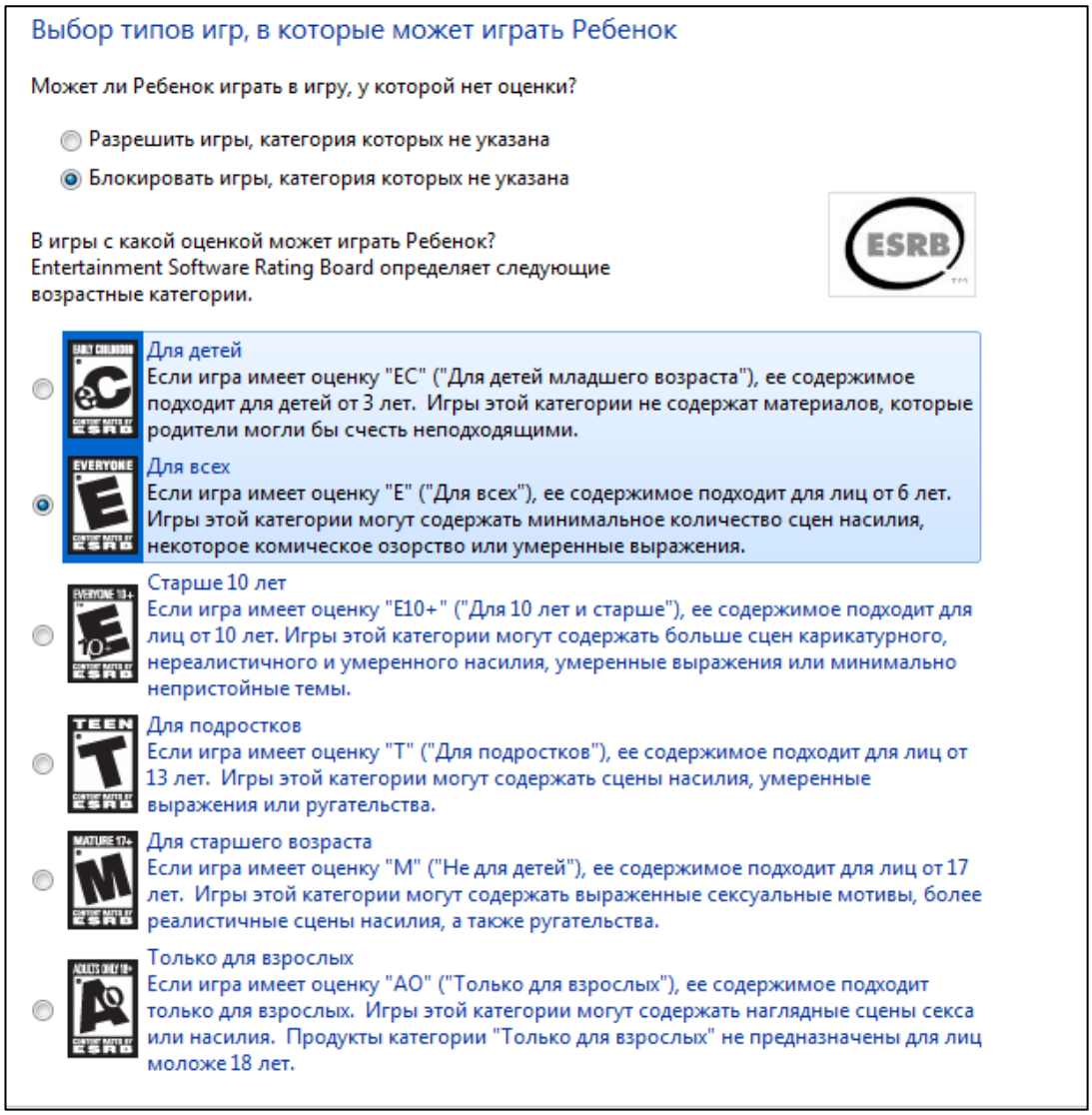

Рисунок 4 — Ограничение запуска игр

«Ограничения на запуск программ» (рисунок 5) Эта функция нужна, чтобы ребёнок ничего не испортил на компьютере.

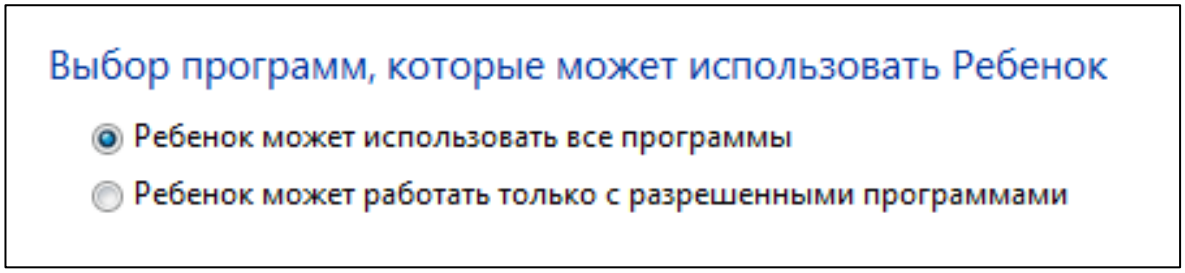

Рисунок 5 — Ограничения на запуск программ

Раздел посвящён настройке родительского контроля с помощью «Kaspersky Safe Kids».

В разделе «Правила» можно настроить защиту для ребёнка так, как сами считаете нужным. Помните, что по умолчанию включена защита, подходящая для ребёнка указанного возраста.

Первое, что можно настроить, используя Safe Kids это правила интернет-сёрфинга для ребёнка (рисунок 6).

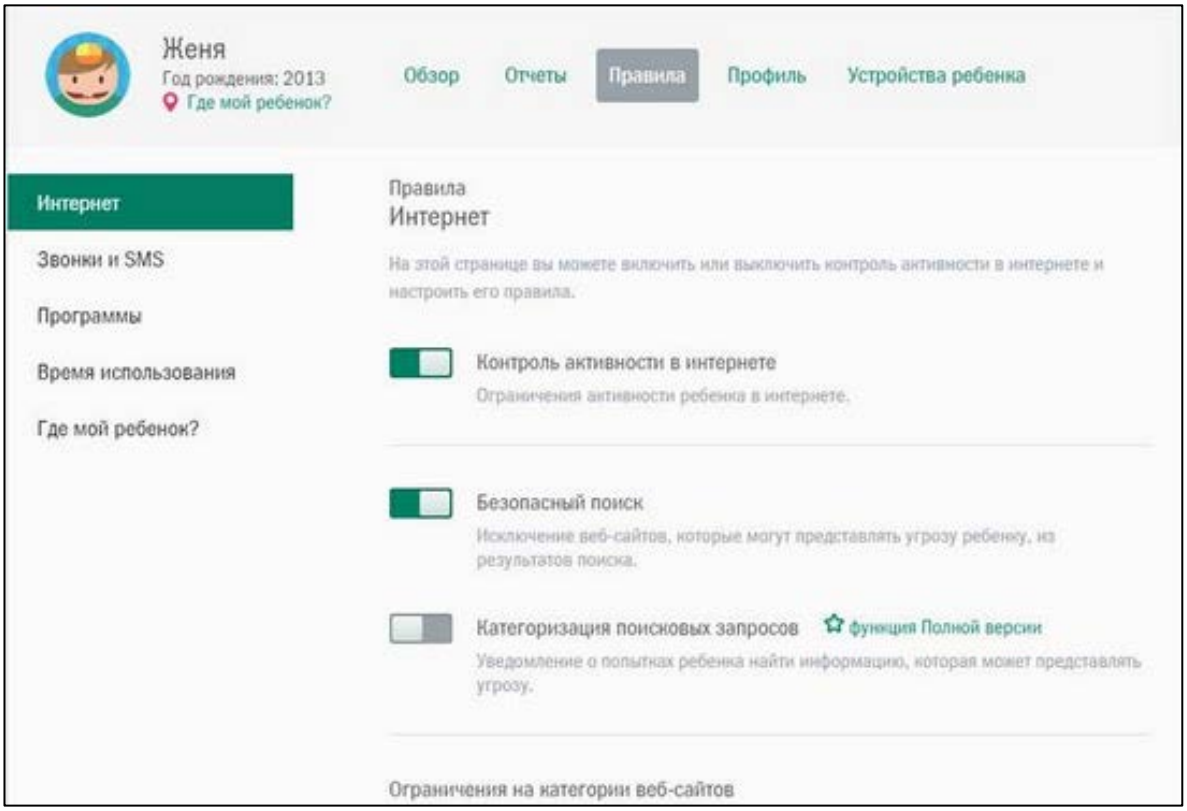

Рисунок 6 — Правила интернет-сёрфинга

Ниже на той же странице можно увидеть категории веб-сайтов, которые можно запретить к посещению (рисунок 7).

В первом блоке могут выбрать одну из категорий и запретить, либо разрешить её. Кроме того, при попадании на сайт некоторых категорий ребёнок может получать предупреждение о том, что содержимое страницы может быть не предназначено для его глаз.

Рекомендуется запрещать категорию «Переадресация HTTP запросов», поскольку дети часто используют такие сайты для обхода ограничений, введённых родительским контролем.

Ниже, во втором блоке, можете добавить сайты-исключения. При том как разрешённые, так и запрещённые.

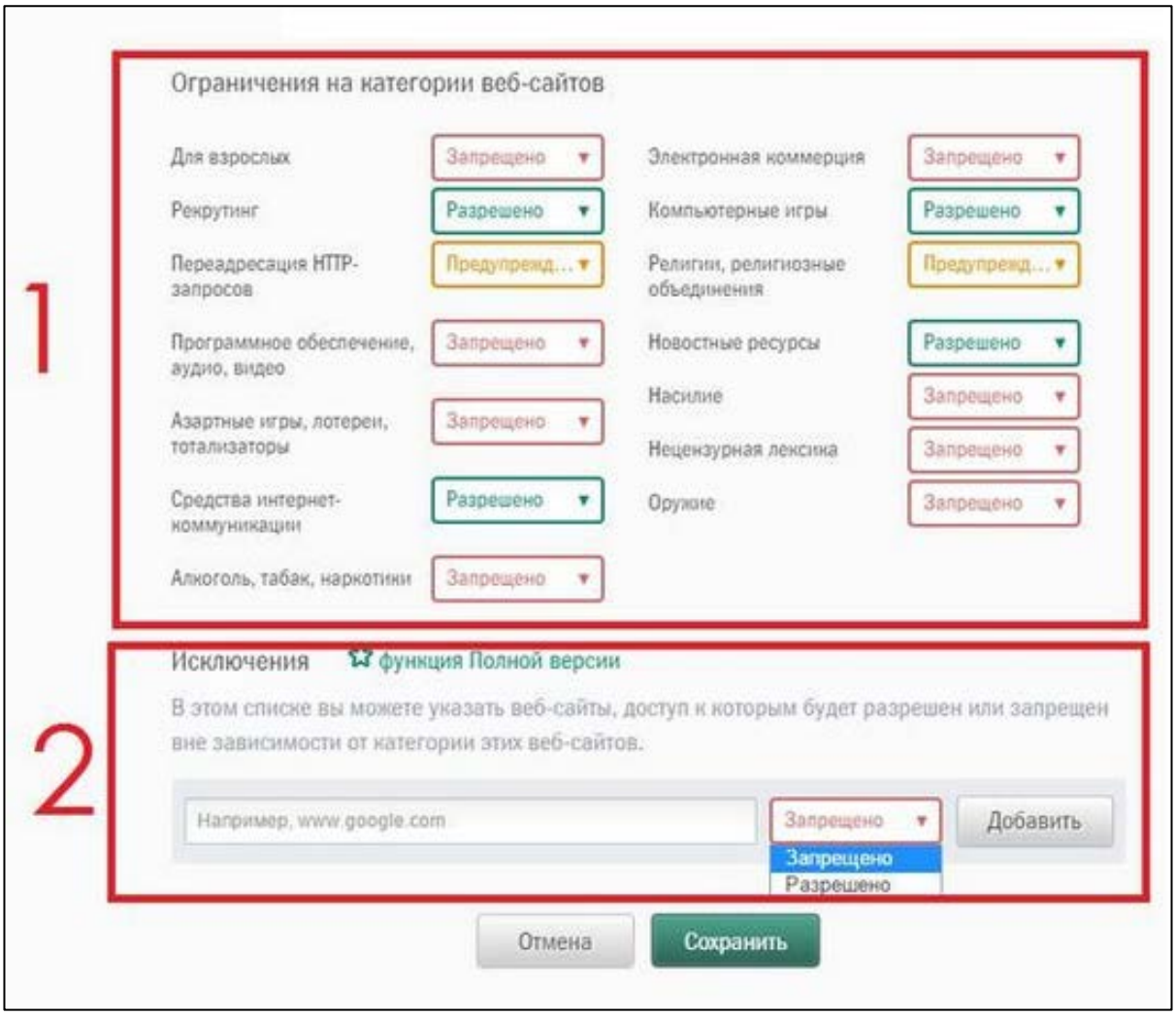

Рисунок 7 — Ограничения веб-сайтов и исключения

Например:

- хотите запретить ребёнку посещение интернет-магазинов, кроме нескольких, в которых он может найти и показать вам книги, которые ему нужны для учёбы, или саморазвития. Запретите категорию «Электронная коммерция» и введите сайты-исключения со статусом «разрешено»;
- не против посещения ребёнком сайтов игровой тематики, кроме сайтов нескольких игр, которые считаются неподходящими для ребёнка. Разрешите категорию «Компьютерные игры» и введите в исключения со статусом «запрещено» сайты, которые нельзя, чтобы он посещал.

Раздел посвящён настройке родительского контроля через маршрутизаторы.

Это возможность ввести ограничение на уровне маршрутизатора, то есть для некоторых или сразу для всех компьютеров, подключённых к Wi-Fi, но в немного другом формате. В этой настройке задаётся не доступ к ресурсам, а время работы в Интернете. Например, можно отключить выход во всемирную сеть в те часы, когда ребёнку положено делать уроки или спать. Либо сотруднику выполнять свою работу, если речь идёт об офисной сети. В некоторых моделях функция блокировки сайтов и временного ограничения совмещены. Настраивать будем на трёх маршрутизаторах.

Маршрутизатор Tenda

В основном меню выбираем «Родительский контроль». В «подключённые устройства» выбираем устройство, на котором хотим настроить контроль. В «ограничение доступа» настраиваем время и дни, когда устройству будет разрешён доступ в сеть, и настраиваем белый и чёрный список сайтов (рисунок 8): 1 — главное меню, 2 — подключённые устройства, 3 — ограничение доступа.

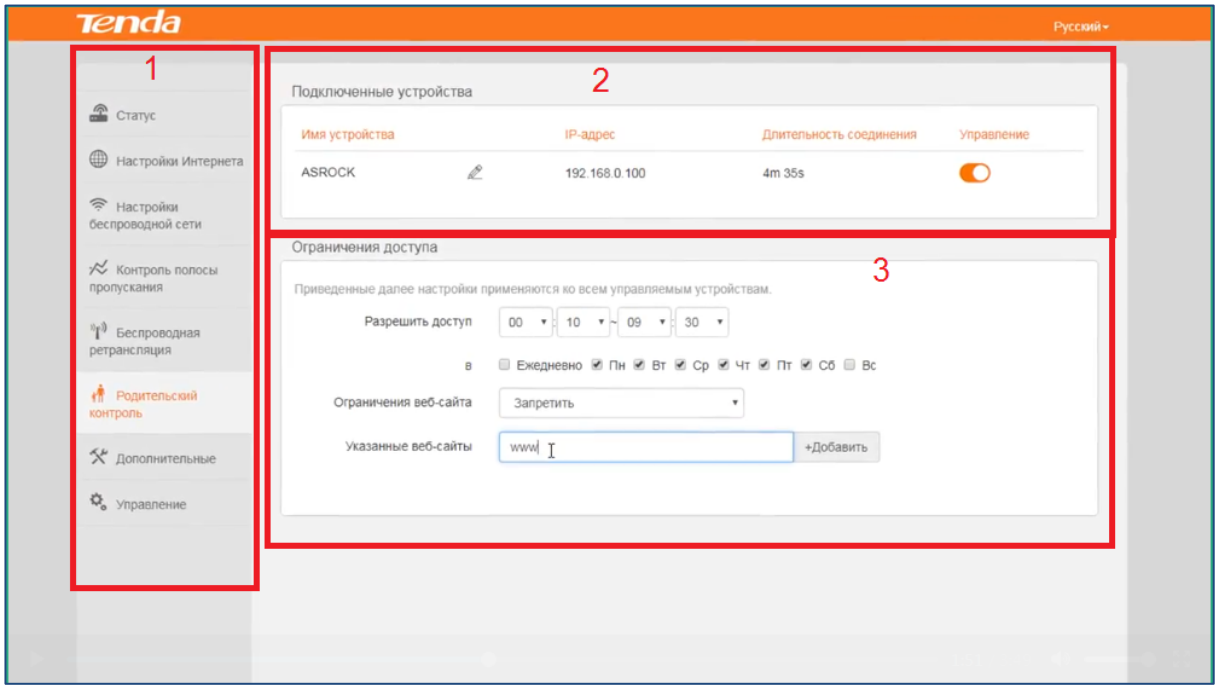

Рисунок 8 — Внешний вид интерфейса маршрутизатора

Маршрутизатор Tp-Link

Откройте «Базовые настройки» или «Дополнительные настройки». Выберите «Родительский контроль» и включите его (рисунок 9).

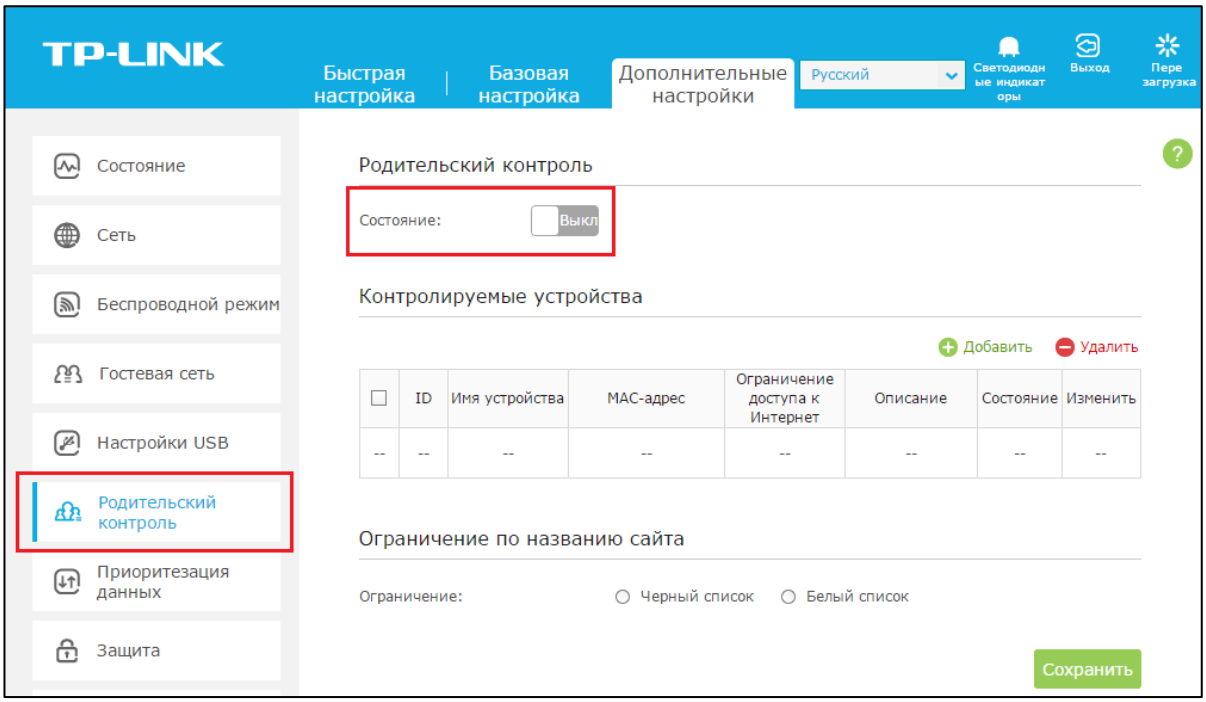

Рисунок 9 — Включение родительского контроля

Нажмите «Добавить».

Нажмите кнопку «Просмотр существующих устройств» и выберите устройство, которое хотите контролировать. Или введите имя устройства и MAC-адрес вручную (рисунок 10).

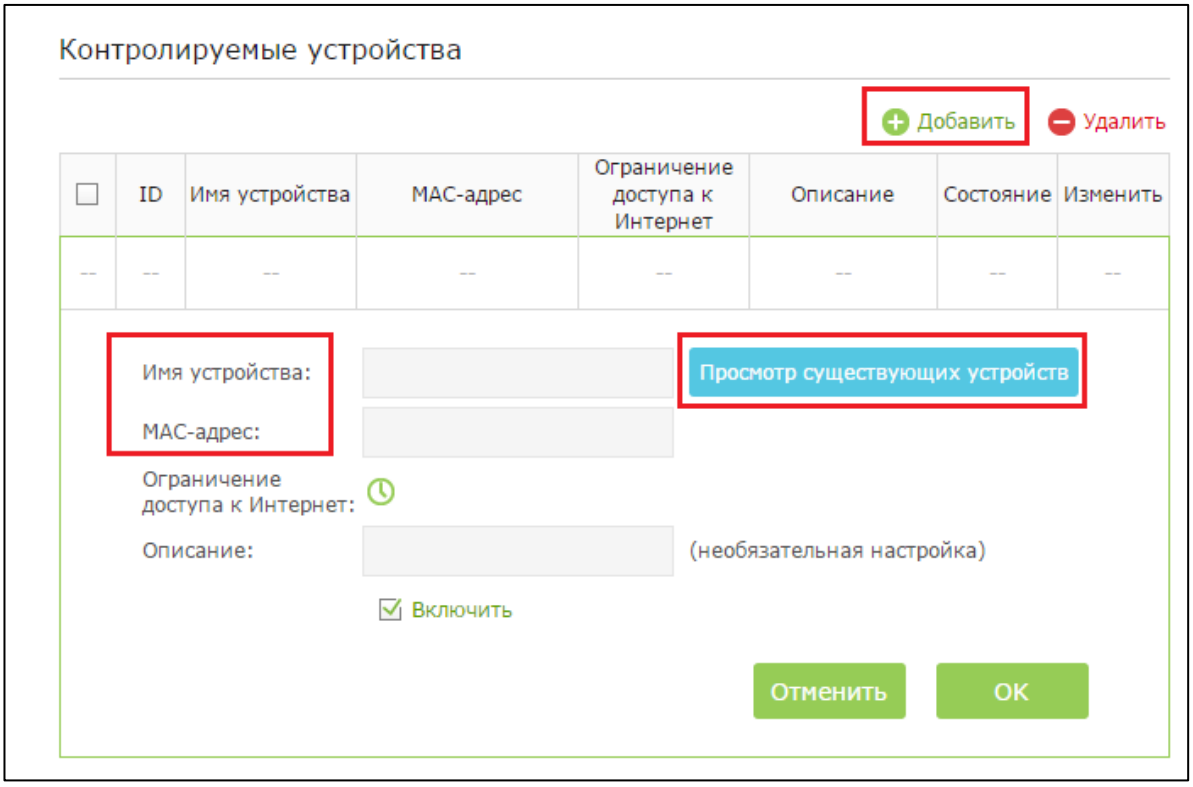

Рисунок 10 — Выбор подключённых устройств

Нажмите значок , чтобы установить время доступа в Интернет. Выделите нужный диапазон времени и нажмите ОК (рисунок 11).

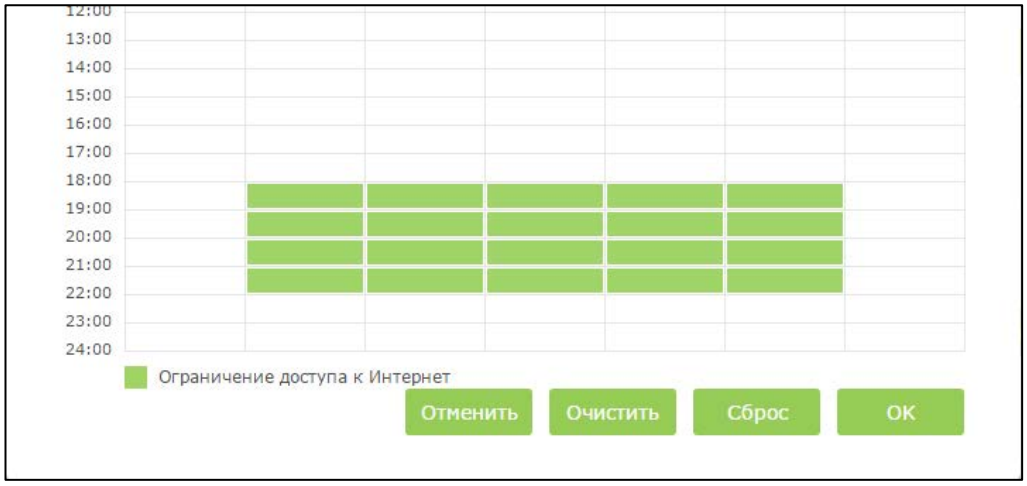

Рисунок 11 — Настройка ограничения на время и дни

Установите флажок, чтобы включить и нажмите ОК.

Выберите тип ограничения:

- когда выбран «чёрный список», управляемые устройства не могут получить доступ к веб-сайтам, содержащим указанные ключевые слова, в течение периода доступа в Интернет;
- при выборе «белого списка» управляемые устройства могут получать доступ к веб-сайтам, содержащим указанные ключевые слова, в течение периода доступа в Интернет.

Нажмите «Добавить новое доменное имя». Можно добавить до 32 ключевых слов для чёрного или белого списка. Введя ключевые слова или веб-сайты, которые необходимо добавить, и нажмите «Сохранить» (рисунок 12).

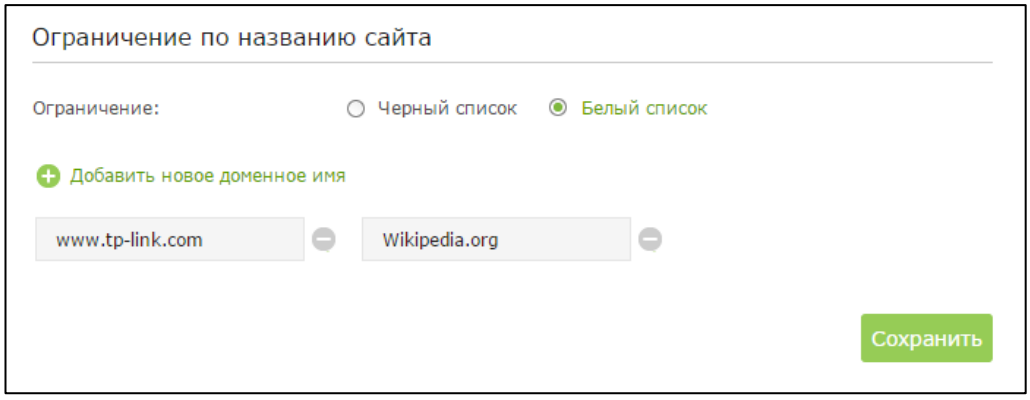

Рисунок 12 — Настройка белого списка

Теперь контролируемому устройству разрешён доступ только к www.tp-link.com и Wikipedia.org, с 18:00 до 22:00 в будние дни, в другие дни доступ в Интернет будет отключён.

Маршрутизатор Asus

Зайдите в раздел «Родительский контроль», переведите переключатель в положение «ON» (рисунок 13).

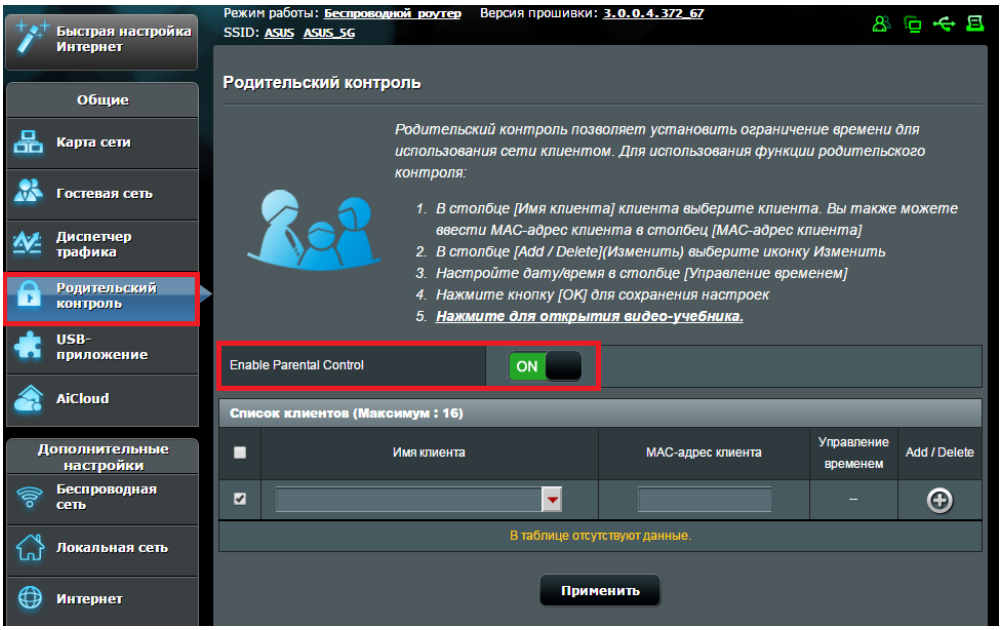

Рисунок 13 — Родительский контроль

Выберите клиента сети из списка, для которого надо применить «Родительский контроль» и нажать на  для добавления клиента (рисунок 14).

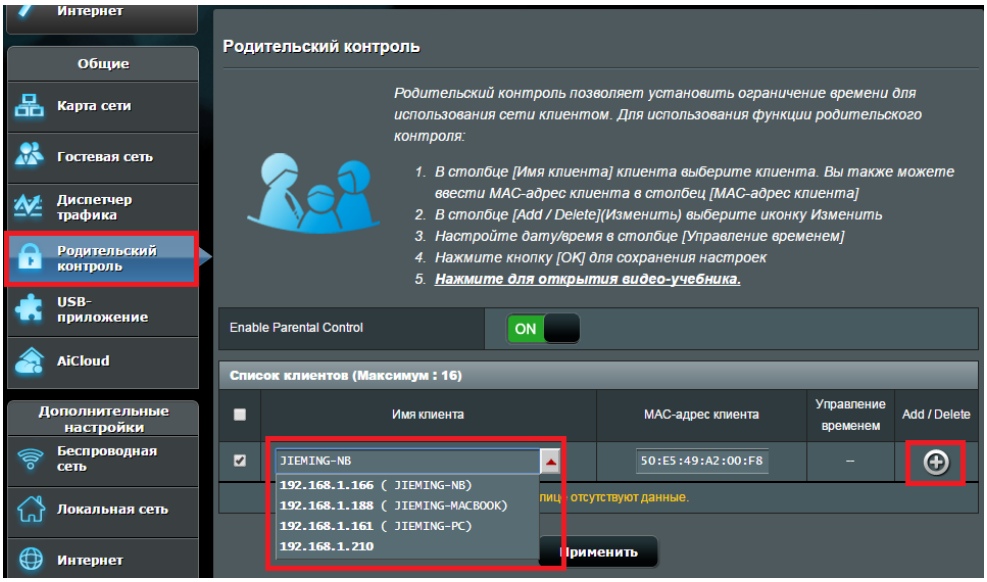

Рисунок 14 — Добавление клиента

Нажмите на иконку  в строке клиента для управления временем (рисунок 15).

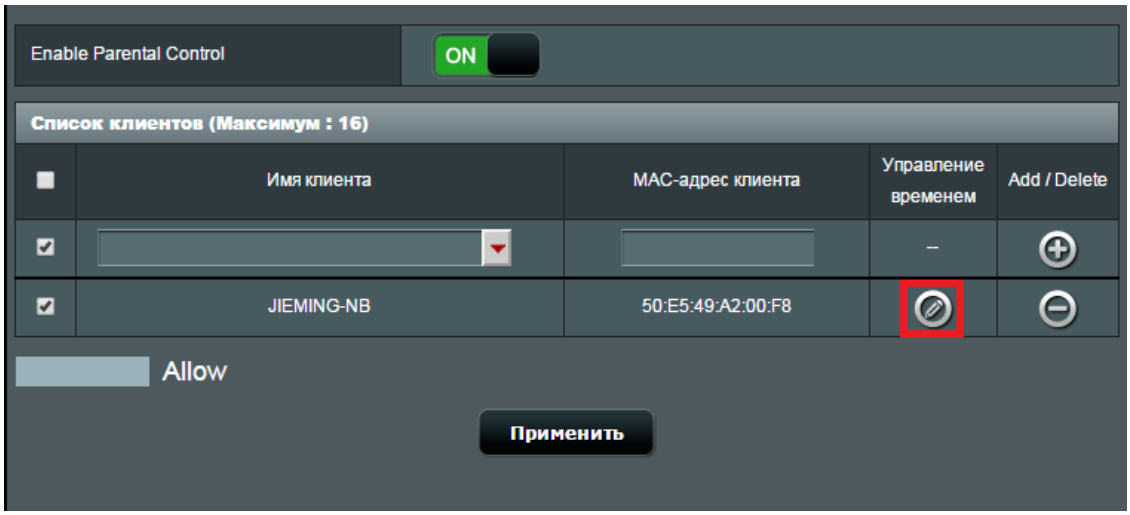

Рисунок 15 — Переход к управлению временем

Отметьте светлосерыми полями дни и время, когда не будет действовать «Родительский контроль».

Нажмите «ОК» для сохранения настроек (рисунок 16).

Рисунок 16 — Настройка времени и дней

Нажмите «Применить» для сохранения настроек.

Яндекс.DNS. Уже касались темы фильтрации контента через настройки маршрутизатора, но используя встроенный брандмауэр, можно лишь заблокировать те сайты, которые знаете сами, всех же сайтов, которые могут быть опасны, самим не отследить. И тут приходит на помощь один замечательный сервис для защиты всех пользователей маршрутизатора — Яндекс.DNS, который на основе своей собранной статистики отслеживает такие ресурсы и объединяет их в одни большой «чёрный список». Главное назначение нового сервиса — обеспечение безопасности при работе в Интернете.

Инструмент может работать в трёх режимах (рисунок 17):

- полный доступ;
- фильтрация мошеннических и вредоносных сайтов;
- фильтр Интернета для детей, совмещающий в себе блокировку как инфицированных ресурсов, так и сайтов с контентом «для взрослых».

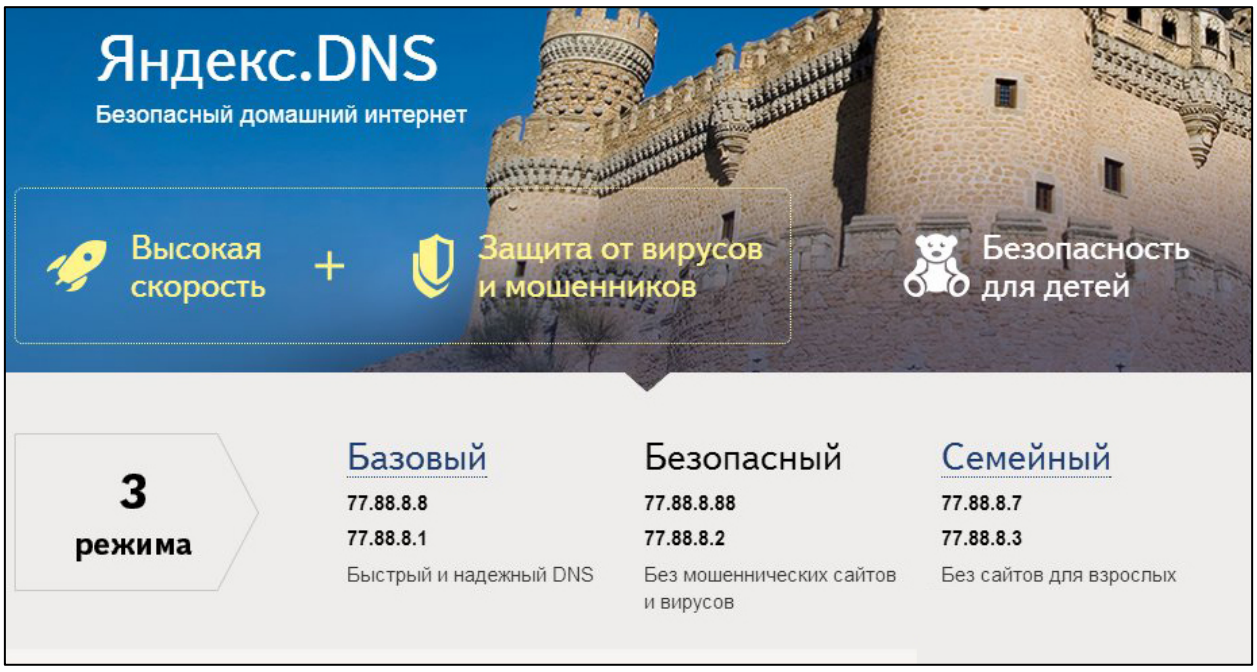

Рисунок 17 — Яндекс.DNS

Выбор режима защиты происходит при помощи добровольного подключения локальной сети или отдельного устройства к одному из серверов «Яндекса».

Пользователи не смогут самостоятельно вносить сайты в категорию блокируемых, но могут оповестить «Яндекс» о сайте, который необходимо заблокировать (через обратную связь).

Подключение к серверу «Яндекса» можно произвести стандартным способом — при помощи соответствующих настроек DNS-сервера маршрутизатора, мобильного устройства или компьютера. Настройки по умолчанию подразумевают, что DNS-фильтр в маршрутизаторе отключён.

Обеспечить блокировку сайтов можно и без роутера на отдельном компьютере или ноутбуке (рисунок 18).

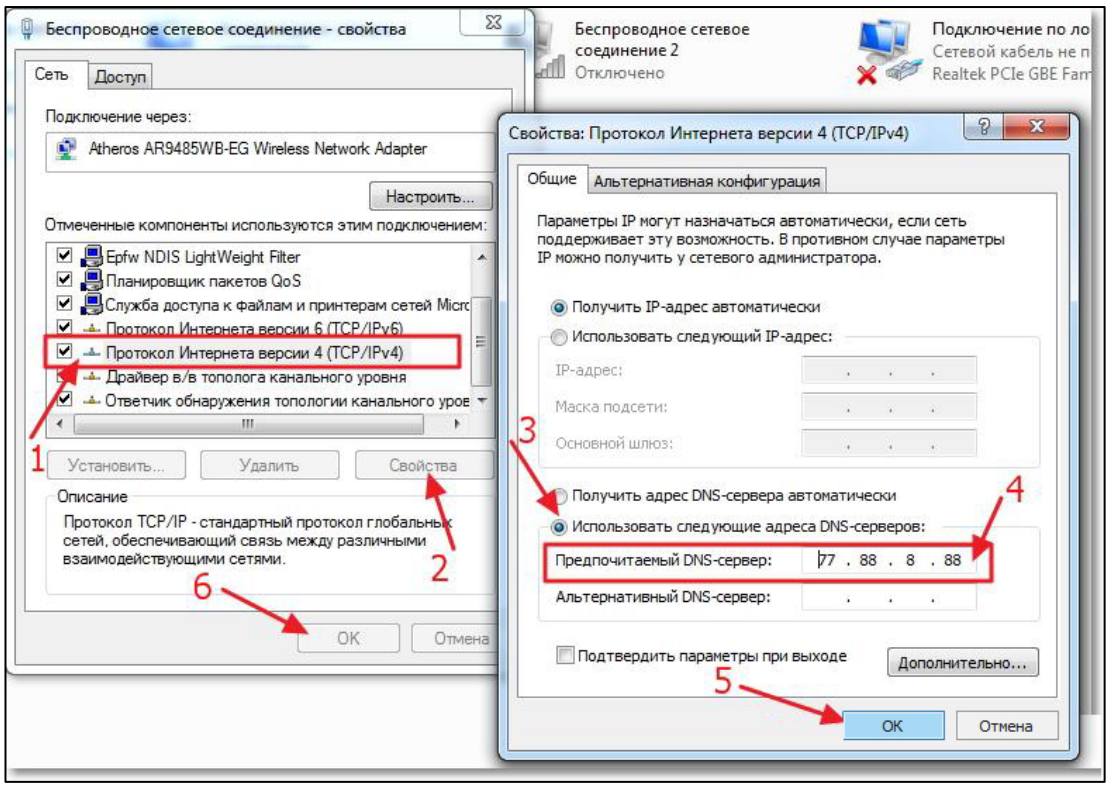

Рисунок 18 — Настройка Яндекс.DNS на компьютере

2.4 Описание экспертной системы

2.4.1 Интерфейс экспертной системы

Экспертная система реализована в формате HTML и открывается запуском ярлыка «ЭС ИПБ». После загрузки титульной страницы (рисунок 19), надо щёлкнуть на белый фон.

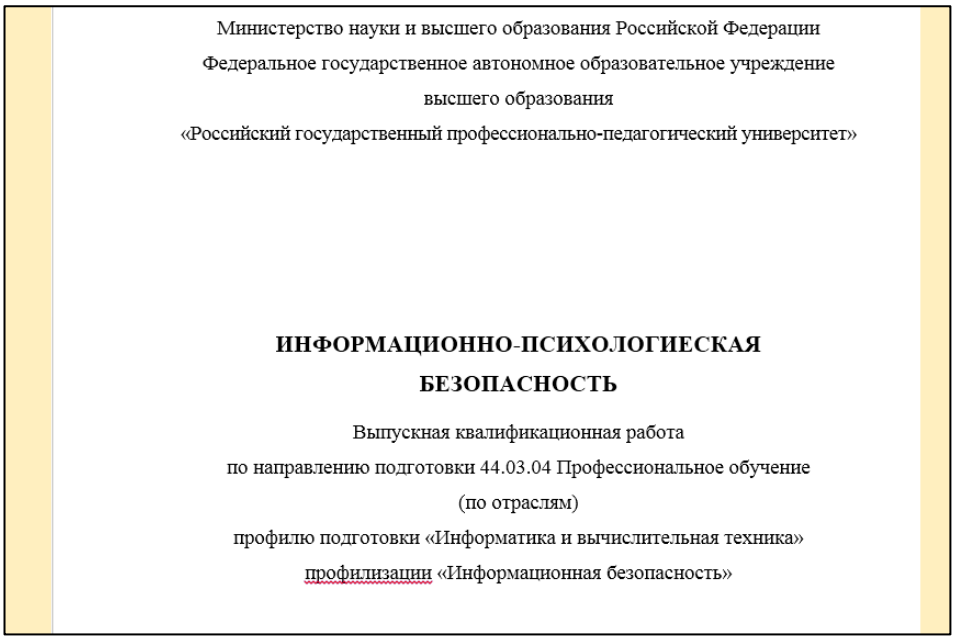

Рисунок 19 — Стартовая страница

Далее пользователь видит главную страницу, представленную на рисунке 20. На ней располагается определение «Информационно-психологическая безопасность» и основные цели обеспечения информационно-психологической безопасности, а так же ссылка для перехода к вопросам (рисунок 21).

Рисунок 20 — Главная страница

Рисунок 21 — Переход к вопросам

Отвечая на вопросы (рисунок 22), можно прийти к одному из нескольких решений (рисунок 23).

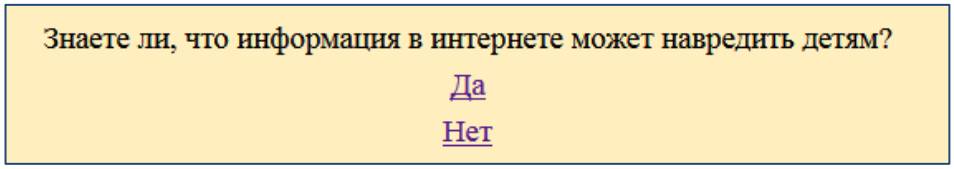

Рисунок 22 — Вопросы системы

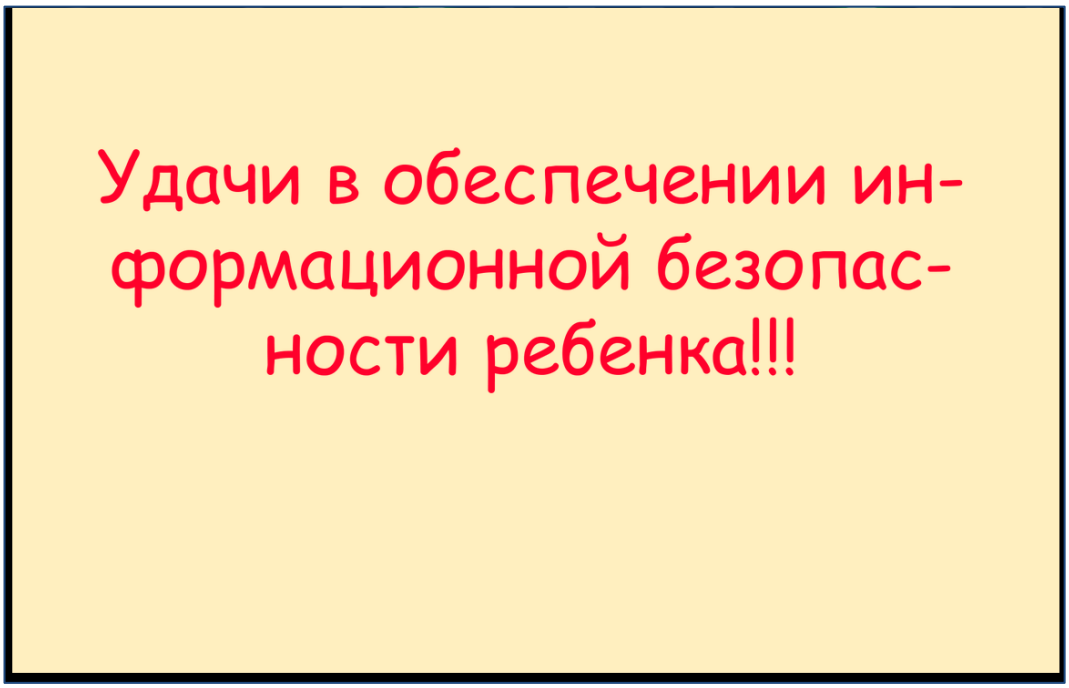

Рисунок 23 — Один из результатов опроса

Некоторые термины в тексте темы выделены. Чтобы читатели обратили на них внимание (рисунок 24).

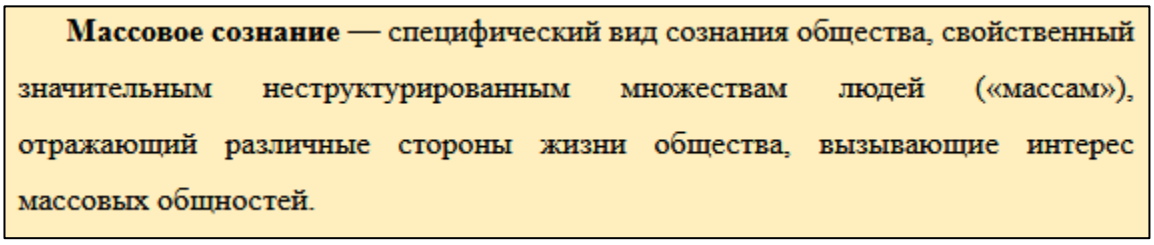

Рисунок 24 — Выделенный термин

В подразделе «Родительский контроль в Windows» можно ознакомится с настройкой контроля на примере Windows 7 с помощью встроенной функции Windows, которая будет использоваться для самостоятельной работы.

2.4.2 Техническое расширение экспертной системы

Поскольку ЭС реализована в формате HTML, то для её расширения необходимо создать новые страницы на языке html (рисунок 25) и написать вопросы с вариантами ответов виде ссылок на соответствующие страницы.

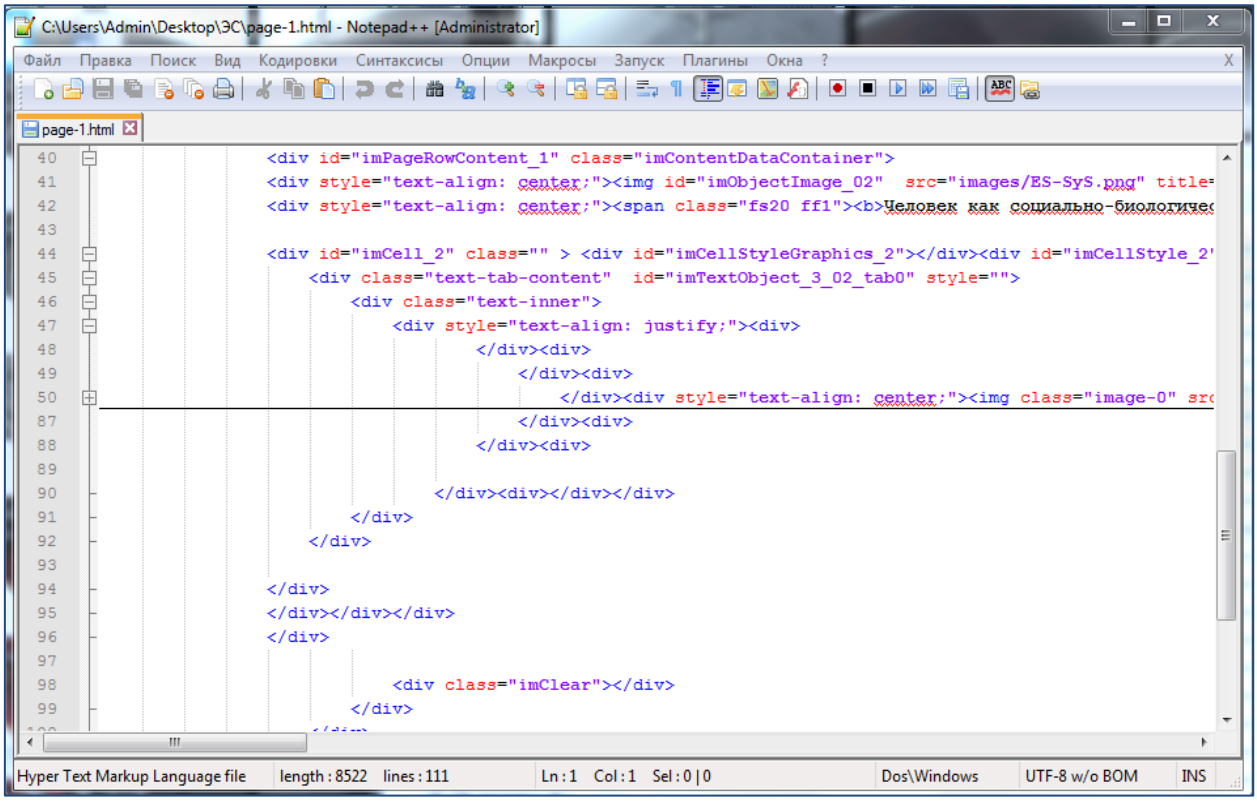

Рисунок 25 — Страница реализованная на языке гипертекстовой разметки

Поместить созданную страницу в папку, где расположены остальные компоненты системы (рисунок 26).

Если на странице есть видеофайлы или изображения, то разместить их в соответствующих папках.

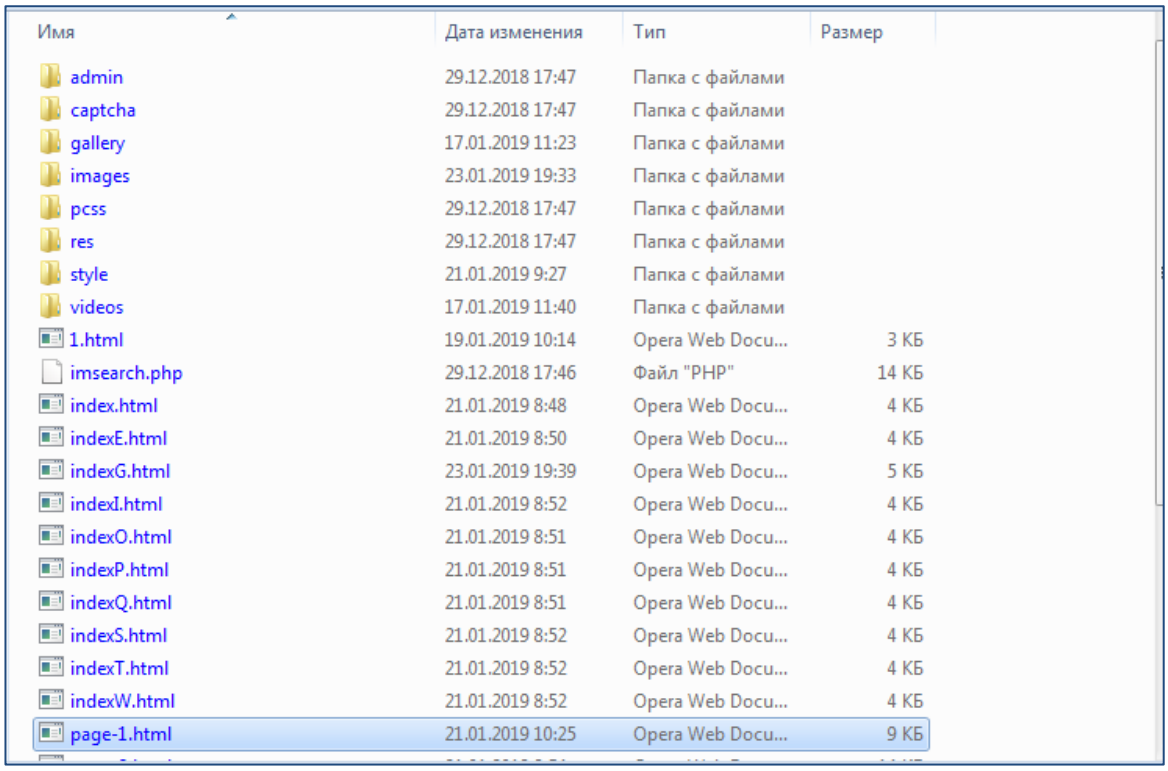

Рисунок 26 — Внешний вид базы фактов экспертной системы

2.4.3 Описание среда разработки модели знаний Wi!Mi

После открытия приложения Wi!Mi (КЭСМИ) [33] автоматически создаётся новая модель. Если она была закрыта, пользователь может создать новую модель. Для этого необходимо в главном меню выбрать пункт «Файл» и в соответствующем контекстном меню выбрать пункт «Создать проект» (рисунок 27). Если перед созданием новой модели имеются несохраненные данные, соответствующее диалоговое окно уведомит вас об этом.

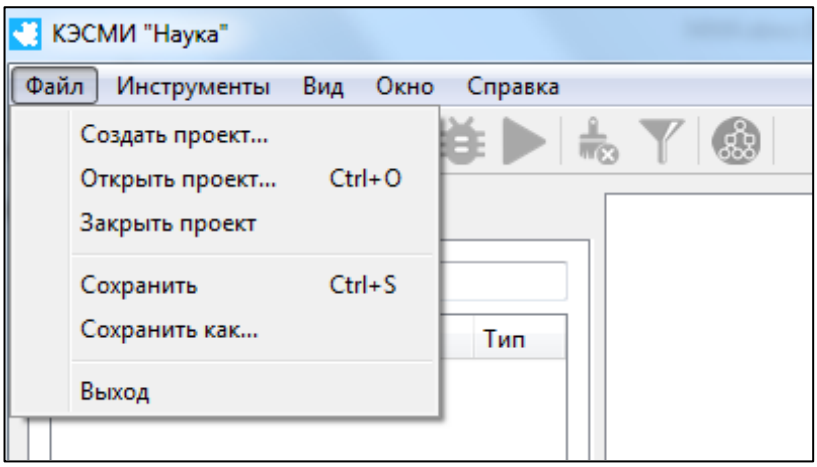

Рисунок 27 — Меню файл

Также пользователь может продолжить работу с существующей моделью. Для этого необходимо выбрать пункт «Открыть проект» из меню «Файл». В появившемся диалоге выберите интересующую модель. Файлы модели хранятся в формате eXtensible Markup Language (XML).

Чтобы закрыть текущую модель без закрытия приложения нажмите на пункт «Закрыть проект» из меню «Файл».

Если необходимо сохранить изменения, сделанные в текущей модели, воспользуйтесь меню «Файл» и выберите пункт «Сохранить» для сохранения изменений в активной вкладке или пункт «Сохранить всё» для сохранения изменений во всех открытых вкладках в текущий файл модели или «Сохранить как...», если требуется сохранить модель в новый файл.

Осуществить перечисленные выше операции можно также с помощью нажатия на соответствующие кнопки на панели инструментов (рисунок 28).

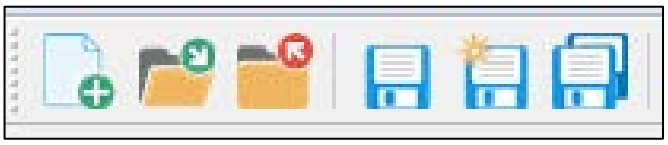

Рисунок 28 — Панель инструментов

После загрузки модели все объекты будут располагаться в древовидном списке в левой части приложения, а все отношения — в правой части. Редактирование соответствующих элементов модели производится в вкладках, расположенных в центральной части приложения. Если в процессе создания модели были обнаружены ошибки, соответствующие записи появятся в списке в нижней части приложения (рисунок 29).

Класс — абстрактная сущность, собирающее понятие. Класс может содержать в себе параметры и другие классы. Класс также имеет название, уровень иерархии и описание.

В любой модели должен существовать хотя бы один класс. Класс с высшим уровнем иерархии называют «корневым». При создании новой модели, по умолчанию также создаётся «корневой» класс.

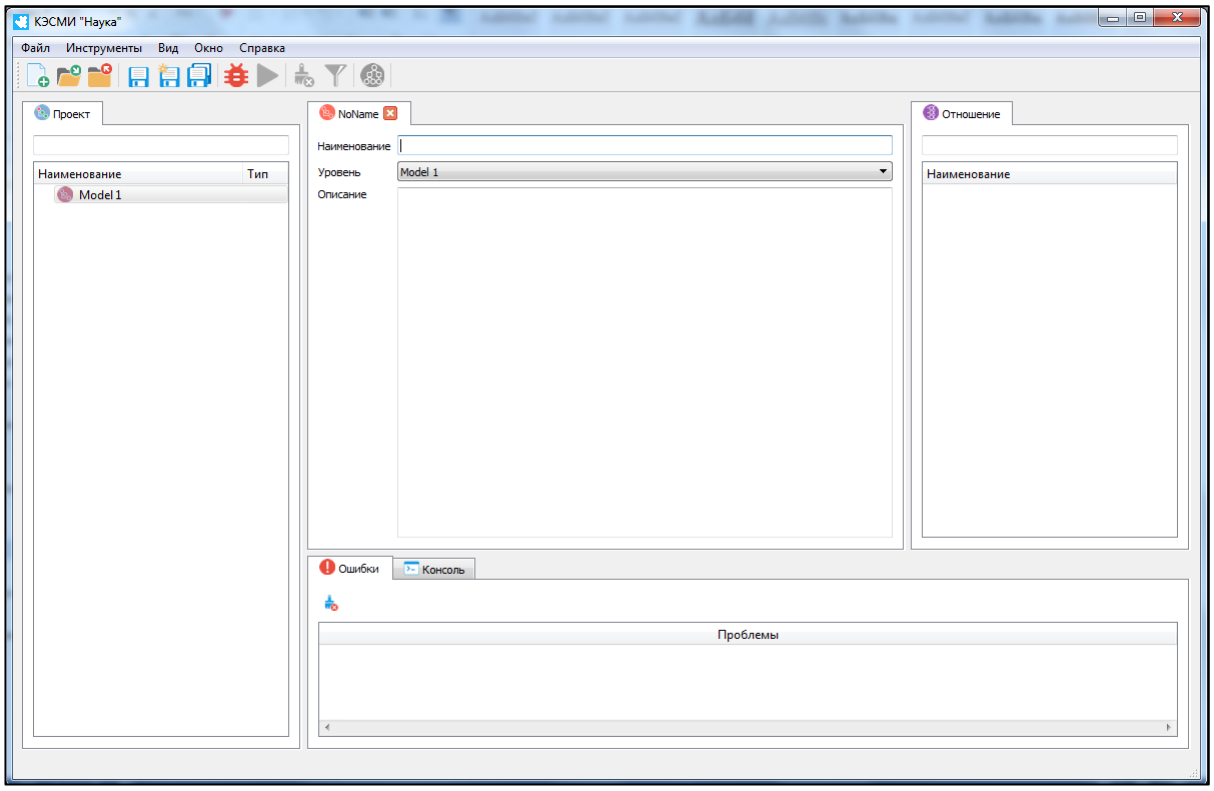

Рисунок 29 — Основное окно приложения

Чтобы создать, отредактировать или удалить класс, необходимо воспользоваться контекстным меню (рисунок 30), вызываемым щелчком правой кнопкой мыши по существующему классу из древовидного списка в левой части окна.

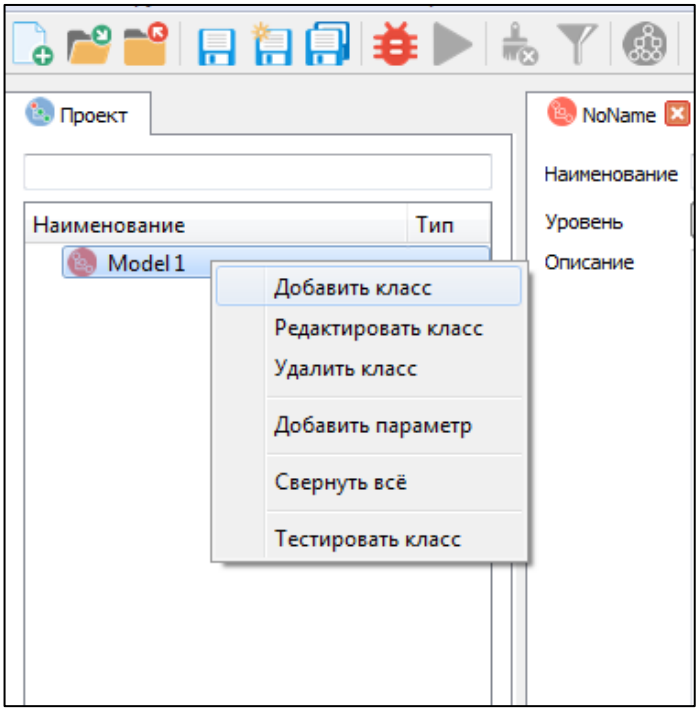

Рисунок 30 — Контекстное меню, вызываемое по щелчку на классе

После нажатия кнопок «Добавить класс» или «Редактировать класс» откроется новая вкладка в центральной части окна, позволяющая совершить соответствующие операции (рисунок 31).

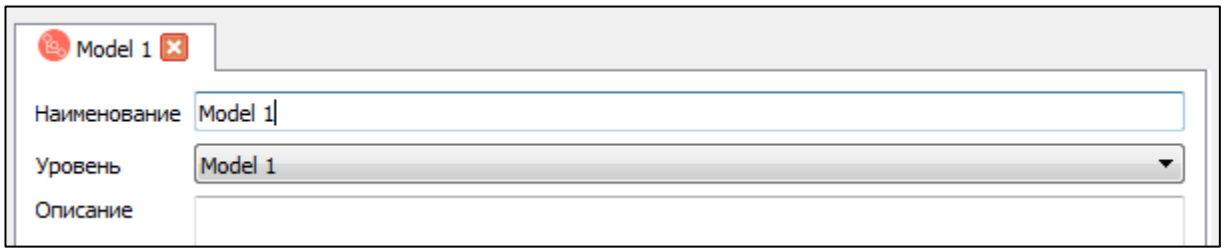

Рисунок 31 — Вкладка, предназначенная для редактирования класса

В появившейся вкладке пользователь может изменить название, поменять уровень иерархии, выбрав новый родительский класс из выпадающего списка, а также, по желанию, добавить описание.

Чтобы применить изменения или завершить процесс создания нового класса, сохраните модель. Новый или изменённый класс будет отображаться в списке в левой части окна.

Параметр — это объект, содержащий значение определённого типа: числового или текстового. Как и класс, параметр имеет название, уровень иерархии и описание. Кроме того, параметр может принимать какое-то значение по умолчанию.

Чтобы создать параметр, необходимо выбрать класс, внутри которого он будет создан, правым щелчком мыши по этому классу вызвать контекстное меню и выбрать пункт

«Добавить параметр» (см. рисунок 30). Для редактирования или удаления существующего параметра, необходимо воспользоваться контекстным меню, вызываемым щелчком правой кнопкой мыши по конкретному параметру из древовидного списка в левой части окна (рисунок 32).

После нажатия кнопок «Добавить параметр» или «Редактировать параметр» откроется новая вкладка в центральной части окна, позволяющая редактировать параметр (рисунок 33).

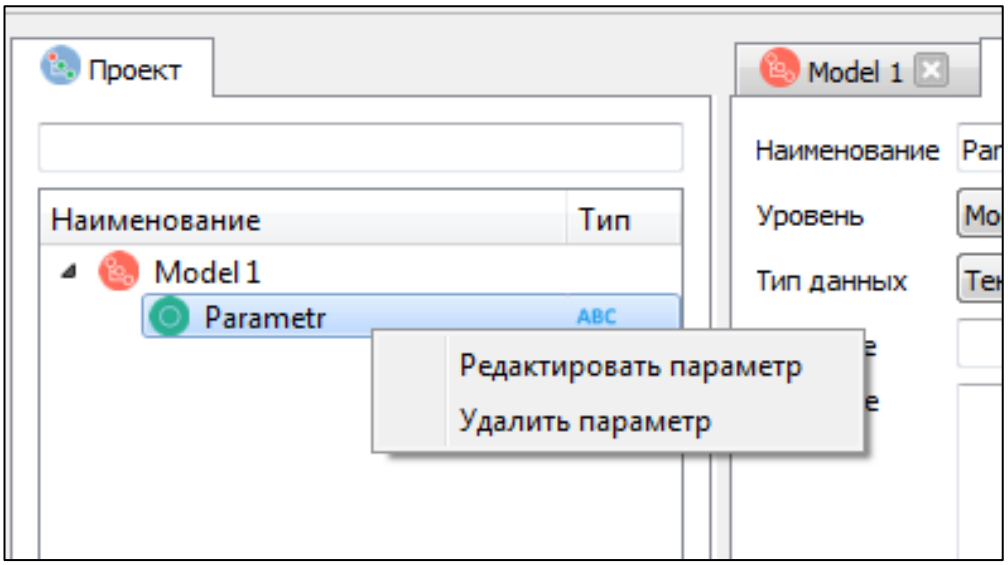

Рисунок 32 — Контекстное меню, вызываемое по щелчку на параметре

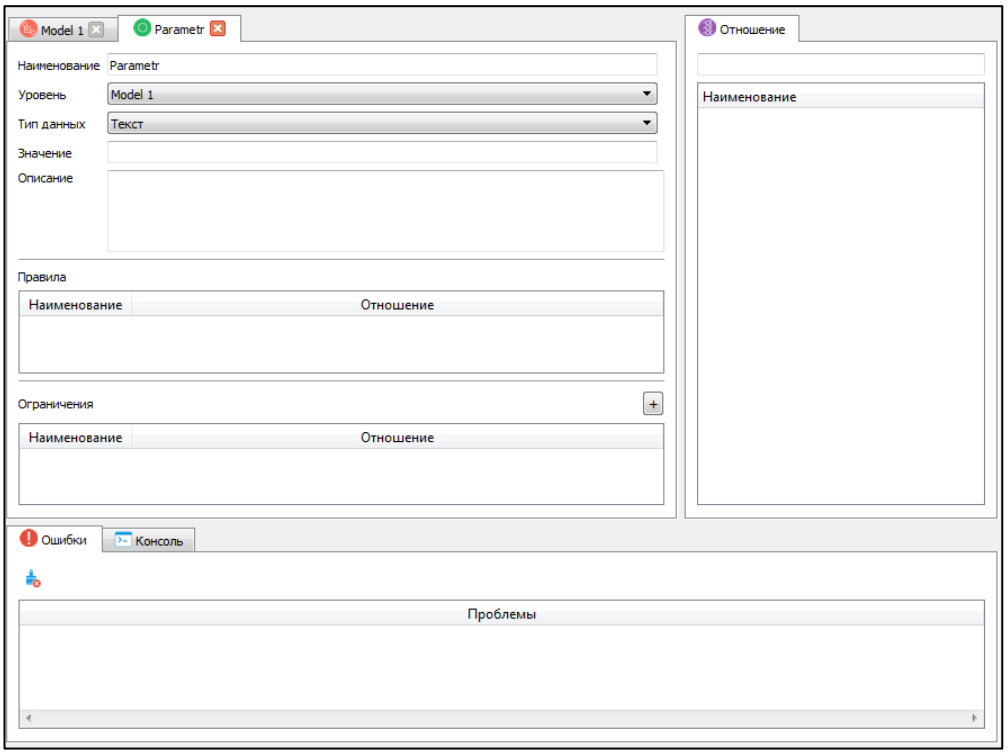

Рисунок 33 — Вкладка, предназначенная для редактирования параметра

В появившейся вкладке пользователь может изменить наименование параметра, поменять уровень иерархии и тип данных. Помимо обязательных свойств, пользователь также может добавить значение по умолчанию и описание. Кроме того, в данной вкладке также существует две таблицы, отображающие связанные с конкретным параметром правила и ограничения. Каждая таблица состоит из двух столбцов: в первом отображается название, а во

втором — отношение, с которым связано соответствующее правило или ограничение. Чтобы применить изменения или завершить процесс создания нового параметра сохраните модель. Новый или изменённый параметр будет отображаться в списке в левой части окна.

Чтобы отобразить граф решения (рисунок 34), необходимо выполнить тестирование модели. В случае успешного тестирования откройте меню «Инструменты» и выберите пункт

«Отобразить граф». Так же это можно сделать, нажав на соответствующую кнопку на панели инструментов

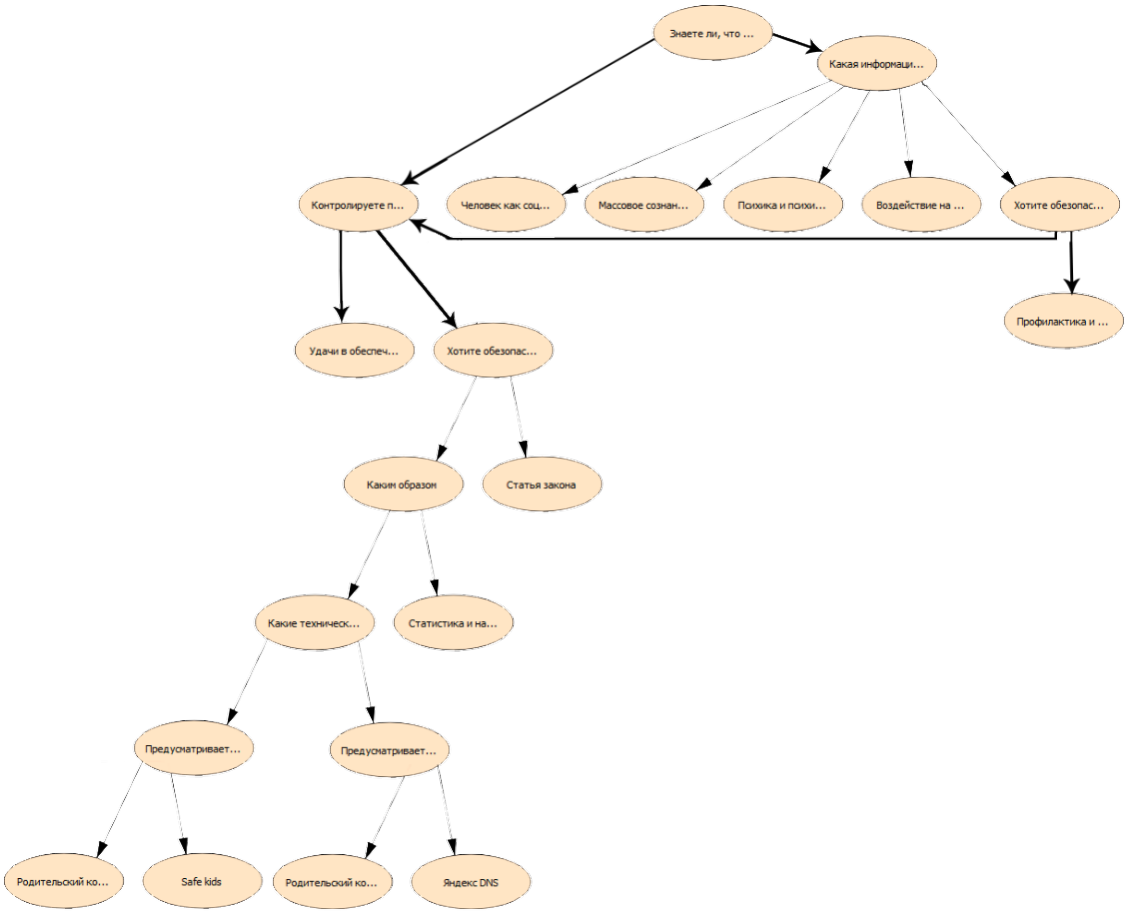

Рисунок 34 — Граф решений

Правила обозначаются прямоугольниками, параметры — эллипсами. При щелчке по правилу отображаются все входящие и выходящие параметры, которые соединяются с правилом зелёными и красными стрелками соответственно. Щелчок по параметру показывает все связанные с ним правила и параметры. Около каждого параметра обозначается его текущее значение. Пе-

ремещаться по графу можно используя полосы прокрутки и мышь. Для перемещения с помощью мыши, наведите курсор на пустое место на графе, опустите левую кнопку мыши, и, не отпуская кнопку, перемещайте курсор. Вместе с движением курсора будет перемещаться и граф.

Если щёлкнуть на какое-либо правило двойным щелчком, то будет отображена лишь часть графа, состоящая из данного правила и связанных с ним входных и выходных параметров. Для возврата к обзору полного графа необходимо снова осуществить двойной щелчок по правилу.

Существует возможность вывода графа на печать. Для этого откройте окно графа и щёлкните на кнопке «Распечатать граф». В открывшемся диалоговом окне, выберите нужные параметры. По завершению настройки нажмите на кнопку «Печать».

ЗАКЛЮЧЕНИЕ

Негативное информационно-психологическое воздействие, являющееся определяющим для информационно-психологической безопасности, может быть сформулировано как информационно-психологическое воздействие на человека, на групповое, массовое и общественное сознание с целью явного или скрытого побуждения индивидуальных и социальных субъектов к действиям в ущерб собственным интересам в интересах отдельных лиц, групп или организаций, осуществляющих это воздействие.

Осознание грозной реальности существования информационно-психологических воздействий вызывает необходимость внимательного рассмотрения проблем обеспечения защиты индивидуального, группового, массового и общественного сознания от подобных воздействий, имеющих негативный (деструктивный) характер. Возможность деструктивного информационно-психологического воздействия на человека с целью модернизации его психики может привести к катастрофическим последствиям для государства, не принявшего заблаговременных мер по нейтрализации такого воздействия. С целью парирования угроз информационно-психологической безопасности страны, необходимо на государственном уровне принять законодательные акты по защите личности и общества от негативных информационно-психологических воздействий, а также разработать и приступить к реализации программы использования психотехнологий в интересах государства.

В рамках выпускной квалификационной работы создана экспертная система «Информационно-психологическая безопасность», которая включает в себя теоретический и практический материал.

При выполнении выпускной квалификационной работы Мы отталкивались от следующего понятия экспертной системы. В области компьютерных наук экспертная система рассматривается вместе с базой знаний как модель

поведения эксперта в области знаний с использованием процессов вывода и принятия решений, а база знаний служит набором фактов и правил вывода в выбранных предметных областях.

Обзор источников информации показал, что литературы по данной тематике довольно много, но основная масса написана ещё в 20-ом веке и иногда перепечатывается, а новых исследований в этой области очень мало.

В результате проделанной работы были решены следующие задачи:

1. Проанализирована литература и интернет-источники с целью выделения требований, предъявляемых к созданию экспертных систем на современном этапе развития образования. Так же проанализирована литература для формирования круга печатных и электронных изданий, рассматривающих область «информационно-психологической безопасности».

2. Выделены теоретические блоки по теме «Информационно-психологическая безопасность», с целью формирования тематических рекомендаций по рассматриваемой теме.

3. Смоделирован процесс принятия решений экспертной системой.

4. Реализована экспертная система «Информационно-психологическая безопасность»

СПИСОК ИСПОЛЬЗОВАНЫХ ИСТОЧНИКОВ

1. Асанович В. Я. Информационная безопасность: анализ и прогноз информационного воздействия [Текст] / В. Я. Асанович, Г. Г. Маньшин. — Минск: Амалфея, 2006. — 320 с.

2. Астахова Л. В. Критическое мышление как средство обеспечения информационно-психологической безопасности личности [Текст] / Л. В. Астахова, Т. В. Харлампьева. — Москва: Эксмо, 2009. — 136 с.

3. Бабаева Ю. Д. Психологические последствия информатизации [Текст] / Ю. Д. Бабаева, А. Е. Войскунский // Психологический журнал. — 1998. — №1. — С. 89–100.

4. Баришполец В. А. Основы информационно-психологической безопасности [Текст] / В А Баришпольца. — Москва: МГФ Знание, 2012. — 413 с.

5. Белоножкин В. И. Информационные аспекты противодействия терроризму [Текст] / В. И. Белоножкин, Г. А. Остапенко. — Москва: Горячая линия-Телеком, 2009. — 112 с.

6. Влияние TV и компьютеров на душу ребёнка [Электронный ресурс]. — Режим доступа: http://medicinform.net/comp/comp_psych1.htm (дата обращения: 23.10.2018).

7. Высокотехнологический терроризм [Текст]: материалы рос.-амер. семинара. — Москва: Российская академия наук, 2002. — 320 с.

8. Гаврилова Т. А. Базы знаний интеллектуальных систем [Текст]: учебник / Т. А. Гаврилова, В. Ф. Хорошевский. — Санкт-Петербург: Питер, 2000. — 384 с.

9. Галицкий Е. Б. Опросы «Интернет в России». 2002 [Электронный ресурс]. — Режим доступа: https://bd.fom.ru/report/map/o0312303 (дата обращения: 10.12.2018).

10. Гафнер В. В. Информационная безопасность [Текст] / В. В Гафнер. — Ростов-на-Дону: Феникс, 2010. — 336 с.

11. Грачев Г. В. Информационно-психологическая безопасность личности [Электронный ресурс]. — Режим доступа: http://www.e-reading.club/bookreader.php/106938/Grachev_-_Informacionno-psihologicheskaya_bezopasnost'_lichnosti.html (дата обращения: 11.12.2018).

12. Губанов В. М. Чрезвычайные ситуации социального характера и защита от них [Текст] / В. М Губанов, Л. А. Михайлов, В. П. Соломин. — Москва: Дрофа, 2007. — 288 с.

13. Джарратано Джозеф Экспертные системы: принципы разработки и программирование [Текст] / Джозеф Джарратано, Гари Райли. — пер. с англ. — Москва: Вильямс, 2006. — 1152 с.

14. Доктрина информационной безопасности Российской Федерации [Электронный ресурс]. — Режим доступа: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 10.12.2018).

15. Доценко Е. Л. Психология манипуляции: феномены, механизмы и защита [Текст] / Е. Л. Доценко. — Санкт-Петербург: Питер, 2004. — 265 с.

16. Жичкина А. Взаимосвязь идентичности и поведения в Интернете пользователей юношеского возраста [Электронный ресурс]. — Режим доступа: http://flogiston.ru/articles/netpsy (дата обращения: 10.12.2018).

17. Жичкина А. Е. Особенности социальной перцепции в Интернете [Текст] / А. Е Жичкина. — Москва: Мир психологии, 1999. — №3. — С. 72–80.

18. Касперски К. Техника и философия хакерских атак [Текст] / К. Касперски. — Москва: Солон-Р, 2004. — 272 с.

19. Количество пользователей Интернета в России [Электронный ресурс]. — Режим доступа: http://www.bizhit.ru/index/users_count/0-151 (дата обращения: 12.01.2019).

20. Кузнецова Ю. М. Психология жителей Интернета [Текст] / Ю. М. Кузнецова, Н. В. Чудова. — Москва: ЛКИ, 2008. — 224 с.

21. Манойло А. В. Государственная информационная политика в условиях информационно-психологической войны [Текст] / А. В. Манойло, А. И. Петренко, Д. Б. Фролов. — Москва: Горячая линия-Телеком, 2009. — 320 с.

22. Основы национальной безопасности [Текст]: учеб. пособие. — Москва: Академия, 2008. — 270 с.

23. Почепцов Г. Г. Информационно-психологическая война [Текст] / Г. Г Почепцов. — Москва: СИНТЕГ, 2000. — 529 с.

24. Рындюк В. А. Основы информационной безопасности [Текст] / рабочая программа / В. А. Рындюк. — Пятигорск: ФГБОУ ВО «Пятигорский государственный университет», 2018. — 33 с.

25. Рысин Ю. С. Социально-информационные опасности телерадиовещания и информационных технологий [Текст] / Ю. С Рысин. — Москва: Гелиос АРВ, 2007 — 272 с.

26. Самохвалова В. И. «Массовый человек» — как герой и потребитель масскульта [Электронный ресурс]. — Режим доступа: http://koi.tspu.ru /koi_books/poleva1/samohvalova.htm (дата обращения: 13.12.2018).

27. Смолян Г. Л. Сетевые информационные технологии и проблемы безопасности личности [Текст] / Г. Л Смолян // Информационное общество. — 1999. — №1. — С. 21–25.

28. Стариков Н. В. «Западная пропаганда, как она работает и форматирует мозги всем народам мира» [Электронный ресурс]. — Режим па: http://soborjane.ru/2016/10/15/zapadnaya-propaganda-kak-ona-rabotaet-i-formatiruet-mozgi-vsem-narodam-mira/ (дата обращения: 12.01.2019).

29. Уфимцев Ю. С. Информационная безопасность России [Текст] / Ю. С. Уфимцев, Е. А. Ерофеев, В. П. Буянов др. — Москва: Экзамен, 2003. — 560 с.

30. Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.01 Организация и технология защиты информации [Электронный ресурс]: Приказ Минобрнауки России от 28.07.2014 N 805 — Режим доступа: http://pglu.ru/upload/iblock/803/10.02.01-organizatsiya-i-tekhnologiya-zashchity-informatsii.pdf (дата обращения: 20.12.2018).

31. Юсупов Р. М. Наука и национальная безопасность [Текст] / Р. М. Юсупов. — Санкт-Петербург: Наука, 2011. — 369 с.

32. Web-canape [Электронный ресурс] — Режим доступа: https://www.web-canape.ru/business/internet-2017-2018-v-mire-i-v-rossii-statistika-i-trendy/ (дата обращения: 12.01.2019).

33. Wi!Mi (КЭСМИ) — среда разработки моделей знаний [Электронный ресурс]. — Режим доступа: http://mivar.ru/products/wimi-kesmi (дата обращения: 12.01.2019).

ПРИЛОЖЕНИЕ