Рекомендации по выбору оптимальной (для конкретного пользователя/организации) системы фильтрации контента

Ноябрь 2015

Одесская национальная
академия связи
им. А.С. Попова, Украина

Международный союз
электросвязи,
Бюро развития электросвязи

Рекомендации по выбору оптимальной (для конкретного пользователя/организации) системы фильтрации контента подготовлены Бюро развития электросвязи МСЭ в рамках реализации региональной инициативы стран СНГ «Создание центра по защите ребёнка в сети Интернет для региона СНГ», принятой на Всемирной конференции по развитию электросвязи 2014 года (Дубай, ОАЭ) при поддержке Одесской национальной академии связи им. А.С. Попова (Украина).

Данные рекомендации являются составляющей частью проекта по созданию единой базы данных с информацией про существующие технические решения и системы выбора оптимальной (для конкретного пользователя/организации) системы фильтрации контента.

Просьба подумать об окружающей среде, прежде чем печатать данный документ

Предисловие

Современные информационные технологии предоставляют уникальные возможности для доступа к практически неограниченному объему разнотипной информации. Человек, использующий сеть Интернет, становится полноправным участником глобального информационного социума, в котором его подстерегает немало опасностей. Интернет, как и любой другой инструмент, созданный человечеством, может нести как пользу, так и вред.

Для защиты человека и, особенно, ребенка, от негативной стороны использования сети Интернет рекомендуется использовать комплексный подход, который включает организационно-педагогические и технические меры. Основной технической мерой защиты человека от негативной информации в сети Интернет служит техническая фильтрация информации. Многообразие характеристик систем технической фильтрации информации порождает множество вариантов их построения и, как следствие, огромное количество программных и программно-аппаратных решений, предназначенных для блокирования доступа к информационным ресурсам на различных уровнях и в сетях разного типа.

Появление значительного количества программных и программно-аппаратных решений, предназначенных для блокирования доступа к информационным ресурсам в компьютерных сетях различного типа, поставило перед пользователями новую задачу – задачу выбора наиболее подходящего с технической и экономической точек зрения решения для конкретной ситуации (дома, школы, офиса и т.д.).

Выбор наиболее подходящего для конкретной ситуации решения, как правило, основывается на комплексном анализе множества факторов, таких как: область применения (персональные компьютеры дома, несколько компьютеров в школе, большая компьютерная сеть в учебном заведении, смартфоны и планшеты, подключенные к сети оператора и т.д.), способ подключения к сети Интернет (один или несколько каналов доступа), наличие специалистов для установки и поддержки решения, наличие «свободной» техники для установки нового решения, желаемая политика доступа к сети Интернет и так далее.

Очевидно, что проведение подобного анализа требует привлечения высококвалифицированных специалистов в области фильтрации контента, что не всегда является возможным, особенно в реалиях общеобразовательных учебных заведений региона СНГ. Учитывая это, на Всемирной конференции по развитию электросвязи 2014 года (Дубай, ОАЭ) была принята региональная инициатива «Создание центра по защите детей в онлайн-среде региона СНГ». Одним из базовых проектов этой инициативы стал проект по созданию единой базы данных с информацией про существующие технические решения и системы выбора оптимальной (для конкретного пользователя/организации) системы фильтрации контента, основополагающей частью которого и являются данные Рекомендации.

Хочу выразить благодарность руководству и сотрудникам Международного союза электросвязи в лице Директора Бюро развития электросвязи Брагимы Сану, руководителя Зонального отделения (ЗО) МСЭ для стран СНГ Орозобека Кайыкова и администратора по программам ЗО МСЭ для стран СНГ Андрея Унтилы за всестороннюю поддержку вопроса защита ребёнка в онлайновой среде в нашем регионе.

Пётр Воробиенко
ректор
Одесской национальной академии связи им. А.С. Попова,
д.т.н., профессор,
заслуженный работник образования Украины,
член-корреспондент Академии педагогических наук Украины,
лауреат Государственной премии в области науки и техники Украины

Содержание

Стр.

Введение

Решаемая задача представляет собой построение автоматической рекомендательной системы.

Рекомендательные системы изменили способы взаимодействия веб-сайтов с пользователями. Вместо предоставления статической информации, когда пользователи ищут и, возможно, покупают продукты, рекомендательные системы увеличивают степень интерактивности для расширения предоставляемых пользователю возможностей. Рекомендательные системы формируют рекомендации независимо для каждого конкретного пользователя на основе его прошлых покупок и поисков, а также на основе поведения других пользователей.

Разработка рекомендательных систем была инициирована из достаточно простого наблюдения - люди часто полагаются на рекомендации для решения обычных повседневных задач. Например, при выборе книги для чтения полагаются на советы сверстников; работодатели учитывают рекомендательные письма; при выборе фильма люди часто полагаются на обзоры и мнения кинокритиков и т.д.

Рекомендательные системы предназначены для поиска объектов, которые понравятся пользователю или будут ему полезны. В типичных системах есть список пользователей $U = (u_1, u_2, \ldots, u_m)$ и продуктов $I = (i_1, i_2, \ldots, i_n)$. В ходе взаимодействия с системой пользователи знакомятся с объектами, формируя матрицу рейтингов R, где $r_{uk,i}$ – рейтинг продукта $i_p \in I$ у пользователя $u_k \in U$. Как правило, матрица рейтингов неполная и разреженная, т.к. количество различных продуктов в системе велико и уже известные u_k продукты $I_{uk} \in I$ составляют лишь малую долю от общего числа. Задача рекомендательной системы обычно формулируется как выдача предсказания[1] и рекомендации[2].

Существуют две основные стратегии создания рекомендательных систем: фильтрация содержимого и коллаборативная фильтрация.

При фильтрации содержимого создаются профили пользователей и объектов. Профили пользователей могут включать демографическую информацию или ответы на определённый набор вопросов. Профили объектов могут включать названия объектов, класс объектов, технические характеристики и т.п. - в зависимости от типа объекта.

При коллаборативной фильтрации используется информация о поведении пользователей в прошлом — например, информация о покупках или оценках. В этом случае не имеет значения, с какими типами объектов ведётся работа, рекомендация формируется на основе пользовательских предпочтений.

Планируемая система не предусматривает сбор, хранение и обработку информации о пользовательских предпочтениях, поэтому для ее реализации целесообразно использовать стратегию фильтрации содержимого, которая базируется на профилях пользователей и профилях объектов.

---

[1] Предсказание – численное значение $P_{uk,i}$, выражающее предсказанную предпочтительность продукта $i \notin I_{uk}$ для пользователя u_k.

[2] Рекомендация – список из N продуктов $I_r \in I$, наиболее предпочтительных для пользователя, причем в него входят лишь незнакомые пользователю элементы $I_r \bigcap I = \emptyset$.

1. Классификационная модель пользователей систем фильтрации контента

Множество пользователей $U = \{u_1, u_2, \ldots, u_m\}$ можно описать с помощью классификационной модели. Классификационная модель может быть сформирована на основе следующих критериев:

1. Степень освоения пользователем возможностей, предоставляемых сетью Интернет (технической грамотностью)
2. Цели, преследуемые пользователем
3. Субъект защиты
4. Масштабность задачи

По степени освоения возможностей предоставляемых сетью Интернет, можно выделить следующие классы пользователей:

1. *Новичок* – к данному классу относятся пользователи, которые только начинают осваивать возможности информационных технологий и сети Интернет. Новички «слабо» представляют, как правильно и безопасно использовать возможности сети Интернет. Не имея навыков безопасной работы в сети, «Новички» начинают активно исследовать ее возможности и как следствие, подвергаются различным сетевым угрозам (просмотру нежелательного контента, загрузке вирусов, получению спама и т.д.).
2. *Пользователь* – наиболее многочисленный класс. Люди, которые относятся к данному классу, используют сеть Интернет в качестве инструмента для решения различных повседневных задач (деловых, учебных, развлекательных). «Пользователи» знакомы с основными правилами безопасной работы в сети и имеют достаточно навыков для противодействия наиболее распространенным «классическим» опасностям, но их знаний и умений не хватает, для обеспечения эффективного уровня безопасности в любой ситуации. К данному классу относятся различные категории граждан – родители, педагоги, менеджеры, начальники отделов, руководители, представители органов власти и т.д.
3. *Опытный пользователь* – люди, которые относятся к данному классу, обладают достаточно большим объемом знаний о принципах функционирования и правилах использования того или иного сетевого сервиса. Они прекрасно знают правила безопасной работы в сети, имеют достаточно навыков, чтобы обеспечить качественную защиту одиночной рабочей станции или небольшой сети. Обеспечить надежную защиту сети среднего масштаба или крупной сети они не могут, так как имеют довольно поверхностные знания о принципах функционирования и построения сетей. К данному классу можно отнести, например, инженера, веб-мастера, веб-дизайнера, контент-менеджера, менеджера поисковой оптимизации, геймера и т.п.
4. *Технический специалист* – к данному классу относятся люди, которые обеспечивают качественное и надежное функционирование сетей любого масштаба. Технические специалисты могут организовать надежную и безопасную работу в Интернете для сетей любого масштаба, однако не всегда предложенное решение будет оптимальным по ряду критериев. Это связано с тем, что не всегда технический специалист понимает все нюансы функционирования и использования того или иного средства защиты.
5. *Эксперт* – наименее многочисленный класс. Эксперт – это технический специалист, специфика работы которого связана с информационной безопасностью. Эксперт прекрасно разбирается во всех нюансах и тонкостях организации безопасной работы в сети Интернет и может выбрать оптимальное, по заданному критерию (например, цена/качество), решение для защиты от угроз в сети.

По целям, которые преследует пользователь можно выделить следующие классы:

1. Обеспечение цензуры.
2. Обеспечение контроля нецелевого использования времени проведено в сети Интернет.
3. Обеспечение защиты несовершеннолетних от ресурсов опасных для них и несовместимых с моральными принципами конкретного социума.

4. Предупреждения развития Интернет-зависимости (кибераддикции) как у несовершеннолетних, так и у взрослых.
5. Обеспечение защиты несовершеннолетних от возможного запугивания и преследования (сексуального, психологического) в сети Интернет.
6. Обеспечение выполнения/соблюдения различных социальных, культурных, правовых норм.
7. Обеспечение снижения нагрузки на каналы связи.
8. Обеспечение защиты от компьютерных вирусов.
9. Обеспечение защиты авторского права (борьба с пиратством).
10. Обеспечение защиты экономических интересов (например, бесплатные VoIP программы и сервисы, такие как Skype, могут блокироваться, так как их использование ведет к убыткам компаний стационарной и сотовой связи).
11. Информационная война.
12. Обеспечение предоставления набора различных контент-услуг.
13. Обеспечение выполнения режима чрезвычайного положения.

По субъекту защиты пользователей можно поделить на тех, кому необходимо обеспечить защиту:

1. Населения страны.
2. Социальной группы.
3. Сотрудников предприятия/компании/учреждения.
4. Абонентов.
5. Детей дома.
6. Учеников школы.
7. Студентов ВУЗа.

В зависимости от масштаба решаемой задачи пользователей можно разделить на тех, кому необходимо обеспечить защиту:

1. Персонального устройства подключенного к сети Интернет.
2. Домашней сети пользователя (несколько персональных устройств пользователя объединенных в сеть и подключенных к Интернету через общий шлюз).
3. Сети малого офиса.
4. Сети предприятия/учреждения, в том числе и учебного (образовательного).
5. Сети корпорации.
6. Сети оператора/провайдера.
7. Публичной сети общего доступа.
8. Сети корпорации.
9. Национальной сети.

2. Детализированная классификационная модель систем фильтрации контента в сети Интернет

Как и множество пользователей, множество продуктов (систем фильтрации контента) $I = (i_1, i_2, \ldots i_n)$ может быть описано путём использования классификационной модели. Предлагаемая классификационная модель (рис. 1) представлена в виде двух плоскостей – плоскости базовых характеристик и плоскости специфических характеристик.

В плоскости базовых характеристик для классификации систем фильтрации контента использует следующие критерии:

- тип реализации (селективный[3]);
- тип сопровождения (селективный);
- тип совместимости с операционными системами (селективный);
- тип управления (селективный);
- тип внутренней безопасности (селективный).

В плоскости специфических характеристик используют следующие критерии:

- тип архитектуры (селективный);
- возможность контроля времени работы (селективный);
- объект фильтрации (множественный[4]);
- способ фильтрации (множественный);
- возможность фильтрации шифрованных данных (селективный);
- тип реакции (способ работы) (множественный).

Плоскость базовых характеристик

По типу реализации:

1. Программные (S). Системы данного класса реализованы в виде программного продукта, который устанавливается либо непосредственно на устройство пользователя либо на специально выделенный сервер. Достоинством систем данного класса является их относительная простота установки, настройки и эксплуатации.
2. Аппаратные (H). Системы данного класса реализованы в виде аппаратного продукта (или программно-аппаратного решения), который устанавливается как отдельное сетевое устройство. Недостатком систем данного класса является высокая стоимость решения, трудоемкость и сложность настройки.

По совместимости с операционными системами:

1. Одноплатформенные (SP). Системы данного класса предназначены для работы с устройствами, которые находятся под управлением операционной системы (ОС) определенного типа, например, только Windows или только Unix;
2. Кроссплатформенные (CP). Системы данного класса поддерживают работу с несколькими ОС, например, система может работать на устройствах под управлением ОС Windows и на устройствах под управлением ОС Android.

[3] Критерии селективного характера предполагают использование лишь одного из классов на выбор

[4] Критерии множественного характера могут описывать систему одновременно несколькими классами

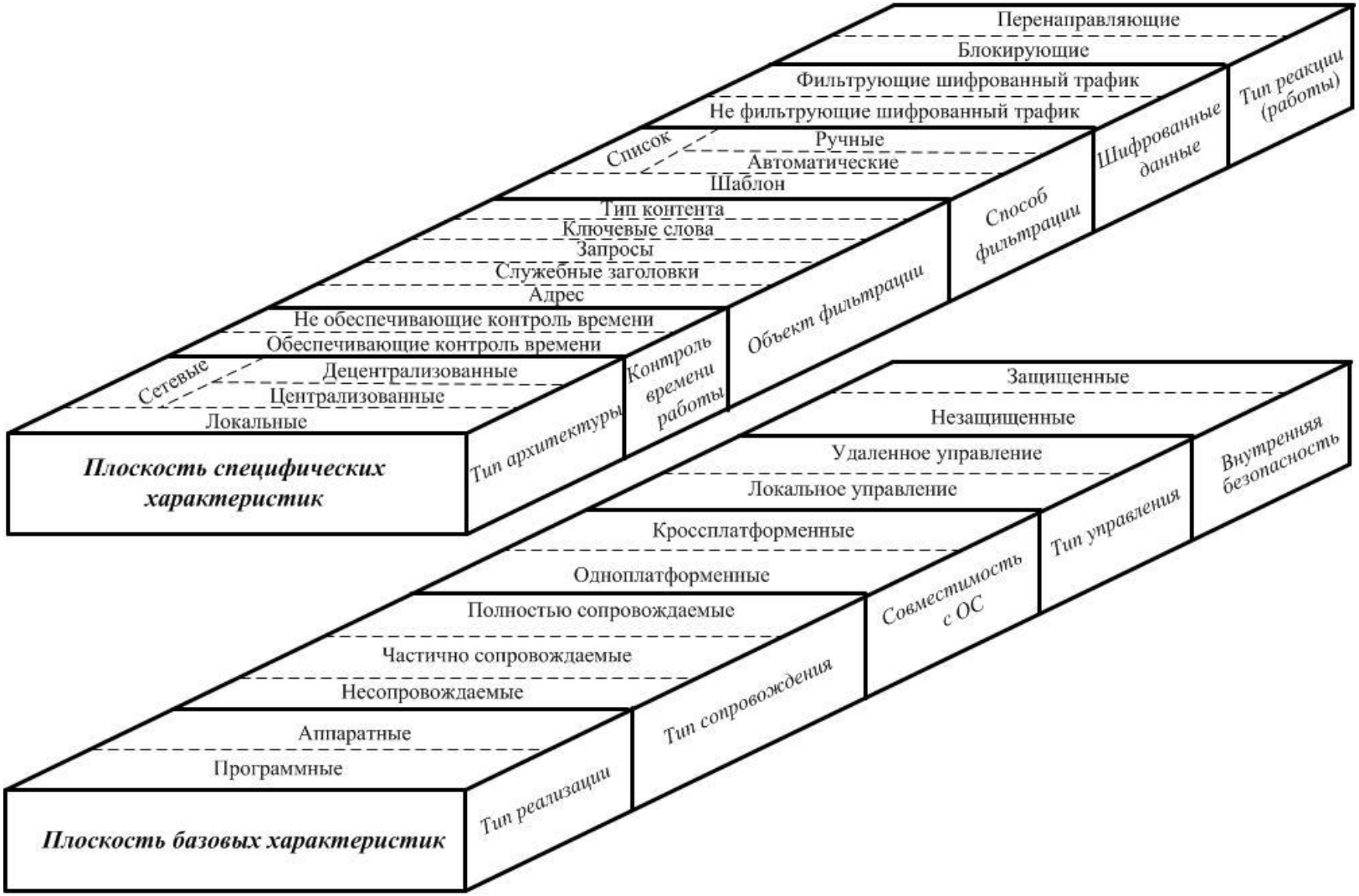

Рисунок 1 - Классификационная модель систем фильтрации контента

По типу сопровождению (поддержки):

1. Полностью сопровождаемые системы (FS) – системы данного класса централизовано и регулярно обновляются с целью улучшения эффективности их работы и удобства эксплуатации. Также для данных систем регулярно обновляются базы стоп-листов (черных/белых списков) ресурсов, вирусов.
2. Частично сопровождаемые системы (PS) – для систем данного класса централизовано и регулярно обновляются только базы стоп-листов (черных/белых списков) ресурсов, вирусов. Обновление функциональных возможностей происходит в случае выявления критических ошибок в работе системы.
3. Несопровождаемые системы (US) – централизованное обновление систем данного класса не проводится. Разработчик системы, как правило, не осуществляет обновлений и пользователь должен сам решать эти задачи.

По типу управления:

1. Системы локального управления (LM) – управление системами данного класса осуществляется «локально» изнутри защищаемого объекта.
2. Системы удаленного управления (RM) – управление системами данного класса возможно не только «локально» изнутри защищаемого объекта.

По типу внутренней безопасности:

1. Защищенные системы (SS) – у систем данного класса настройки системы (параметры фильтрации) защищены паролем, не каждый пользователь, который имеет доступ к системе, может изменять режим ее работы.
2. Незащищенные системы (NSS) – у системы данного класса настройки системы (параметры фильтрации) не защищены паролем, любой пользователь имеющий доступ к системе может изменять режим ее работы.

Плоскость специфических характеристик

По типу архитектуры:

1. Локальные (L) – предназначены для организации фильтрации контента только на одном устройстве (компьютер, смартфон, планшет).
2. Сетевые (N) – предназначены для организации фильтрации контента для устройств, объединенных в сеть:

- Централизованные (NC) – предполагает наличие единой, для всех устройств, политики фильтрации, которая осуществляется центральным элементом (устройством). Достоинством является простота организации и относительно низкая стоимость, недостаток – при выходе из строя центрального элемента система становится полностью не работоспособной.
- Децентрализованные (ND) – фильтрация осуществляется группой элементов (устройств) распределенных по сети, каждый из которых может реализовывать свою собственную политику фильтрации, центральный элемент осуществляет функцию согласования и координации работы остальных элементов. Достоинством является гибкость настройки (можно организовать уникальные политики фильтрации для отдельных пользователей, группы пользователей) и высокая надежность (отказ одного из элементов не приводит к выходу из строя всей системы). Недостатки – более высокая стоимость решения, требует больше трудозатрат на настройку и последующую эксплуатацию.

По возможности контроля времени работы:

1. Системы, обеспечивающие контроль времени работы в сети Интернет (TC) – позволяют контролировать время, проведенное в сети Интернет пользователями.
2. Системы, не обеспечивающие контроль времени работы в сети Интернет (TNC).

По объекту фильтрации:

1. Фильтрация по адресу (AIF) – системы данного класса позволяют осуществлять фильтрацию на базе адресной информации (URI, IP и т.д).
2. Фильтрация по служебным заголовкам (полям) (SHF) – системы данного класса позволяют осуществлять фильтрацию на базе таких служебных данных, как тип протокола, номер порта и т.д.
3. Фильтрация по запросам к поисковым системам (HRF) – анализируется содержимое запросов пользователей отправляемых к поисковым системам на соответствие заданным регулярным выражениям. Проверяется как запрос пользователя, так и ответ ресурса.
4. Фильтрация по ключевым словам (морфологический анализ) (KWF) – анализируется содержимое ресурса (сайта) на наличие определенных слов или словосочетаний. Если контент содержит указанные ключевые слова/словосочетания, то ресурс блокируется.
5. Фильтрация по типу контента (TCF) – блокирует доступ/загрузка контента заданного типа – видео контента, аудио контента, изображений, документов, архивов и исполняемых файлов и т.д.

По способу фильтрации:

1. Фильтрация по спискам (LF) – решение о доступе к ресурсу принимается на основе анализа черных (запрещенных)/белых (разрешенных) списков. В зависимости от способа формирования списков можно выделить два подкласса:
   - системы с ручным формированием списков (MLF);
   - системы с автоматическим формированием списков (ALF).
2. Фильтрация по шаблонам (FT) – решение о доступе к ресурсу принимается на основе анализа шаблона, если анализируемый ресурс совпадает с заданным шаблоном, то он блокируется/разрешается.

По возможности фильтрации шифрованных данных:

1. Системы позволяющие фильтровать шифрованные данные (HSS) – системы данного класса предоставляют возможность фильтровать данные, которые передаются по шифрованным каналам (протоколы HTTPS, SSH).
2. Системы, не позволяющие фильтровать шифрованные данные (NHS).

По типу реакции (способу работы):

1. Блокирующие (BS) – системы данного класса при обнаружении попытки доступа к запрещенному контенту/ресурсу блокируют доступ к этому контенту/ресурсу.
2. Перенаправляющие (RS) – системы данного класса при обнаружении попытки доступа к запрещенному контенту/ресурсу переадресовывает пользователя на специальную страницу, где поясняется, почему не может быть предоставлен доступ к запрошенному контенту/ресурсу или где может быть размещена любая другая информация заданная администратором системы.

В Приложении А приведены характеристики систем фильтрации контента сгруппированные по категориям, в соответствии с тем как они позиционируются на рынке программного обеспечения

фильтрации контента, описание их характеристик и принадлежности к определенным классам в соответствии с предложенной классификационной моделью.

3. Алгоритмы выбора системы фильтрации контента

Для выбора оптимальной системы фильтрации контента необходимо определить требования пользователя к системе и сопоставить их с функциональными возможностями доступных для выбора систем. Общий алгоритм выбора системы показан на рисунке 2.

Рисунок 2 – Алгоритм выбора системы фильтрации контента

Для выбора оптимальной системы фильтрации контента необходимо решить следующие задачи:

- определить уровень пользователя;
- получить от пользователя список требований к системе (в зависимости от уровня пользователя применяются разные алгоритмы);

– выбрать систему/системы, которая/которые соответствуют требованиям пользователя;
– определить экономические показатели - стоимость внедрения выбранной системы.

3.1 Определение уровня компетенции пользователя

В соответствии с пунктом 2 алгоритма (рис. 2) выделяется 5 классов пользователей. Для определения класса пользователя применяется следующий алгоритм:

1. Для каждого класса пользователей формируется набор вопросов, позволяющих оценить степень освоения пользователем возможностей предоставляемых сетью Интернет.
2. Начиная с низшего класса (новичок) пользователю задают набор соответствующих вопросов.
3. Если пользователь отвечает правильно на три вопроса ($СЧ_{пр}=3$), то ему предлагается ответить на вопросы соответствующие вышестоящему классу.
4. Если пользователь отвечает неправильно на три вопроса ($СЧ_{непр}=3$), то его уровень соответствует классу задаваемых вопросов.

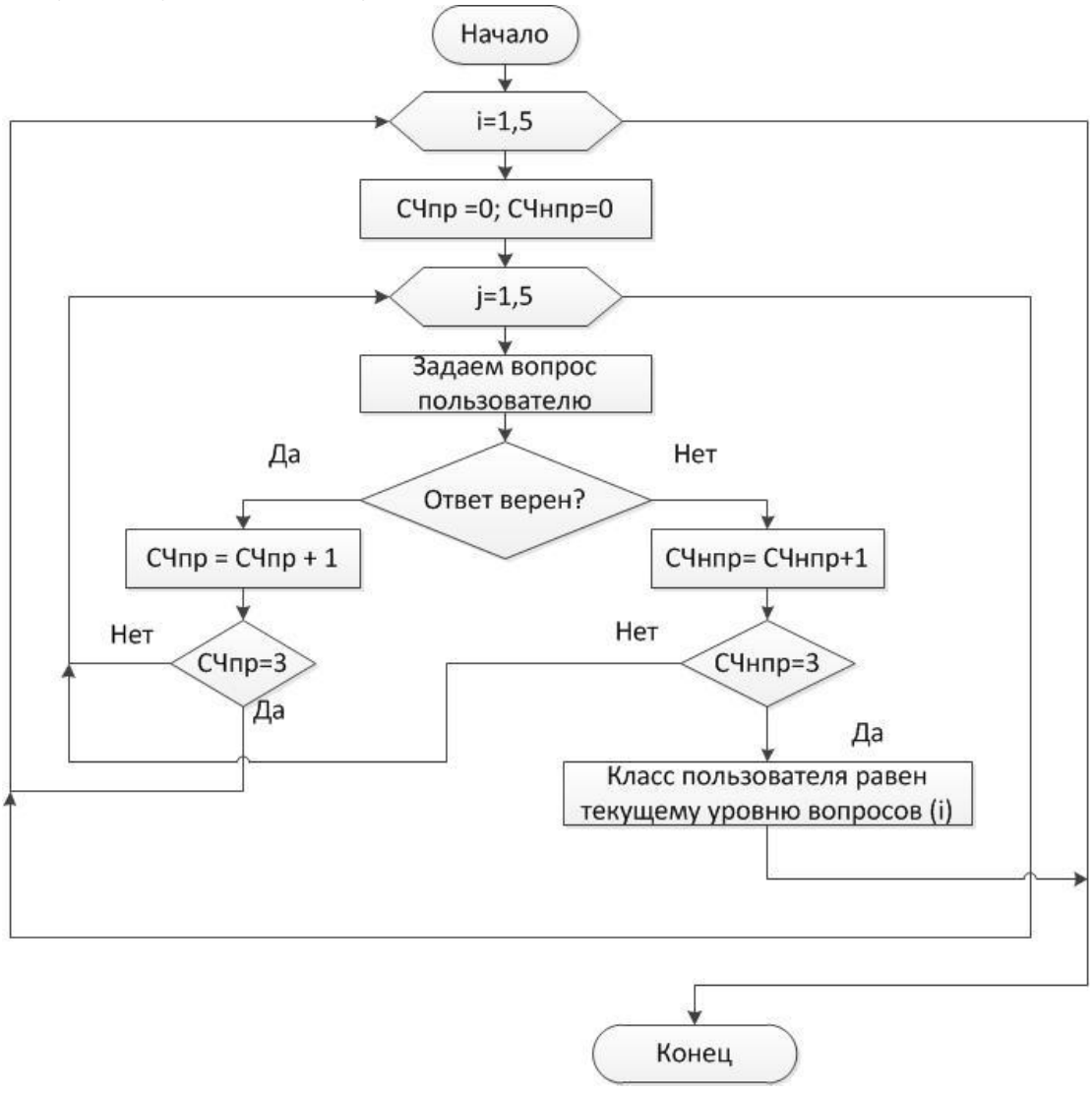

Рисунок 3 – Алгоритм определения класса пользователя

Алгоритм определения класса пользователя приведен на рис. 3. Для определения класса пользователя предлагаются могут быть использованы вопросы приведённые в Приложении Б.

3.2 Определение требований пользователя

В общем случае, для определения требуемых характеристик системы и последующего её выбора, от пользователя необходимо получить ответы на ряд базовых вопросов. Формат вопросов определяется уровнем пользователя:

3.2.1 Новичок

№ п/п	Вопрос	Пояснение
1	Вы будете защищать одно или несколько «независимых» устройств, не объединенных в сеть?	Ответьте «Да» если у Вас дома (на работе/в школе) используется только одно/несколько устройств (компьютер/ноутбук/планшет/смартфон) которое Вы хотите защитить, и которые не объединены в домашнюю/локальную/корпоративную сеть. Ответьте «Нет» если Вас есть несколько устройства объединенных в сеть, и Вы хотите обеспечить защиту всех устройств.
2	Должна ли система работать всегда, при любых условиях?	Вопрос задается, если был дан ответ «Нет» на предыдущий вопрос. Ответьте «Да» если Вы хотите, чтобы система защиты сохраняла свою работоспособность при перебоях в работе сети, потери соединения с сервером. Ответьте «Нет» если Вам не требуется постоянная работоспособность системы
3	Вы можете указать, какая операционная система (ОС) используете на Вашем устройстве/устройствах?	Если Вы укажите тип ОС - это позволит выбрать систему защиты, предназначенную для работы с Вашей ОС. Совместимость с ОС повышает вероятность того, что система защиты будет работать без конфликтов и ошибок. Невозможно гарантировать, что система не совместимая с ОС будет корректно работать и сможет удовлетворить Ваши требования. Пользователю предлагается выбрать ОС из следующего списка: 1.ОС семейства Windows 2.Linux 3.Unix 4.Android 5.Free BSD 6.Mac OS 7.iOS

4	Система должна быть реализована в виде программного обеспечения?	Ответьте «Да» если Вы хотите чтобы система защиты устанавливалась на защищаемые устройства в виде отдельного программного продукта или модуля на существующее устройство (смартфон, планшет, персональный компьютер). Ответьте «Нет», если Вы хотите, чтобы система была реализована в виде отдельного устройства подключаемого к сети (сервер, маршрутизатор и т.д.).
5	Вы хотели бы контролировать время, проведённое в Сети?	Ответьте «Да» если Вы хотите контролировать и ограничивать время, проведенное в Интернете Вашим ребенком/сотрудником/учеником школы/студентом ВУЗа. Ответьте «Нет» если Вы не планируете контролировать время проведенное в сети.
6	Настраивать систему будет один человек?	Ответьте «Да» если Вы хотите, чтобы настраивал, управлял и обслуживал систему один человек. Доступ к функциям управления системой будет ограничен, осуществлять управление и настройку сможет осуществлять человек (или несколько человек), обладающий советующими для этого правами (разрешениями). Ответьте «Нет», если Вы не хотите ограничивать доступ к функциям управления системой. Имейте в виду, что в этом случае, изменять настройки системы может любой пользователь. Это может привести к тому, что система будет неправильно работать или вообще может выйти из строя.
7	Хотите ли Вы управлять системой постоянно?	Ответьте «Да» если Вам необходимо иметь возможность быстро и оперативно управлять системой, не зависимо от того, где вы находитесь. Ответьте «Нет» если у Вас нет необходимости постоянно иметь доступ к управлению системой.
8	Вы хотите иметь возможность проверять любые данные?	Данные в сети могут передаваться как в «открытом», так и в «закрытом» виде. Ответьте «Да» если Вы хотите, что бы система проверяла данные, которые передаются даже в «закрытом» виде. Ответьте «Нет» если Вам необходимо проверять данные, которые передаются только в «открытом» виде. Имейте в виду, что данные, которые передаются в «закрытом» виде системой проверятся не будут, и в этом случае пользователи могут получать доступ к запрещенным ресурсам, которые передают данные в «закрытом» формате.
9	Вы будете сами принимать решение о закрытии/открытии доступа к ресурсу?	Ответьте «Да» если Вы хотите сами формировать правила (шаблон) для принятия решения о закрытии/открытии доступа к ресурсам. Имейте в виду, что правила необходимо будет регулярно обновлять и добавлять новые. Ответьте «Нет» если Вы не хотите / не умеете сами формировать правила для принятия решения о закрытии/открытии доступа к ресурсам.

10	Вы хотите иметь возможность блокировать страницы по их именам (адресам)?	Ответьте «Да» если Вы хотите блокировать доступ к странице используя её имя (адрес), например fishki.net или eva.ru. Ответьте «Нет» если у Вас нет необходимости блокировать ресурсы по их именам.
11	Вы хотите иметь возможность блокировать доступ к порнографическим материалам?	Ответьте «Да» если Вы хотите заблокировать доступ к ресурсам, содержащим порнографические материалы. Имейте ввиду, также можно блокировать доступ к игровым ресурсам (on-line игры и казино), ресурсам содержащим экстремистские материалы и т.п.
12	Вы хотели бы иметь возможность блокировать результаты поиска?	Ответьте «Да» если Вы хотите блокировать результаты работы поисковых систем по определённым запросам пользователя. Например, блокировать (не отображать) результаты поиска на запрос пользователя «Как сделать бомбу?» или «Как варить маковую соломку?» и т.п. Ответьте «Нет» если Вы не хотите блокировать результаты работы поисковых систем по определённым запросам пользователя.
13	Вы хотите иметь возможность блокировать доступ к ресурсам, содержащим определённые слова или фразы?	Ответьте «Да» если Вы хотите блокировать весь ресурс (или его часть), который содержит заданное слово/фразу. Например, блокировать ресурсы, которые содержат слова «секс», «порно» и т.д. Ответьте «Нет» если у Вас нет необходимости блокировать ресурс (или его часть) по наличию ключевых слов/фраз.
14	Вы хотели бы иметь возможность при необходимости блокировать загрузку/просмотр видео, музыки?	Ответьте «Да» если Вы хотите запретить возможность загружать/просматривать из сети фильмы, музыку, архивы, картинки. Ответьте «Нет» если Вы не хотите блокировать возможность загружать/просматривать из сети фильмы, музыку, архивы, картинки.
15	Система должна постоянно обновляться?	Ответьте «Да» если Вы хотите чтобы функциональные возможности системы, базы стоп-листов (чёрных / белых списков) ресурсов, вирусов и т.д. обновлялись постоянно. Ответьте «Нет» если функция обновления системы для Вас не важна.

3.2.2 Пользователь

№ п/п	Вопрос	Пояснение
1	Вы будете защищать одно или несколько «независимых» устройств, не объединенных в сеть?	Ответьте «Да» если у Вас дома (на работе/в школе) используется только одно/несколько устройств (компьютер/ноутбук/планшет/смартфон) которое Вы хотите защитить, и которые не объединены в домашнюю/локальную/корпоративную сеть. Ответьте «Нет» если Вас есть несколько устройства объединенных в сеть, и Вы хотите обеспечить защиту всех устройств.

2	Должна ли система выполнять свои функции при возникновении проблем в её работе?	Вопрос задается, если был дан ответ «Нет» на предыдущий вопрос. Ответьте «Да» если Вы хотите, что бы система защиты сохраняла свою работоспособность при перебоях в работе сети, потери соединения с сервером.
3	Вы можете указать, какую операционную систему Вы используете на Вашем устройстве/устройствах?	Если Вы укажите тип ОС – это позволит выбрать систему защиты, предназначенную для работы с Вашей ОС. Совместимость с ОС повышает вероятность того, что система защиты будет работать без конфликтов и ошибок. Невозможно гарантировать, что система не совместимая с ОС будет корректно работать и сможет удовлетворить Ваши требования. Пользователю предлагается выбрать ОС из следующего списка: 1.ОС семейства Windows 2.Linux 3.Unix 4.Android 5.Free BSD 6.Mac OS 7.iOS
4	Система должна быть реализована в виде программного обеспечения?	Ответьте «Да» если Вы хотите что бы система защиты устанавливалась на защищаемые устройства в виде отдельного программного продукта или модуля.
5	Вы хотели бы контролировать время, проведённое в Сети?	Ответьте «Да» если Вы хотите контролировать и ограничивать время, проведённое в Интернете Вашим ребенком/сотрудником/учеником школы / студентов ВУЗа.
6	Настраивать систему будет один человек?	Ответьте «Да» если Вы хотите ограничить доступ к функциям управление и настройки системы. Имейте в виду, что ограничение доступа к настройкам системы повышает общий уровень безопасности.
7	Хотите ли Вы управлять системой постоянно?	Ответьте «Да» если Вам необходимо иметь возможность быстро и оперативно управлять системой, независимо от того, где вы находитесь.
8	Вы хотите иметь возможность фильтровать любые данные?	Данные в сети могут передаваться как в «открытом», так и в «шифрованном» виде. Ответьте «Да» если Вы хотите, что бы система проверяла не только «открытые» данные, но и данные которые передаются в «шифрованном» виде. Возможность фильтровать «шифрованные» данные значительно повышает эффективность использования системы защиты.
9	Вы будете сами определять правила фильтрации?	Ответьте «Да» если Вы хотите сами формировать правила (шаблоны) для принятия решения о закрытии/открытии доступа к ресурсам. Имейте в виду, что правила необходимо будет периодически обновлять и добавлять новые.
10	Вы хотите иметь возможность блокировать ресурсы по их именам, адресам?	Ответьте «Да» если Вы хотите блокировать доступ к странице используя ее имя (fishki.net или eva.ru) или адрес (195.5.25.120)

11	Вы хотели бы иметь возможность блокировать работу социальных сетей, Skype?	Ответьте «Да» если Вы хотите ограничить или блокировать доступ ребенку/сотруднику/ученику/студенту к определенному сетевому сервису/сервисам.
12	Вы хотели бы иметь возможность блокировать результаты поиска?	Ответьте «Да» если Вы хотите блокировать результаты работы поисковых систем по определённым запросам пользователя. Например, блокировать (не отображать) результаты поиска на запрос пользователя «Как сделать бомбу?» или «Как варить маковую соломку?» и т.п.
13	Вы хотите иметь возможность блокировать доступ к ресурсам, содержащим определённые слова или фразы?	Ответьте «Да» если Вы хотите блокировать весь ресурс (или его часть), который содержит заданное слово/фразу. Например, блокировать ресурсы, которые содержат слова «секс», «порно» и т.д.
14	Вы хотели бы иметь возможность блокировать загрузку/просмотр видео, музыки, архивов?	Ответьте «Да» если Вы хотите запретить возможность загружать/просматривать из сети фильмы, музыку, архивы, картинки.
15	Система должна постоянно обновляться?	Ответьте «Да» если Вы хотите чтобы функциональные возможности системы, базы стоп-листов (черных/белых списков) ресурсов, вирусов обновлялись постоянно.

3.2.3 Опытный пользователь

№ п/п	Вопрос	Пояснение
1	Вы будете защищать одно или несколько «независимых» устройств, не объединенных в сеть?	Ответьте «Да» если у Вас дома (на работе/в школе) используется только одно/несколько устройств (компьютер/ноутбук/планшет/смартфон) которое Вы хотите защитить, и которые не объединены в домашнюю/локальную/корпоративную сеть. Ответьте «Нет» если Вас есть несколько устройства объединенных в сеть, и Вы хотите обеспечить защиту всех устройств.
2	Должна ли система выполнять свои функции при возникновении проблем в ее работе?	Вопрос задается, если был дан ответ «Нет» на предыдущий вопрос. Ответьте «Да» если Вы хотите, что бы система защиты сохраняла свою работоспособность при перебоях в работе сети, потери соединения с сервером.

3	Система будет защищать устройства, работающие под управлением одной ОС?	Укажите ОС – это позволит выбрать систему, предназначенную для работы с Вашей ОС. Совместимость с ОС повышает вероятность того, что система защиты будет работать без конфликтов с системными процессами ОС. Имейте в виду, что невозможно гарантировать, что система сможет удовлетворить Ваши требования, если она не совместима Вашей ОС. Пользователю предлагается выбрать ОС из следующего списка: 1.ОС семейства Windows 2.ОС семейства Linux 3.ОС семейства Unix 4.Android 5.Free BSD 6.Mac OS 7.iOS Ответьте «Нет», если у вас используется несколько разных ОС. Пользователь может указать несколько ОС из предлагаемого выше списка
4	Система должна быть реализована в виде программного обеспечения?	Ответьте «Да» если Вы хотите что бы система защиты устанавливалась на защищаемые устройства в виде отдельного программного продукта или модуля.
5	Вы хотели бы контролировать время, проведённое в Сети?	Ответьте «Да» если Вы хотите контролировать и ограничивать время, проведенное в Интернете Вашим ребенком/сотрудником/учеником школы/студентом ВУЗа.
6	Доступ к настройкам системы должен быть ограничен?	Ответьте «Да» если Вы хотите ограничить доступ к функциям управление и настройки системы. Имейте в виду, что ограничение доступа к настройкам системы повышает общий уровень безопасности.
7	Нужна ли функция удаленного управления?	Ответьте «Да» если Вам необходимо иметь возможность удаленного управления системой. Имейте в виду, что возможность удаленного управление системой повышает вероятность выхода из строя системы в случае атаки злоумышленником.
8	Необходимо ли фильтровать шифрованные данные?	Ответьте «Да» если Вы хотите, что бы система проверяла не только «открытые» данные, но и данные которые передаются в «шифрованном» виде. Возможность фильтровать «шифрованные» данные значительно повышает эффективность использования системы защиты.
9	Вы будете сами определять правила фильтрации?	Ответьте «Да» если Вы хотите сами формировать правила (шаблоны) для принятия решения о закрытии/открытии доступа к ресурсам. Имейте в виду, что правила необходимо будет периодически обновлять и добавлять новые.
10	Вы хотите иметь возможность блокировать ресурсы по их именам, адресам?	Ответьте «Да» если Вы хотите блокировать доступ к странице используя ее имя (fishki.net или eva.ru) или адрес (195.5.25.120)

11	Вы хотите иметь возможность блокировать ресурсы по используемым портам, протоколам?	Ответьте «Да» если, например, Вы хотите блокировать работу сервиса FTP который использует 20 и 21 порты.
12	Вы хотели бы иметь возможность осуществлять фильтрацию поисковых запросов?	Ответьте «Да» если Вы хотите блокировать результаты работы поисковых систем по определённым запросам пользователя. Например, блокировать (не отображать) результаты поиска на запрос пользователя «Как сделать бомбу?» или «Как варить маковую соломку?» и т.п.
13	Вы хотите иметь возможность блокировать доступ к ресурсам, содержащим определённые слова или фразы?	Ответьте «Да» если Вы хотите блокировать весь ресурс или его часть, который содержит заданное слово/фразу. Например, блокировать ресурсы, которые содержат слова «секс», «порно» и т.д.
14	Вы хотели бы иметь возможность блокировать загрузку данных определенного типа?	Ответьте «Да» если Вы хотите запретить возможность загружать/просматривать из сети контент определенного типа - фильмы, музыку, архивы, картинки.
15	Система должна блокировать запрещенные ресурсы?	Ответьте «Да» если Вы хотите что бы система при выявлении обращения к запрещенному ресурсу блокировала к нему доступ – выводила страницу с ошибкой, например 404.
16	Система должна обновлять функционал?	Ответьте «Да» если Вы хотите чтобы функциональные возможности системы, базы стоп-листов (черных/белых списков) ресурсов, вирусов обновлялись постоянно.
17	Система должна постоянно обновлять свои базы?	Ответьте «Да» если Вы хотите чтобы обновлялись только базы стоп-листов (черных/белых списков) ресурсов, вирусов.

3.2.4 Технический специалист/Эксперт

№ п/п	Вопрос	Пояснение
1	Система нужна для защиты одного или нескольких «независимых» устройств, не объединенных в сеть?	Ответьте «Да» если у Вас дома (на работе/в школе) используется только одно/несколько устройств (компьютер/ноутбук/планшет/смартфон) которое Вы хотите защитить, и которые не объединены в домашнюю/локальную/корпоративную сеть. Ответьте «Нет» если Вас есть несколько устройства объединенных в сеть, и Вы хотите обеспечить защиту всех устройств.
2	Система должна сохранять работоспособность при выходе из строя центрального элемента?	Вопрос задается, если был дан ответ «Нет» на предыдущий вопрос. Ответьте «Да» если Вам необходимо сохранить работоспособность системы даже при перебоях в работе сети, потери соединения с сервером.

3	Система будет использоваться для защиты устройств под управление одной ОС?	Ответьте «Да» если у Вас используется ОС одного типа на всех устройствах. Пользователю предлагается выбрать ОС из следующего списка: 1.ОС семейства Windows 2.ОС семейства Linux 3.ОС семейства Unix 4.Android 5.Free BSD 6.Mac OS 7.iOS Ответьте «Нет», если у вас используется несколько разных ОС. Пользователь может указать несколько ОС из предлагаемого выше списка
4	Система должна быть реализована в виде отдельного устройства?	Ответьте «Да» если Вы хотите использовать систему реализованную в виде отдельного аппаратного устройства.
5	Нужна ли возможность удаленного управления системой?	Ответьте «Да» если Вам необходимо иметь возможность удаленного управления системой.
6	Доступ к настройкам системы должен быть доступен только авторизированным пользователям?	Ответьте «Да» если Вы хотите ограничить доступ к функциям управления и настройки системы.
7	Нужна ли возможность фильтровать шифрованные данные?	Ответьте «Да» если Вы хотите фильтровать «шифрованный» (HTTPS) трафик. Наличие данной функции значительно повышает эффективность системы защиты.
8	Система должна иметь возможность контролировать время, проведённое в Сети?	Ответьте «Да» если Вы хотите устанавливать лимит на время, проведённое пользователем в Интернете.
9	Решение о фильтрации данных будет осуществляться в соответствии с шаблоном?	Ответьте «Да» если Вы сами будете формировать шаблон для определения правил фильтрации трафика.
10	Списки блокировки должны формироваться автоматически?	Ответьте «Да» если Вы не планируете самостоятельно формировать черные/белые списки запрещенных/разрешенных ресурсов.
11	Система должна фильтровать данные, используя адресную информацию?	Ответьте «Да» если Вам необходимо иметь возможность фильтровать контент по адресу ресурса, его доменному имени.
12	Система должна фильтровать данные, используя служебные заголовки?	Ответьте «Да» если Вам необходимо иметь возможность фильтровать контент по номеру порта, типу протокола и т.д.
13	Система должна фильтровать запросы к поисковым системам?	Ответьте «Да» если Вы хотите блокировать результаты работы поисковых систем по определённым запросам пользователя.
14	Необходима ли фильтрация по ключевым словам?	Ответьте «Да» если Вы хотите блокировать весь ресурс или его часть, если он содержит заданное ключевое слово/фразу.

15	Планируете ли Вы фильтровать отдельные типы контента?	Ответьте «Да» если Вы планируете блокировать загрузку/просмотр контент определенного типа – видео контент, аудио контент и т.п.
16	При обращении к запрещенному ресурсу система должна перенаправлять на безопасную страницу?	Ответьте «Да», если Вы хотите, что бы система, при обнаружении попытки доступа к запрещенному ресурсу, загружала страницу содержащую специальный контент – например пояснения почему доступ заблокирован.
17	Система должна иметь сопровождение?	Ответьте «Да» если Вы хотите использовать систему, разработчики которой обеспечивают стабильное и постоянное сопровождение системы.
18	Обновления системы должны включать обновление функциональных возможностей и обновление баз стоп-листов (черных/белых списков) ресурсов, вирусов?	Ответьте «Да» если Вы хотите чтобы функциональные возможности системы, базы стоп-листов (черных/белых списков) ресурсов, вирусов обновлялись постоянно.

Получив ответ на вопросы можно определить требования пользователя к системе фильтрации контента. Соответствие требований пользователя классу системы представлено в таблице.

№ пп.	Вопрос	Ответ	Класс (признак) системы
	Новичок		
1	Вы будете защищать одно или несколько «независимых» устройств, не объединенных в сеть?	I_ANS_DEV_ONE	L
		I_ANS_DEV_NET	N
		I_ANS_DEV_IDN	N
2	Должна ли система работать всегда, при любых условиях?	I_ANS_MW_YES	ND
		I_ANS_MW_NO	NC
		I_ANS_MW_IDN	ND
3	Вы можете указать, какая операционная система используется на Вашем устройстве/устройствах?	I_ANS_OS_YES	SP
		I_ANS_OS_NO	CP
		I_ANS_OS_IDN	CP
4	Система должна быть реализована в виде программного обеспечения?	I_ANS_ARC_YES	S
		I_ANS_ARC_NO	H
		I_ANS_ARC_IDN	S
5	Введите тип ОС	ANS_TP_OS	TP_OS
6	Вы хотели бы контролировать время, проведённое в Сети?	I_ANS_TC_YES	TC
		I_ANS_TC_NO	NTC
		I_ANS_TC_IDN	TC
7	Настраивать систему будет один человек?	I_ANS_SS_YES	SS
		I_ANS_SS_NO	NSS
		I_ANS_SS_IDN	SS
8	Хотите ли Вы управлять системой постоянно?	I_ANS_SM_YES	RM
		I_ANS_SM_NO	LM
		I_ANS_SM_IDN	LM
9	Вы хотите иметь возможность проверять любые данные?	I_ANS_CD_YES	HSS
		I_ANS_CD_NO	NHS
		I_ANS_CD_IDN	HSS
10	Вы будете сами принимать решение о закрытии/открытии доступа к ресурсу?	I_ANS_AS_YES	FT
		I_ANS_AS_NO	LF
		I_ANS_AS_IDN	LF

11	Система сама должна формировать списки запрещенных ресурсов?	I_ANS_LF_YES	ALF
		I_ANS_LF_NO	MLF
		I_ANS_LF_IDN	ALF
12	Вы хотите иметь возможность блокировать страницы по их именам?	I_ANS_SN_YES	AIF
		I_ANS_SN_NO	-[5]
		I_ANS_SN_IDN	AIF
13	Вы хотите иметь возможность блокировать доступ к порнографическим материалам?	I_ANS_PORN_YES	TCF
		I_ANS_PORN_NO	-
14	Вы хотели бы иметь возможность блокировать результаты поиска?	I_ANS_SE_YES	HRF
		I_ANS_SE_NO	-
		I_ANS_SE_IDN	HRF
15	Вы хотите иметь возможность блокировать доступ к ресурсам, содержащим определённые слов или фразы?	I_ANS_KW_YES	KWF
		I_ANS_KW_NO	-
		I_ANS_KW_IDN	KWF
16	Вы хотели бы иметь возможность при необходимости блокировать загрузку/просмотр видео, музыки?	I_ANS_CB_YES	TCF
		I_ANS_CB_NO	-
		I_ANS_CB_IDN	TCF
17	Система должна постоянно обновляться?	I_ANS_UD_YES	FS
		I_ANS_UD_NO	US
		I_ANS_UD_IDN	PS
Пользователь			
1	Вы будете защищать одно или несколько «независимых» устройств, не объединенных в сеть?	I_ANS_DEV_ONE	L
		I_ANS_DEV_NET	N
		I_ANS_DEV_IDN	N
2	Должна ли система выполнять свои функции при возникновении проблем в ее работе?	I_ANS_MW_YES	ND
		I_ANS_MW_NO	NC

[5] ***Примечание***: «-» означает, что данная характеристика (свойство) системы не нужна пользователю. Например, если на вопрос «Необходима ли фильтрация по ключевым словам?» дан ответ «Нет» (I_ANS_KW_NO) и в графе «Класс системы» стоит «-» - это означает, что пользователю не нужна возможности фильтрации контента по ключевым словам, и следовательно нужно выбирать систему, которая не имеет возможности фильтрации контента по ключевым словам.

		I_ANS_MW_IDN	ND
3	Вы можете указать, какая операционная система используется на Вашем устройстве/устройствах?	I_ANS_OS_YES	SP
		I_ANS_OS_NO	CP
		I_ANS_OS_IDN	CP
4	Введите тип ОС	ANS_TP_OS	TP_OS
5	Система должна быть реализована в виде программного обеспечения?	I_ANS_ARC_YES	S
		I_ANS_ARC_NO	H
		I_ANS_ARC_IDN	S
6	Вы хотели бы контролировать время, проведённое в Сети?	I_ANS_TC_YES	TC
		I_ANS_TC_NO	NTC
7	Настраивать систему будет один человек?	I_ANS_SS_YES	SS
		I_ANS_SS_NO	NSS
8	Хотите ли Вы управлять системой постоянно?	I_ANS_SM_YES	RM
		I_ANS_SM_NO	LM
		I_ANS_SM_IDN	LM
9	Вы хотите иметь возможность фильтровать любые данные?	I_ANS_FD_YES	HSS
		I_ANS_FD_NO	NHS
		I_ANS_FD_IDN	HSS
10	Вы будете сами определять правила фильтрации?	I_ANS_AS_YES	FT
		I_ANS_AS_NO	LF
11	Вы будите формировать списки сами?	I_ANS_LF_YES	MLF
		I_ANS_LF_NO	ALF
		I_ANS_LF_IDN	ALF
12	Вы хотите иметь возможность блокировать ресурсы по их именам, адресам?	I_ANS_SNA_YES	AIF
		I_ANS_SNA_NO	-
		I_ANS_SNA_IDN	AIF
13	Вы хотели бы иметь возможность блокировать работу социальных сетей, Skype?	I_ANS_SB_YES	SHF
		I_ANS_SB_NO	-
		I_ANS_SB_ IDN	SHF
14	Вы хотели бы иметь возможность блокировать результаты поиска?	I_ANS_SE_YES	HRF
		I_ANS_SE_NO	-

15	Вы хотите иметь возможность блокировать доступ к ресурсам, содержащим определённые слов или фразы?	I_ANS_KW_YES	KWF
		I_ANS_KW_NO	-
		I_ANS_KW_IDN	KWF
16	Вы хотели бы иметь возможность блокировать загрузку/просмотр видео, музыки, архивов?	I_ANS_CB_YES	TCF
		I_ANS_CB_NO	-
17	Система должна постоянно обновляться?	I_ANS_UD_YES	FS
		I_ANS_UD_NO	US
		I_ANS_UD_IDN	PS
Опытный пользователь			
1	Вы будете защищать одно или несколько «независимых» устройств, не объединенных в сеть?	I_ANS_DEV_ONE	L
		I_ANS_DEV_NET	N
2	Должна ли система выполнять свои функции при возникновении проблем в ее работе?	I_ANS_MW_YES	ND
		I_ANS_MW_NO	NC
3	Система будет защищать устройства, работающие под управлением одной ОС?	I_ANS_OS_YES	SP
		I_ANS_OS_NO	CP
4	Введите тип ОС	ANS_TP_OS	TP_OS
5	Система должна быть реализована в виде программного обеспечения?	I_ANS_ARC_YES	S
		I_ANS_ARC_NO	H
6	Вы хотели бы контролировать время, проведённое в Сети?	I_ANS_TC_YES	TC
		I_ANS_TC_NO	NTC
7	Доступ к настройкам системы должен быть ограничен?	I_ANS_SS_YES	SS
		I_ANS_SS_NO	NSS
8	Нужна ли функция удаленного управления?	I_ANS_RM_YES	RM
		I_ANS_RM_NO	LM
9	Необходимо ли фильтровать шифрованные данные?	I_ANS_SFD_YES	HSS
		I_ANS_SFD_NO	NHS
		I_ANS_FD_IDN	HSS
10	Вы будете сами определять правила фильтрации?	I_ANS_AS_YES	FT
		I_ANS_AS_NO	LF

11	Вы будите формировать списки сами?	I_ANS_LF_YES	MLF
		I_ANS_LF_NO	ALF
		I_ANS_LF_IDN	ALF
12	Вы хотите иметь возможность блокировать ресурсы по их именам, адресам?	I_ANS_ADR_YES	AIF
		I_ANS_ADR_NO	-
13	Вы хотите иметь возможность блокировать ресурсы по используемым портам, протоколам?	I_ANS_SNAP_YES	SHF
		I_ANS_SNAP_NO	-
14	Вы хотели бы иметь возможность осуществлять фильтрацию поисковых запросов?	I_ANS_SQF_YES	TCF
		I_ANS_SQF_NO	-
15	Вы хотите иметь возможность блокировать доступ к ресурсам, содержащим определённые слов или фразы?	I_ANS_KW_YES	HRF
		I_ANS_KW_NO	-
16	Вы хотели бы иметь возможность блокировать загрузку данных определенного типа?	I_ANS_DB_YES	KWF
		I_ANS_DB_NO	-
17	Система должна блокировать запрещенные ресурсы?	I_ANS_RB_YES	BS
		I_ANS_RB_NO	RS
18	Система должна обновлять функционал?	I_ANS_UF_YES	FS
		I_ANS_UF_NO	US
19	Система должна постоянно обновлять свои базы?	I_ANS_DBU_YES	PS
		I_ANS_DBU_NO	US
Технический специалист/Эксперт			
1	Система нужна для защиты одного или нескольких «независимых» устройств, не объединенных в сеть?	I_ANS_DEV_ONE	L
		I_ANS_DEV_NET	N
2	Система должна сохранять работоспособность при выходе из строя центрального элемента?	I_ANS_MW_YES	ND
		I_ANS_MW_NO	NC
3	Система будет использоваться для защиты устройств под управление одной ОС?	I_ANS_OS_YES	SP
		I_ANS_OS_NO	CP
4	Введите тип ОС	ANS_TP_OS	TP_OS
5	Система должна быть реализована в виде отдельного устройства?	I_ANS_SD_YES	S
		I_ANS_SD_NO	H
6	Нужна ли возможность удаленного управления системой	I_ANS_RM_YES	RM
		I_ANS_RM_YES	LM

7	Доступ к настройкам системы должен быть доступен только авторизированным пользователям?	I_ANS_ASS_YES	SS
		I_ANS_ASS_NO	NSS
8	Необходимо ли фильтровать шифрованные данные?	I_ANS_SFD_YES	HSS
		I_ANS_SFD_NO	NHS
9	Система должна иметь возможность контролировать время, проведенное в Сети?	I_ANS_TC_YES	TC
		I_ANS_TC_NO	NTC
10	Решение о фильтрации данных будет осуществляться в соответствии с шаблоном?	I_ANS_DFT_YES	FT
		I_ANS_DFT_NO	-
11	Списки блокировки должны формироваться автоматически?	I_ANS_BLF_YES	ALF
		I_ANS_BLF_NO	MLF
12	Система должна фильтровать данные, используя адресную информацию?	I_ANS_ADR_YES	AIF
		I_ANS_ADR_NO	-
13	Система должна фильтровать данные, используя служебные заголовки?	I_ANS_SNAP_YES	SHF
		I_ANS_SNAP_NO	-
14	Система должна фильтровать запросы к поисковым системам?	I_ANS_SSF_YES	HRF
		I_ANS_SSF_NO	-
15	Необходима ли фильтрация по ключевым словам?	I_ANS_KW_YES	KWF
		I_ANS_KW_NO	-
16	Планируете ли Вы фильтровать контент, блокировать отдельные его типы?	I_ANS_CB_YES	TCF
		I_ANS_CB_NO	-
17	При обращении к запрещенному ресурсу система должна перенаправлять на безопасную страницу?	I_ANS_RB_YES	RS
		I_ANS_RB_NO	BS
18	Система должна иметь сопровождение?	I_ANS_HSS_YES	FS
		I_ANS_HSS_NO	US
19	Обновления системы должны включать обновление функциональных возможностей и обновление баз стоп-листов (черных/белых списков) ресурсов, вирусов?	I_ANS_UFDB_YES	FS
		I_ANS_UFDB_NO	PS

3.3 Формирование списка систем соответствующих требованиям пользователя

Формирование списка доступных для выбора (внедрения) систем фильтрации осуществляется в соответствии с требованиями выдвинутыми пользователем. Для предоставления пользователю возможности выбрать систему, отвечающую его требованиям в максимальной степени, формируется два списка систем:

– Список рекомендуемых системы – в данный список включаются системы характеристики, которых полностью соответствуют или превосходят требования заявленные пользователем;

– Список возможных системы – в данный список включаются системы, которые не удовлетворяют не более чем одному из заявленных пользователем требований.

Алгоритм формирования списков доступных для выбора систем фильтрации приведен на рисунке 4.

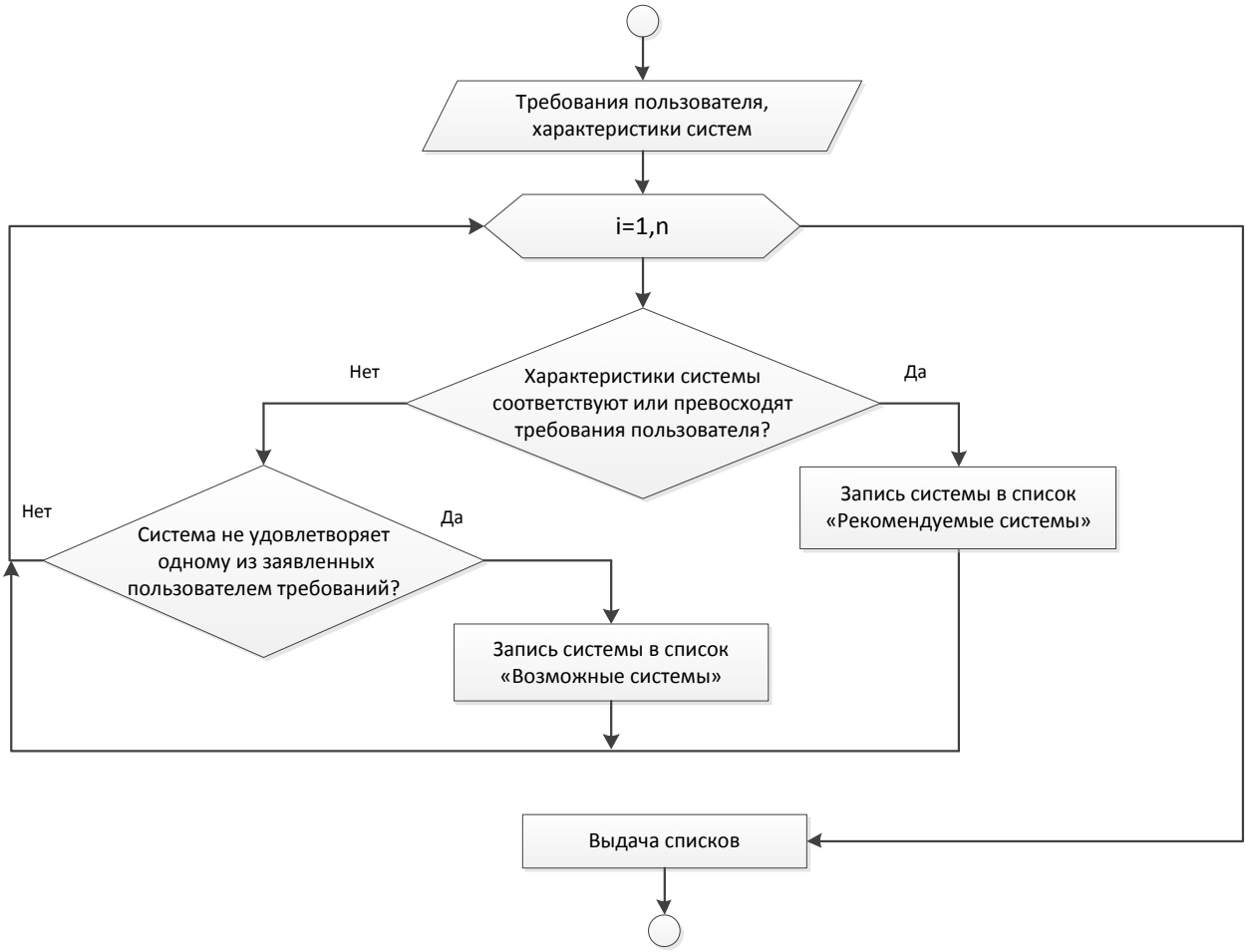

Рисунок 4 - Алгоритм формирования списков доступных для выбора систем фильтрации контента

3.4 Определение стоимости системы

Для каждой системы фильтрации рассчитываются следующие параметры:

1. Стоимость внедрения необходимой для работы системы фильтрации контента инфраструктуры:

$$C_{инфр} = N_{серв} \cdot C_{серв},$$

где $N_{серв}$ – количество устанавливаемых серверов; $C_{серв}$ – стоимость одного сервера, ден.ед.;

В случае построения либо модернизации сети:
– для проводной сети

$$C_{инфр} = N_{серв} \cdot C_{серв} + \sum_i N_{акт.i} \cdot C_{акт.i} + C_{СКС} \ ,$$

– для беспроводной сети

$$C_{инфр} = N_{серв} \cdot C_{серв} + C_{WIFI} \ ,$$

где $N_{акт.i}$ – количество единиц активного сетевого оборудования *i*-того типа; $C_{акт.i}$ – стоимость единицы активного сетевого оборудования, ден.ед.; $C_{СКС}$ – общая стоимость материалов и монтажа проводной ЛВС, ден.ед. (см. Приложение В.1); C_{WIFI} – общая стоимость материалов и монтажа беспроводной ЛВС, ден.ед. (см. Приложение В.2);

Количество устанавливаемых серверов $N_{серв}$ рассчитывается по формуле:

$$N_{серв} \geq \frac{K_{wp}}{N_{макс.серв}},$$

где K_{wp} – количество рабочих мест; $N_{макс.серв}$ – максимальное количество клиентов, которое может обслужить один сервер системы фильтрации контента.

Если система относится к классу локальных систем, то:

$$C_{инфр} = 0$$

2. Стоимость внедрения системы фильтрации $C_{внедр}$, которая рассчитывается по следующей формуле:

$$C_{внедр} = C_{лиц} + C_{час} \cdot \sum_i N_i \cdot T_{настр} + C_{ком}$$

где $C_{лиц}$ – общая стоимость лицензии, ден.ед./год; $C_{инфр}$ – стоимость установки и настройки системы, ден.ед.; $C_{ком}$ – стоимость услуг (например, командировки сотрудников) обслуживающей компании, ден.ед..

$$C_{настр} = C_{час} \sum_i N_i T_{настр}$$

где $C_{час}$ – стоимость часа работы по инсталляции необходимого аппаратного и программного обеспечения, ден.ед./час; N_i – количество единиц оборудования *i*-того типа, которое необходимо настроить; $T_{настр}$ – время настройки оборудования *i*-того тип, часы.

Если пользователь не нуждается в помощи внешнего технического специалиста по установке и настройке системы, то:

$$C_{настр} = 0,$$
$$C_{ком} = 0,$$
$$C_{внедр} = C_{лиц}.$$

3. Стоимость годового обслуживания системы фильтрации C_p, которая рассчитывается по следующей формуле:

$$C_p = N_{польз} \cdot C_{польз.\,лиц} + C_{обсл.сист} + C_{поддерж}$$

где $N_{польз}$ – количество пользователей системы фильтрации; $C_{польз.\,лиц}$ – стоимость лицензии одного пользователя, ден.ед./год; $C_{обслсист}$ – стоимость обслуживания системы, ден.ед./год; $C_{поддерж}$ – стоимость технической поддержки системы, ден.ед./год.

Если система относиться к классу несопровождаемых систем, то:

$$C_{обслсист} = 0,$$
$$C_{поддерж} = 0$$
$$C_p = N_{польз} C_{польз.\,лиц}.$$

Алгоритм определения стоимости системы показан на рисунке 5.

3.5 Алгоритм выбора системы фильтрации контента

Обобщенная постановка задачи многокритериального оптимального выбора системы фильтрации контента (рис. 5) заключается в формировании иерархической структуры обобщённого критерия оптимальности в виде соподчинённых уровней целей, подцелей и целевых функций; математического описания функциональных зависимостей и параметрических ограничений задачи многокритериального оптимального выбора; формирования иерархической структуры взаимосвязи альтернатив принимаемых решений.

На основе анализа профилей пользователей средств фильтрации контента формируется множество критериев $F_C = \{f_i, i \in \overline{1,k}\}$.

Для выбора оптимального решения из списка отобранных средств фильтрации контента, необходимо доопределить предпочтения пользователя, а именно: ранжировать критерии f_i по степени их важности для пользователя. Для определения относительной важности f_i пользователем заполняется матрица парных сравнений S_f.

В ходе заполнения матрицы пользователю предлагается сделать выбор одной из трех альтернатив:

1) критерий f_i важнее чем f_j – $f_i \succ f_j$;

2) критерий f_i равнозначен f_j – $f_i = f_j$;

3) критерий f_i менее важен чем f_j – $f_i \prec f_j$;

В соответствии с этим элементы матрицы S_f будут принимать значения

$$s_{f,ij} = \begin{cases} 2, & f_i \succ f_j; \\ 1, & f_i = f_j; \\ 0{,}5, & f_i \prec f_j; \end{cases} \quad , \forall j \geq i \, .$$

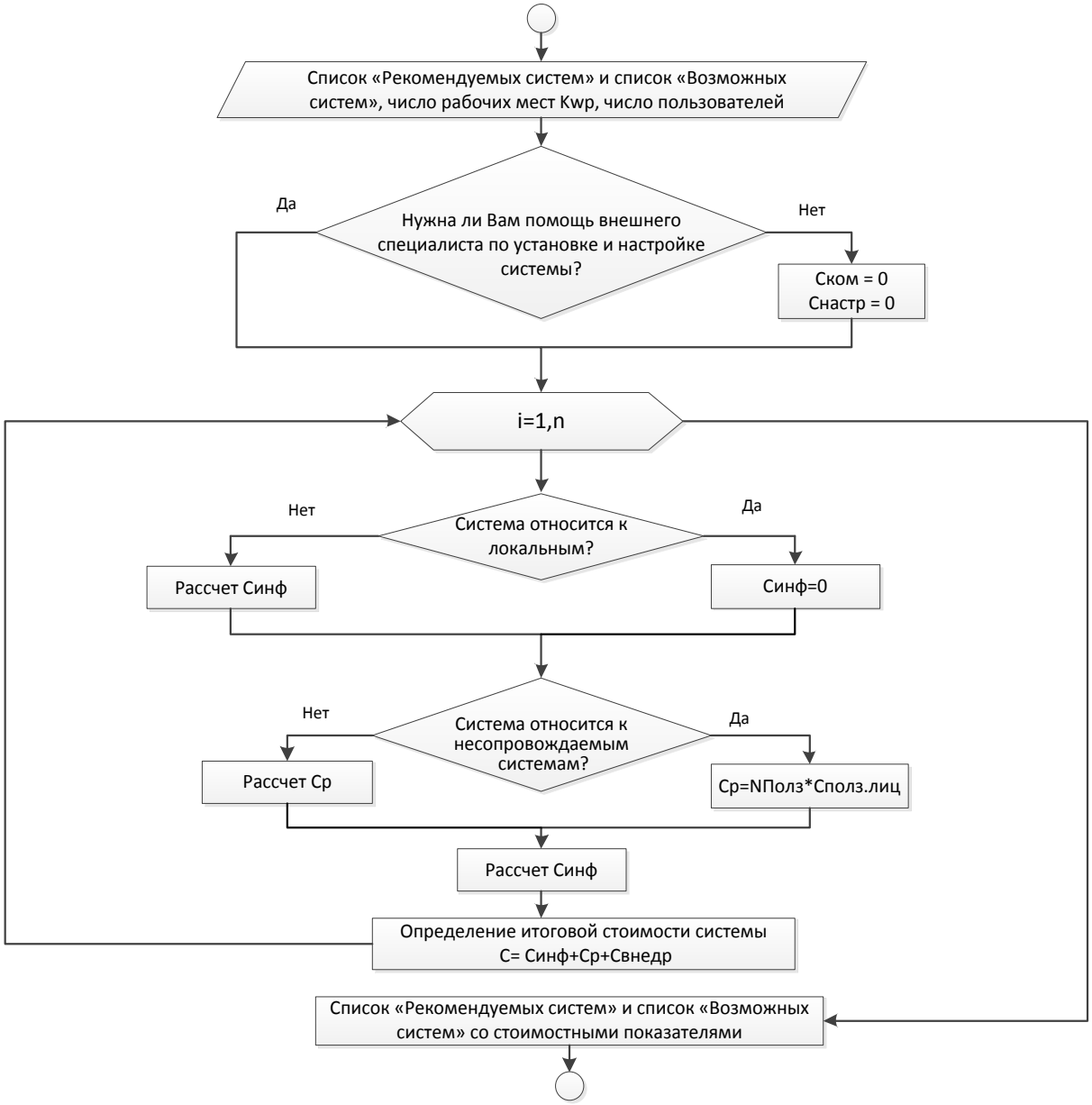

Рисунок 5 – Алгоритм определения стоимости системы

Поскольку матрица S_f – обратно симметричная, то

$$s_{ji} = \frac{1}{s_{ij}} \, .$$

Для строк матрицы S_f вычисляются сначала геометрические средние

$$\left\langle s_{f_i} \right\rangle = \sqrt[k]{\prod_{j=1}^{k} s_{f,ij}} ,$$

а затем сумма

$$\varepsilon_{f_i} = \sum_{i=1}^{k} \left\langle s_{f_i} \right\rangle$$

Усредненные оценки критериев нормируются по формуле

$$\left\langle f_i \right\rangle^n = \frac{\left\langle s_{f_i} \right\rangle}{\varepsilon_{f_i}},$$

где $\left\langle f_i \right\rangle^n$ – относительная важность критериев оценивания средств фильтрации контента с точки рения пользователя.

Приведем алгоритм определения относительной важности критериев пользователем.

Сформированный на основании анализа требований пользователя список доступных для выбора средств фильтрации контента, образует множество альтернатив $X = \{x_i : i \in [1, I_U]\}$, где I_U – количество альтернатив. Для выбора оптимального решения альтернативы оцениваются с учетом предпочтений пользователя выраженных в относительной важности критериев. Сравнительная оценка альтернатив x_i для каждого критерия f_k осуществляется по такому же принципу, как и сравнительная оценка критериев, путем заполнения матрицы парных сравнений S_{f_i} с использованием, полученных на стадии формирования базы средств фильтрации контента, бальных экспертных оценок B_{f_k,x_i}.

Элементы матрицы парных сравнений альтернатив S_{X,f_i} для 5-ти бальных оценок альтернатив по критерию f_i определяются по формуле:

$$s_{f_i,x_k x_j} = \begin{cases} 9, & (b_{f_i,x_k} - b_{f_i,x_j}) = 4; \\ 7, & (b_{f_i,x_k} - b_{f_i,x_j}) = 3; \\ 5, & (b_{f_i,x_k} - b_{f_i,x_j}) = 2; \\ 3, & (b_{f_i,x_k} - b_{f_i,x_j}) = 1; \\ 1, & (b_{f_i,x_k} - b_{f_i,x_j}) = 0; \\ 1/3, & (b_{f_i,x_k} - b_{f_i,x_j}) = -1; \\ 1/5, & (b_{f_i,x_k} - b_{f_i,x_j}) = -2; \\ 1/7, & (b_{f_i,x_k} - b_{f_i,x_j}) = -3; \\ 1/9, & (b_{f_i,x_k} - b_{f_i,x_j}) = -4; \end{cases},$$

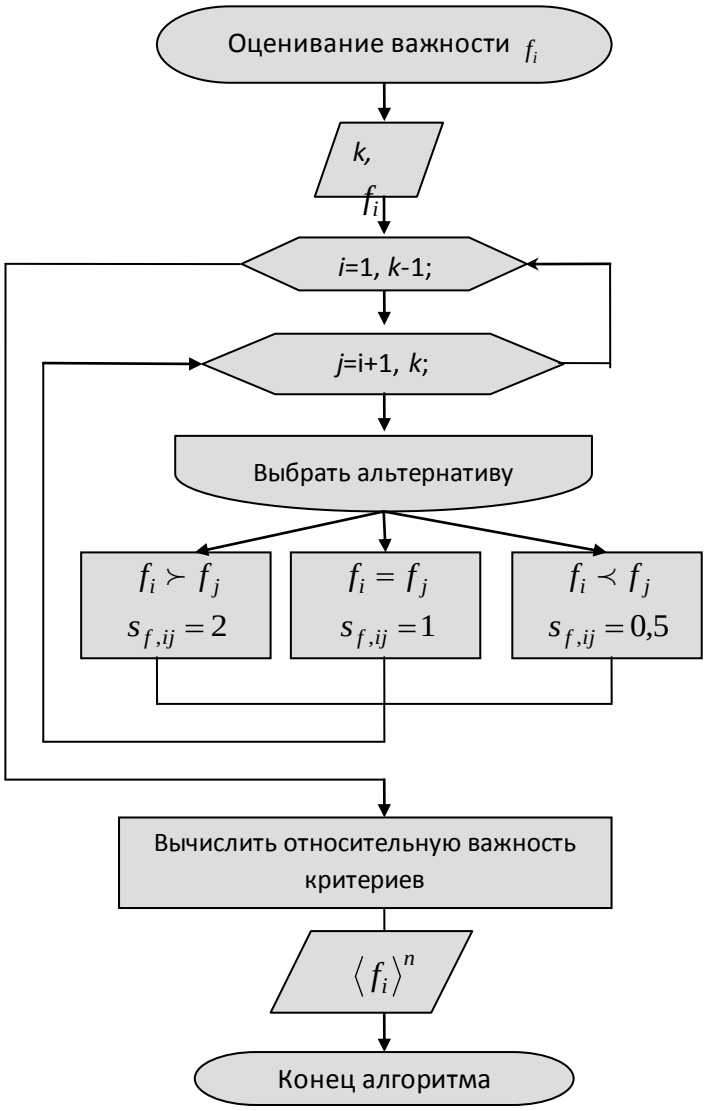

Рисунок 6 – Вычисление относительной важности критериев $\forall j \geq k$.

Для каждой матрицы вычисляются: геометрические средние по строкам

$$\left\langle s_{f_i} \right\rangle_{x_k} = \sqrt[I_U]{\prod_{j=1}^{I_U} s_{f_i, x_k x_j}} \ , \ \forall k \in \overline{1, I_U}$$

и суммы

$$\Omega_{f_i} = \sum_{k=1}^{I_U} \left\langle s_{f_i} \right\rangle_{x_k} .$$

Усредненные оценки предпочтительности альтернатив нормируются по формуле

$$\left\langle s_{f_i} \right\rangle_{x_i}^n = \frac{\left\langle s_{f_i} \right\rangle_{x_i}}{\Omega_{f_i}},$$

где $\left\langle s_{f_i} \right\rangle_{x_i}^{n}$ – относительная предпочтительность альтернатив с точки зрения пользователя.

Алгоритм вычисления матриц сравнения альтернатив приведен на рис. 7.

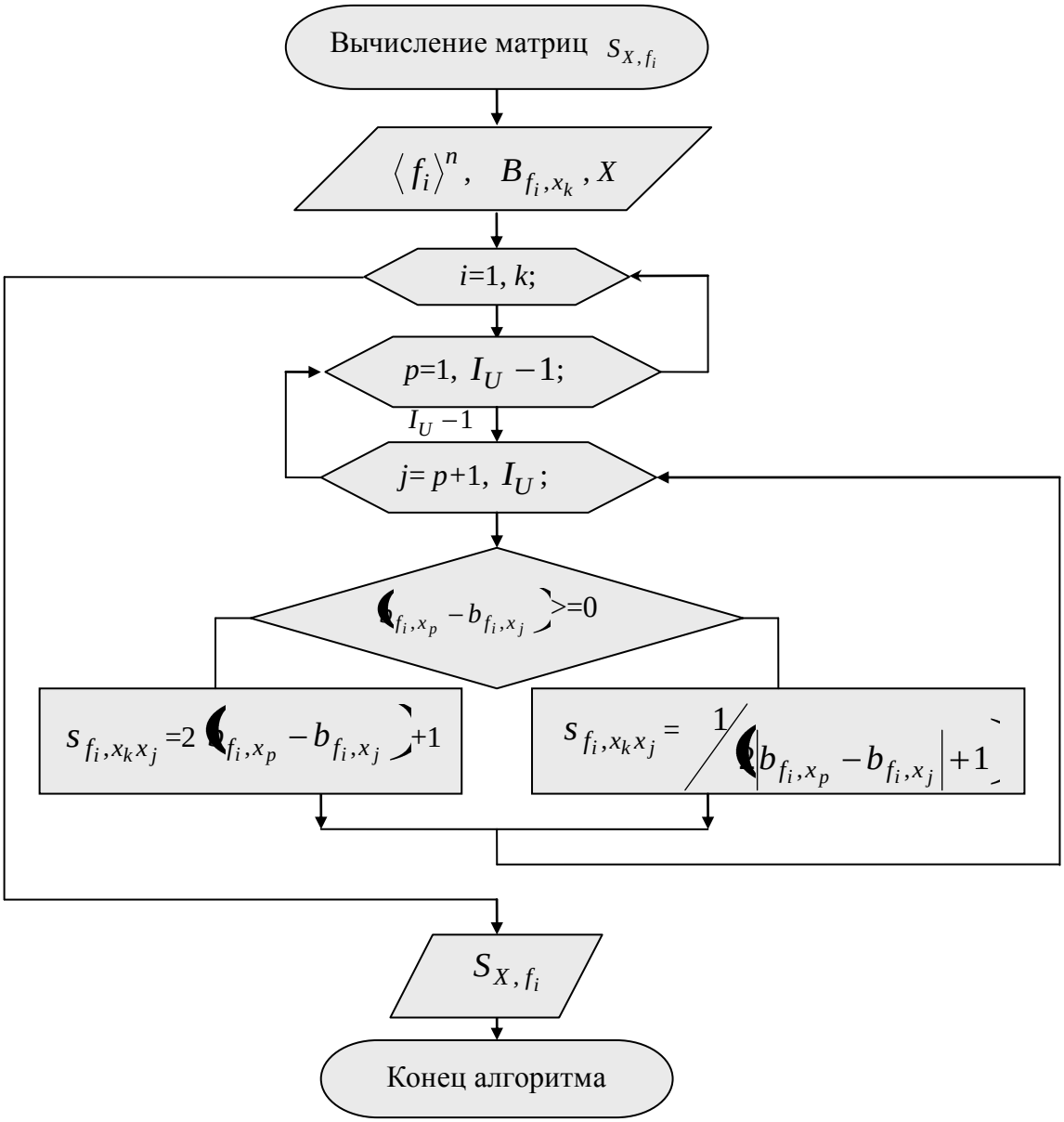

Рисунок 7 – Алгоритм вычисления матриц парных сравнений альтернатив

После заполнения матриц и вычисления относительной предпочтительности альтернатив для критерия находим взвешенные относительные оценки альтернатив для каждого критерия:

$$a_{x_i} = \langle f_j \rangle^n \langle S_{f_i} \rangle_{x_i}^{n}.$$

Интегральные оценки альтернатив вычисляются по формуле:

$$A_{x_i} = \sum_{f_i} a_{x_i} .$$

Оптимальное решение – это:

$$x_{i\ \max} = \arg\max_{x_j} A_{x_j}.$$

Если предложенное оптимальное решение не устраивает пользователя, следующее оптимальное решение определяется по формуле:

$$x_{k\ \max} = \arg\max_{x_j} \left(A_{x_j} \setminus x_{i\ \max} \right).$$

3.6. Формирование бальных оценок систем фильтрации контента в соответствии с выбранными критериями

Предположим, множество F состоит из следующих критериев:

1) f_1 – уровень защиты от несанкционированного доступа;
2) f_2 – простота использования;
3) f_3 – функциональность;
4) f_4 – стоимость ПОФ.

При наполнении базы данных СФК бальная оценка B_{f_k, x_i} альтернативы x_i по критерию f_k определяются путём экспертного оценивания с использованием метода непосредственной (балльной) оценки. Для каждого экземпляра СФК экспертом выносится оценка по 5-балльной шкале, в соответствии с предложенными 5 уровнями компетенции пользователя: новичок, пользователь, опытный пользователь, технический специалист и эксперт. Это относится только к критериям f_1, f_2.

Для критериев $f_1 - f_4$ примеры шкал приведены в таблице.

Согласно стандарта ISO 9126:2001 функциональность – способность ПО в определенных условиях решать задачи, нужные пользователям, и для его оценки необходимо оценить следующие параметры:

- Функциональная пригодность. Способность решать нужный набор задач.
- Точность. Способность выдавать нужные результаты.
- Способность к взаимодействию. Способность взаимодействовать с нужным набором других систем.
- Соответствие стандартам и правилам. Соответствие ПО имеющимся индустриальным стандартам, нормативным и законодательным актам, другим регулирующим нормам.

Каждому из перечисленных параметров в описании производителя соответствует набор функций. В соответствии с этим эксперт проверяет для каждой альтернативы x_i заявленный производителем функционал, подсчитывая: общее количество заявленных функций N_{f, x_i} и количество функций N_{zr, x_i}, которые в процессе тестирования дали заявленный результат. По результату тестирования эксперт выставляет оценку:

$$B_{f_3, x_i} = \left\lceil \frac{5N_{zr, x_i}}{N_{f, x_i}} \right\rceil .$$

Критерий, f_k	Уровень компетенции пользователя	Балл, B_{f_k, x_i}	Примечание
1	2	3	4
f_1 – уровень защиты	Новичок	1	СФК взаимодействует только с одним конкретным приложением доступа к контенту, например с одним конкретным браузером, или информационным ресурсом, и для обхода достаточно воспользоваться другим приложением из стандартной поставки ОС, офисного пакета или аналогичным ресурсом; фильтрация отключается одной не требующей введения пароля настройкой, например включить/выключить режим фильтрации, поставить/снять галочку напротив категории фильтрации и т.д.
	Пользователь	2	Достаточно воспользоваться приложением не из стандартной поставки ОС или офисного пакета, например альтернативным браузером или торрент-клиентом, отключить межсетевой экран, отыскать без использования специальных терминов несложную инструкцию в Интернет и т.д.
	Опытный пользователь	3	Необходимо загрузить из Интернета, установить и настроить приложение, воспользоваться генератором паролей для взлома пароля, внести изменения в системные настройки ПК, создать новую учётную запись пользователя ПК, выполнить детальную перенастройку сетевого экрана и т.д.
	Технический специалист	4	Требуется понимание сетевых технологий и протоколов, умение работать со специализированным программным обеспечением, конфигурировать локальные сети и настраивать межсетевое взаимодействие, знания специализированных ресурсов и сервисов, и т.д.
	Эксперт	5	Сложность обхода не ограничена
f_2 – простота использования	Новичок	5	Не требуется установка и настройка ПО, либо процесс установки и настройки максимально упрощён (1-2 действия без ввода каких-либо сетевых или системных параметров, обновление системы осуществляется автоматически)
	Пользователь	4	Требуется установка, несложная настройка приложения с использованием графического интуитивно понятного интерфейса, обновление системы осуществляется автоматически и т.п.

Продолжение табл. 6

	Опытный пользователь	3	Требуется установка, детальная настройка приложения без применения специальных знаний, дополнительная настройка других работающих в системе приложений, например межсетевого экрана, обновление системы осуществляется вручную и т.п.
	Технический специалист	2	Требуется установка, полное конфигурирование приложения с использованием специальных знаний, дополнительное конфигурирование системного ПО и сетевого оборудования, настройка автоматического обновления системы и т.п
	Эксперт	1	Сложность установки, настройки и сопровождения не ограничена
f_3 – функциональность	Не связан с уровнем компетенции пользователя	$\left\lceil \frac{5N_{zr,x_i}}{N_{f,x_i}} \right\rceil$	N_{f,x_i} – общее количество заявленных функций; N_{zr,x_i} – количество функций, которые в процессе тестирования дали заявленный результат.
f_4 – стоимость	Не связан с уровнем компетенции пользователя	1	$C_{\min} \le C_{x_i} \le C_1,\ C_1 = C_{\min} + \frac{C_{\max} - C_{\min}}{5},$ C_{x_i} – итоговая стоимость альтернативы x_i согласно п. 3.4
		2	$C_1 \le C_{x_i} \le C_2,\ C_2 = C_{\min} + \frac{2(C_{\max} - C_{\min})}{5}$
		3	$C_2 \le C_{x_i} \le C_3,\ C_3 = C_{\min} + \frac{3(C_{\max} - C_{\min})}{5}$
		4	$C_3 \le C_{x_i} \le C_4,\ C_4 = C_{\min} + \frac{4(C_{\max} - C_{\min})}{5}$
		5	$C_4 \le C_{x_i} \le C_{\max}$

Также при заполнении базы в соответствующее поле вводится бальная оценка стоимости системы фильтрации B_{f_4,x_i}. Оценка стоимости B_{f_4,x_i} определяется экспертами, с учетом определенной в пункте 3.4 итоговой стоимости системы и может принимать значение:

$$B_{f_4,x_i} = \begin{cases} 5, & C_{\min} \le C_{x_i} \le C_1 \\ 4, & C_1 \le C_{x_i} \le C_2 \\ 3, & C_2 \le C_{x_i} \le C_3 \\ 2, & C_3 \le C_{x_i} \le C_4 \\ 1, & C_4 \le C_{x_i} \le C_{\max} \end{cases}$$

где C_{min} – минимальное значение стоимости среди всех доступных к выбору систем (списки «Рекомендуемые системы» и «Возможные системы»); C_{max} – максимальное значение стоимости среди всех доступных к выбору систем (списки «Рекомендуемые системы» и «Возможные системы»).

Инструкция по проведению экспертизы существующих технических решений фильтрации контента и наполнению единой базы данных систем фильтрации контента приведена в Приложении Г.

Алгоритм выбора оптимального решения показан на рисунке 8.

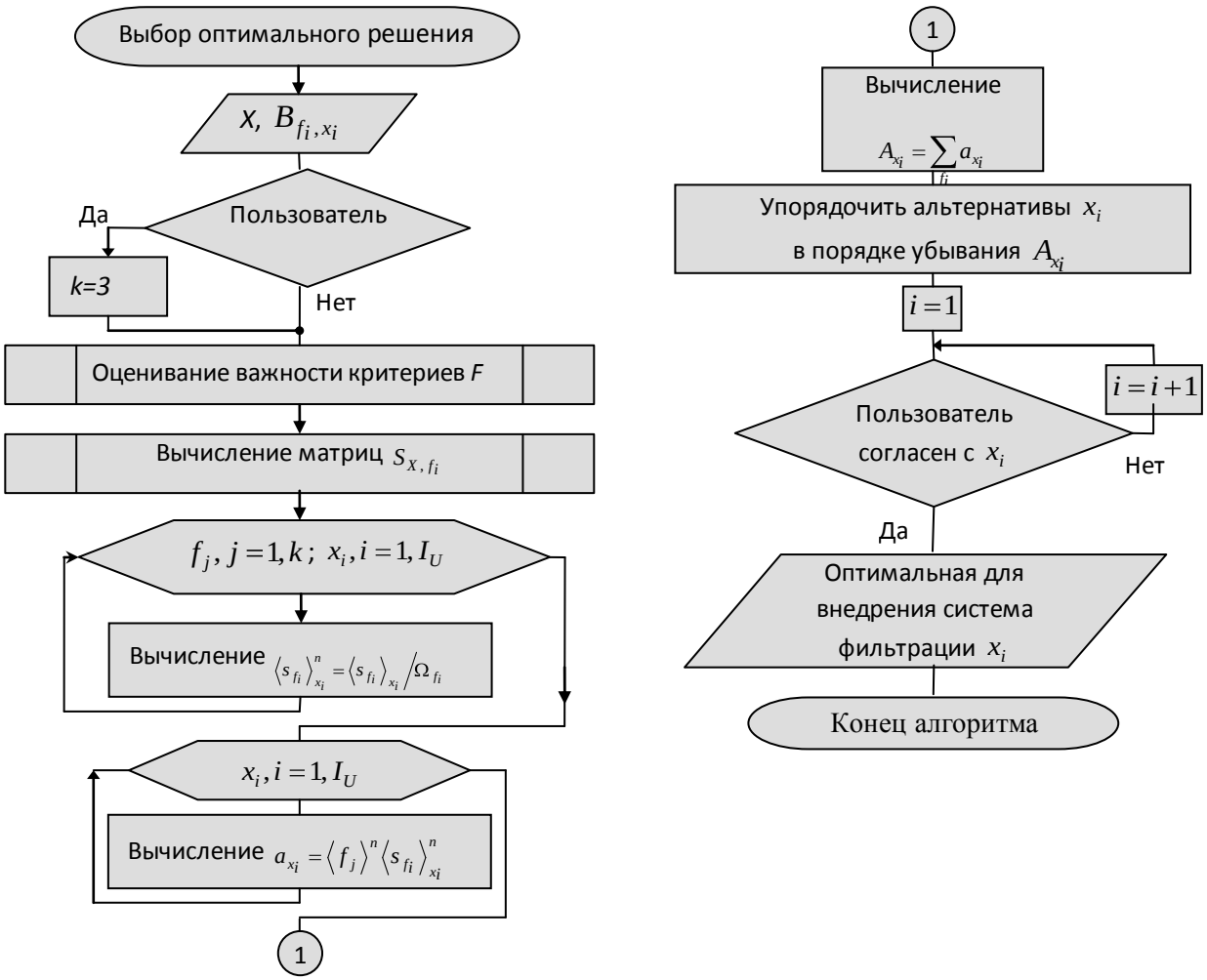

Рис. 8 – Алгоритм выбора оптимальной системы фильтрации.

4. Рекомендации по реализации программного обеспечения для выбора системы фильтрации контента

4.1 Обобщённая архитектура автоматической рекомендательной системы

Обобщённая архитектура автоматической рекомендательной системы по выбору СФК приведена на рис. 9. Она состоит из следующих элементов:

1. Интерфейс пользователей системы.
2. Рекомендательна система.
3. Интерфейс экспертов системы.

Интерфейсы пользователей стратифицированы в зависимости от их компетентности. На рис. 9 приведена группа пользователей соответствующая уроню компетентности «Пользователь». Такая стратификация позволяет более точно учесть пожелания пользователя для оптимального выбора системы фильтрации контента.

Следующая группа – это персонифицированные интерфейсы экспертов. Эксперты анализируют и тестируют новые решения в области ограничения доступа к нецелевым ресурсам, оценивают их свойства и, тем самым, актуализируют базу данных о системах фильтрации контента.

Рекомендательная система в обобщенной форме представлена тремя компонентами.

1) Клиентская часть, которая обеспечивает взаимодействие с пользователями системы.
2) Экспертная часть, которая обеспечивает взаимодействие с экспертами.
3) База данных, которая состоит из системы управления базой данных, администратора базы данных и непосредственно хранилища данных о системах фильтрации контента.

Общая задача системы управления базой данных и администратора базы данных – обеспечение целостности данных. В свою очередь система управления базой данных выполняет функцию обработки требований или запросов пользователей и, в соответствии с запросом, формирует список систем фильтрации контента, а также реализует выбор оптимальной системы фильтрации контента и передает результаты пользователю через соответствующий интерфейс.

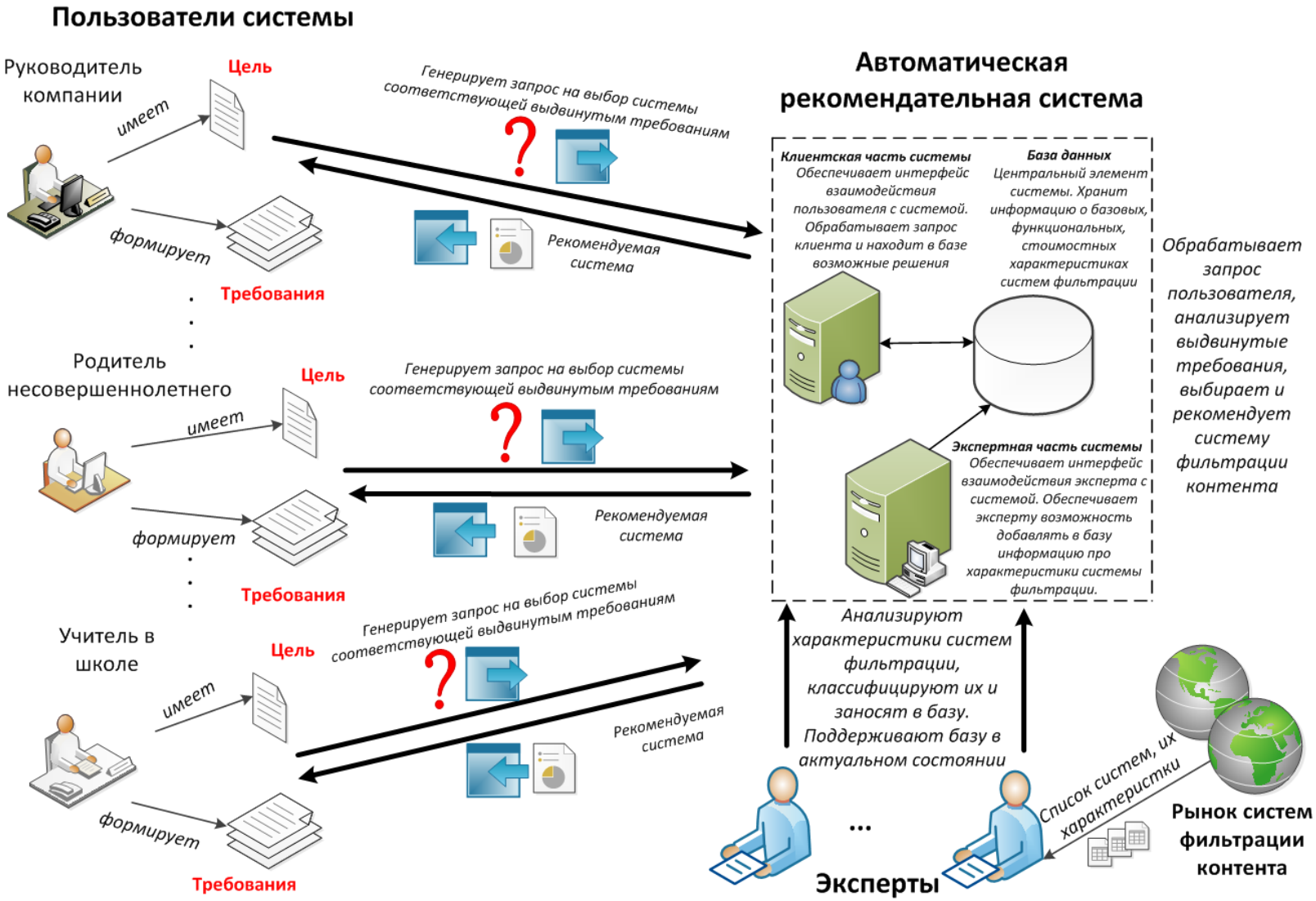

Рис. 9 – Обобщённая архитектура автоматической рекомендательной системы.

4.2 Внешний вид интерфейса пользователя системы

Интерфейс пользователя системы имеет иерархическую структуру. Первый уровень иерархии – это окно регистрации пользователя (рис. 10).

1. Окно регистрации пользователя

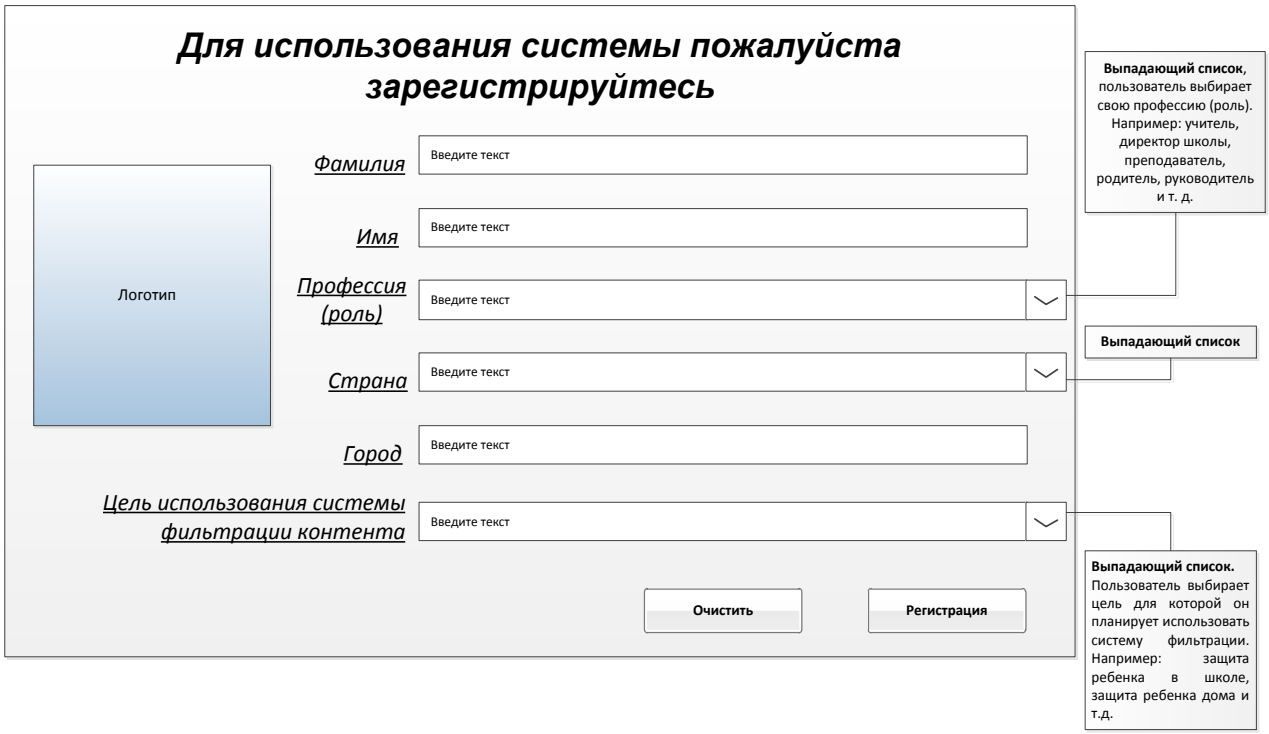

Рис. 10 – Окно регистрации пользователя

После регистрации пользователя определяется уровень его компетентности с использованием последовательности окон (рис. 11-13)

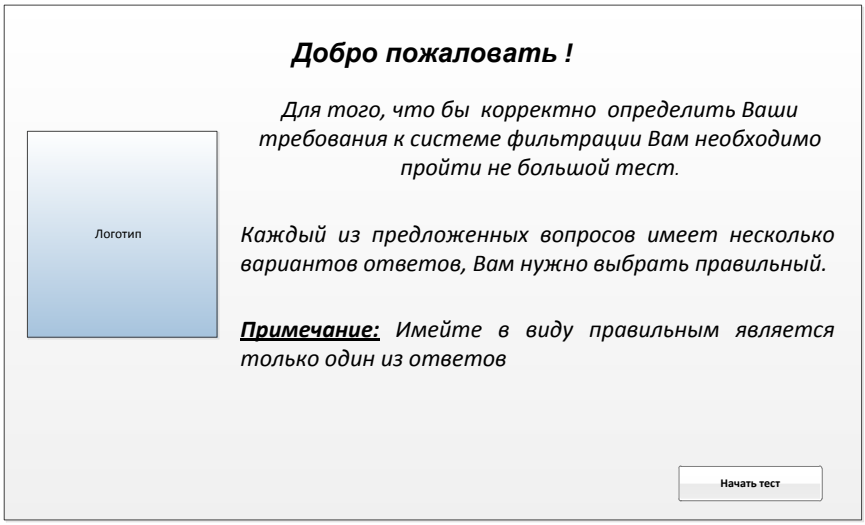

Рис. 11 – Стартовое окно процедуры определения компетентности пользователя

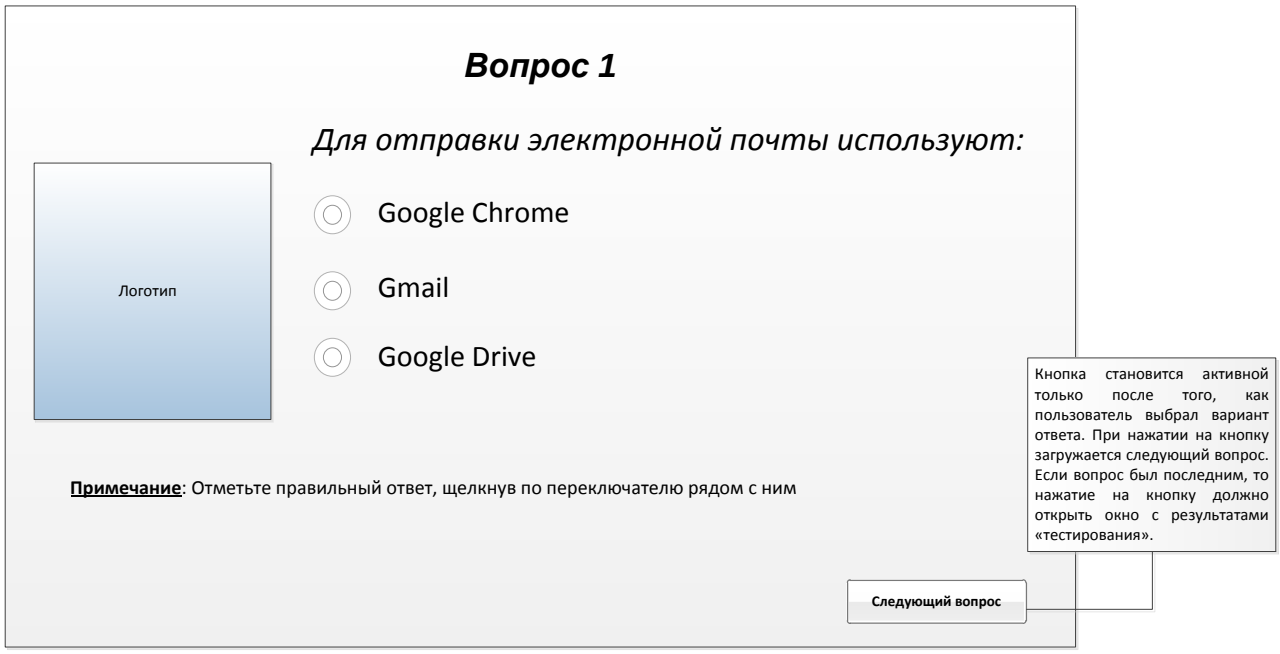

Рис. 12 – Пример окна тестирования пользователя

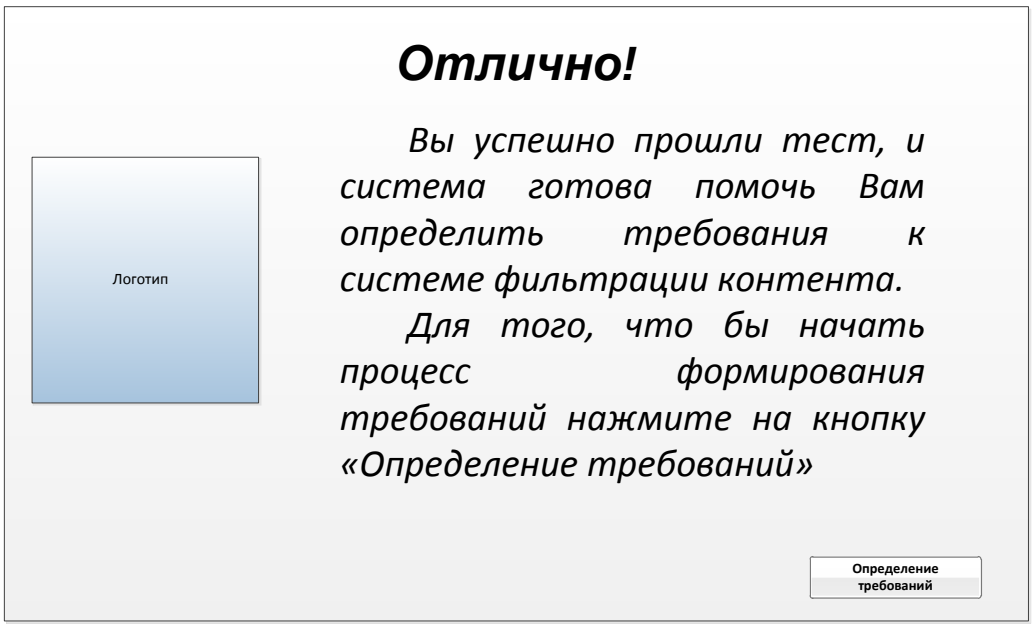

Рис. 13 – Окончание тестирования и перехода к выбору системы.

На рис. 14 приведен стартовый интерфейс пользователя по выбору системы фильтрации контента. С помощью этого интерфейса пользователь может указать способ реализации СФК и определить стоимость модернизации или создания локальной компьютерной сети (см. рис. 15,16)

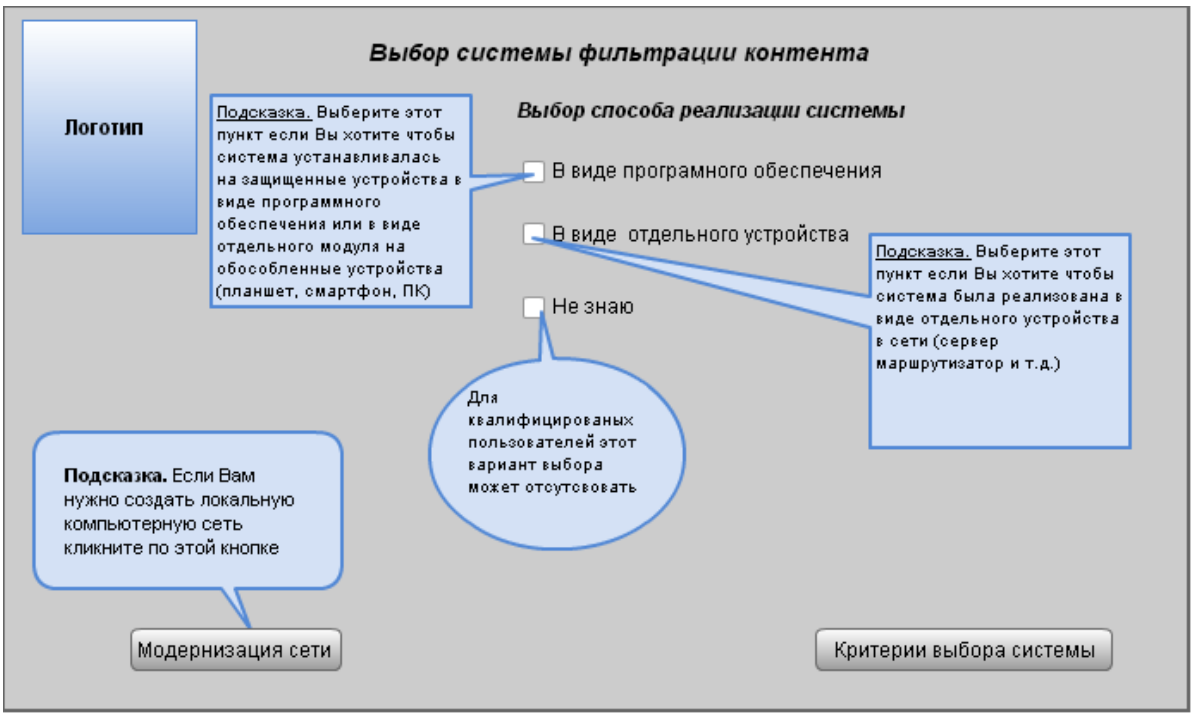

Рис. 14 – Стартовое окно выбора системы фильтрации контента

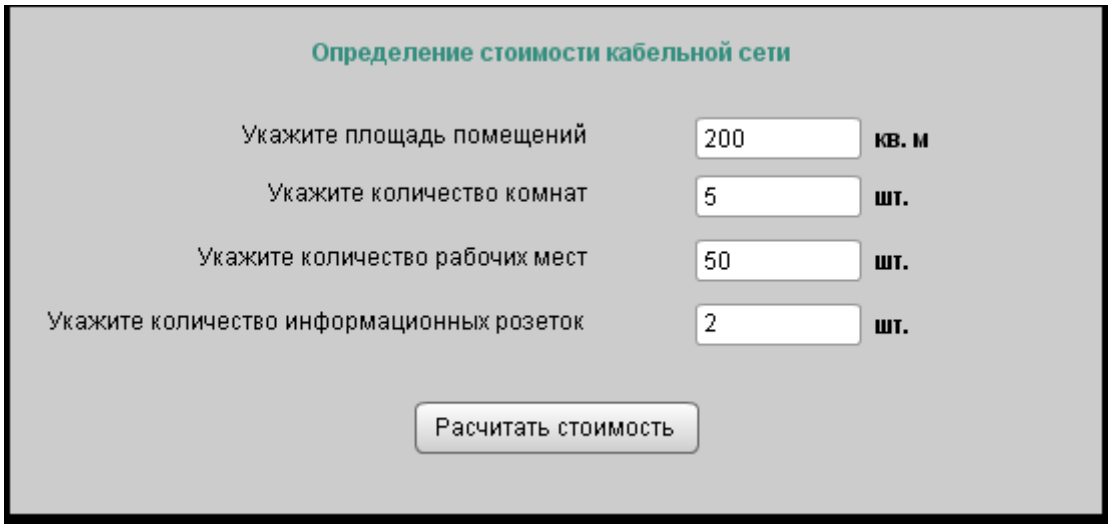

Рис. 15 – Окно для определения стоимости локальной кабельной компьютерной сети

После заполнения полей окна пользователь получает отчет о примерной стоимости локальной кабельной сети. Вид отчета приведен на рис. 16.

Стоимость монтажа локальной компьютерной сети

Стоимость работ

Вид работ	*Стоим. за ед.*	*Объем*	*Сумма*
Прокладка кабеля	15 руб/м.	2012	30180
Монтаж короба	45 руб/м.	175	7877
Монтаж порта розетки	95 руб/шт	100	9500
Расшивка одного порта кросс/патч панели	40 руб/шт	100	4000
		Итого	**51 550**

Стоимость материалов

Наименование	*Количество*	*Стоимость*	*Сумма*
Кабель	2012	10	2012
Короб	175	110	19250
Модуль розетки	100	42	4200
		Итого	**43 570**

Вернуться к выбору СФК

Общая стоимость **95 120**

Рис. 16 – Стоимость локальной кабельной сети

После нажатия кнопки «Критерии выбора системы» пользователь в открывшемся окне определяет относительную важность критериев оптимального выбора СФК

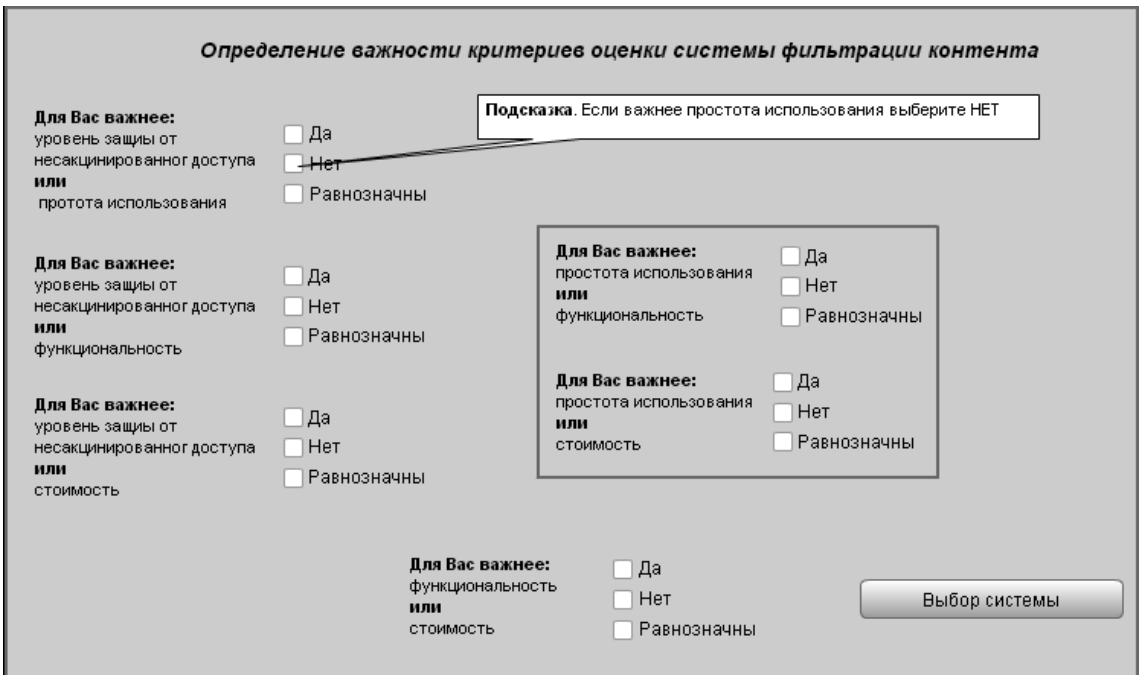

Рис. 17 – Определение предпочтений пользователя

После заполнения всех форм в окне (рис. 18) пользователю предлагается наиболее оптимальный, с учетом его предпочтений вариант СФК.

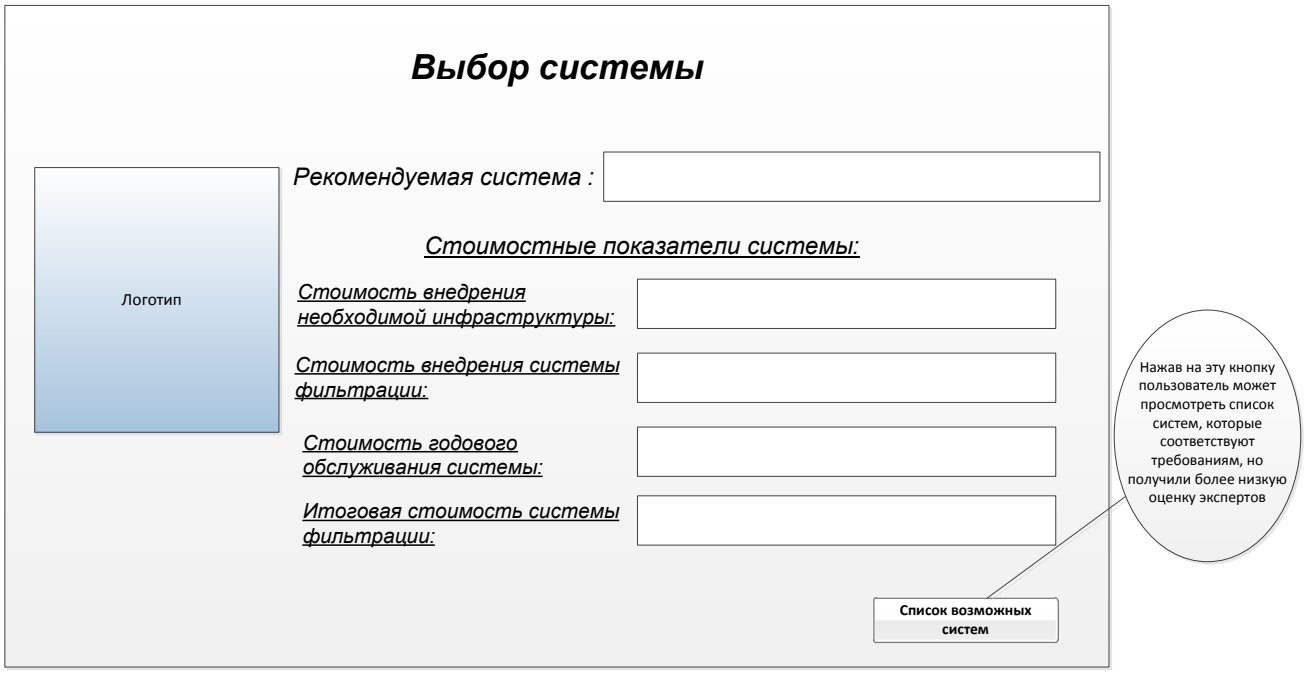

Рис. 18 – Рекомендуемая система

Если по каким-то причинам данный выбор не устраивает пользователя он может просмотреть все отобранные, в соответствии с его требованиями, СФК и выбрать подходящую (см. рис. 19).

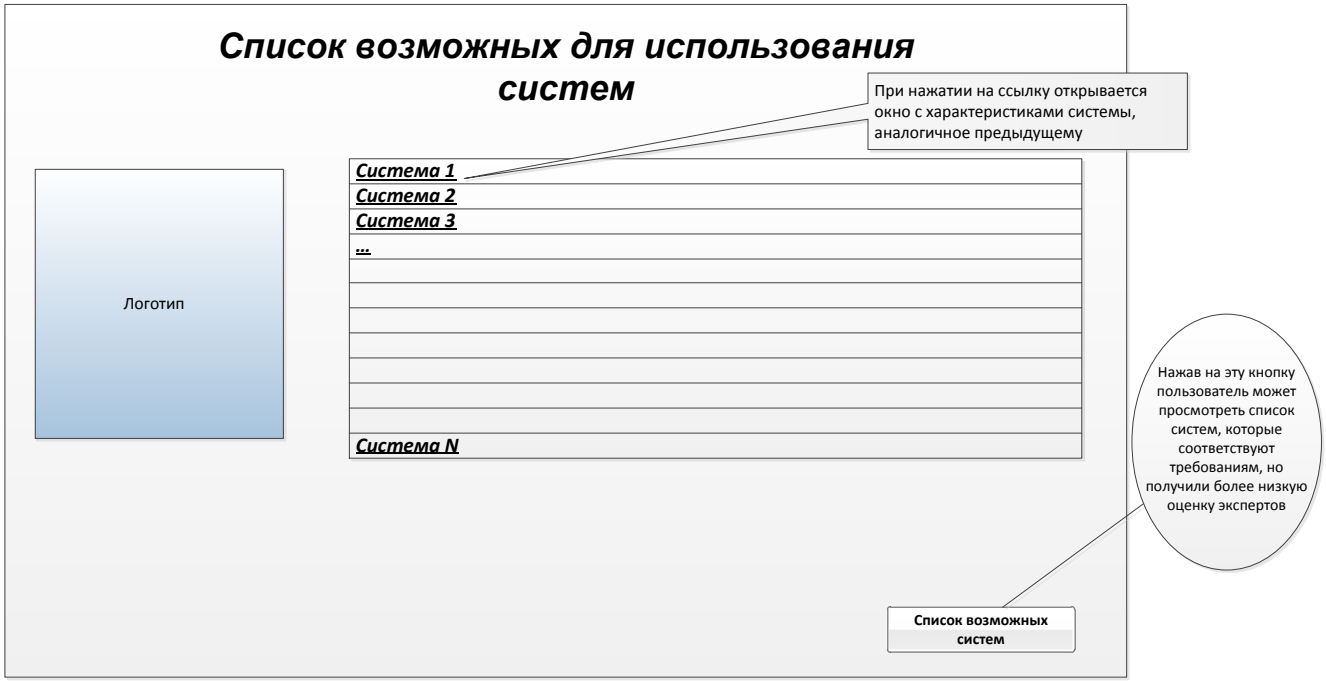

Рис. 19 – Перечень отобранных СФК

4.3 Интерфейс наполнения системы и экспертного оценивания СФК

В соответствии предложенным принципом формирования базы решений по фильтрации контента все СФК должны пройти процедуру экспертного оценивания. Интерфейс подсистемы экспертного оценивания СФК состоит из следующих компонент. Первое окно – авторизация эксперта (рис. 20)

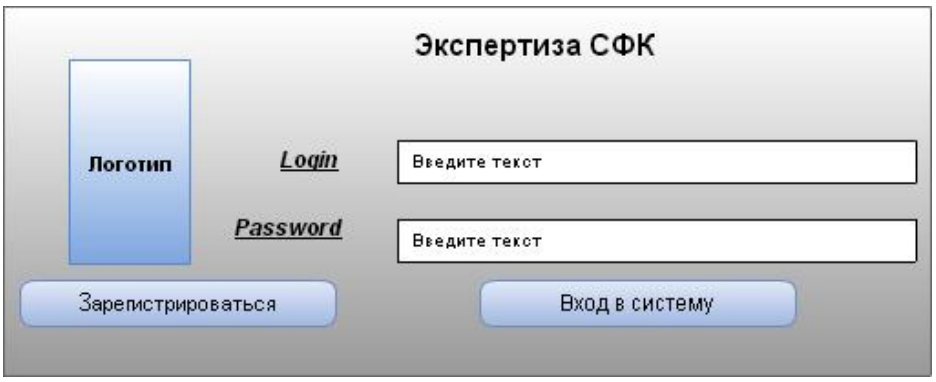

Рис. 20 – Окно авторизации или регистрации эксперта

После регистрации или авторизации эксперт получает доступ к системе управления базой данных СФК в пределах указанных функций (рис. 21)

Рис. 21 – Функции эксперта в системе управления базой данных СФК

При выборе функции «Добавить новую СФК» эксперт путем выбора характеристик в формах приведенных на рис. 22, описывает новую СФК:

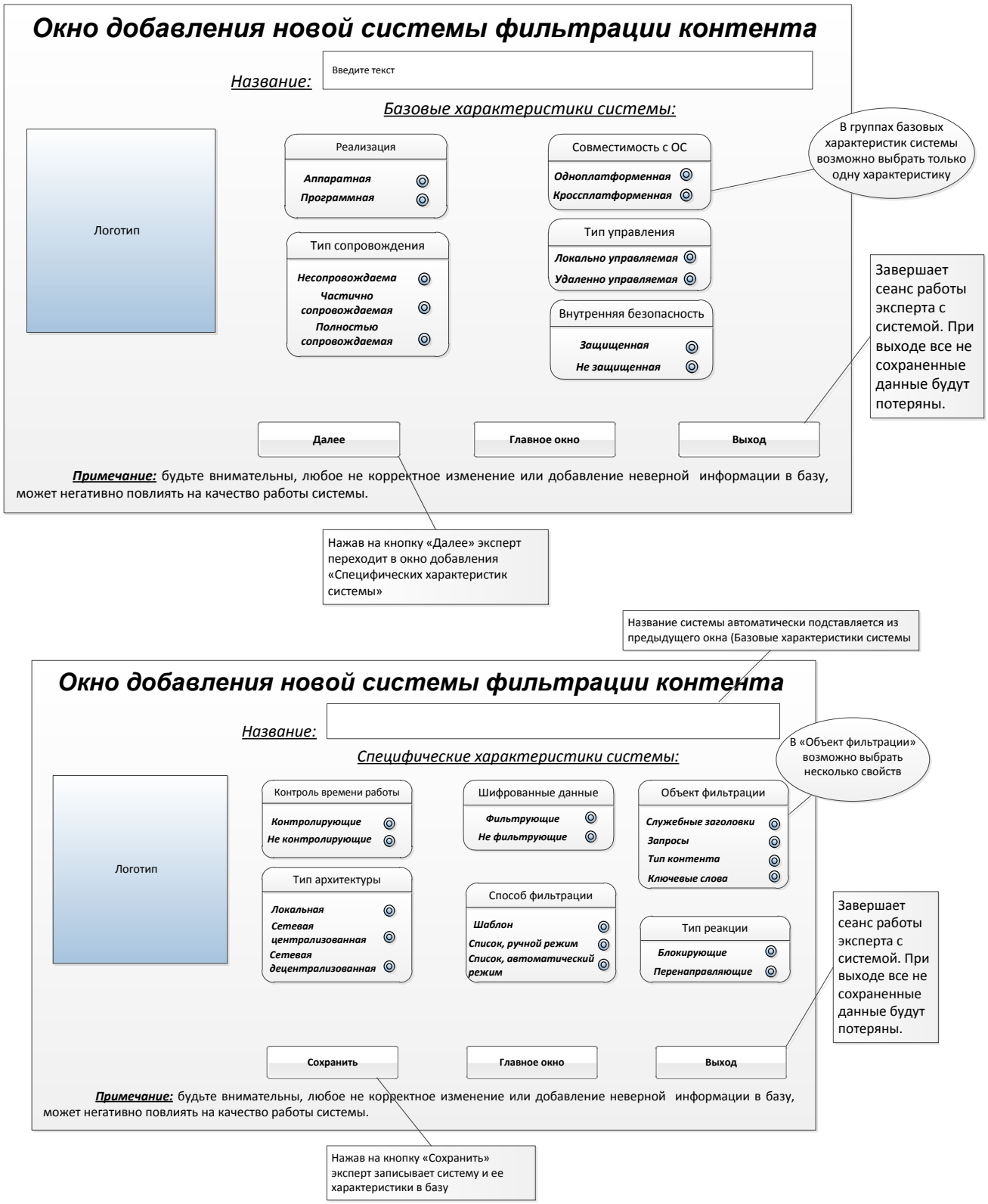

Рис. 22 – Описание новой СФК

При необходимости внести изменения в описание системы эксперт обращается к функции «Редактирование характеристик СФК» и корректирует данные в формах, приведенных на рис. 23-24.

Рис. 23 – Редактирование базовых и специфических характеристик системы

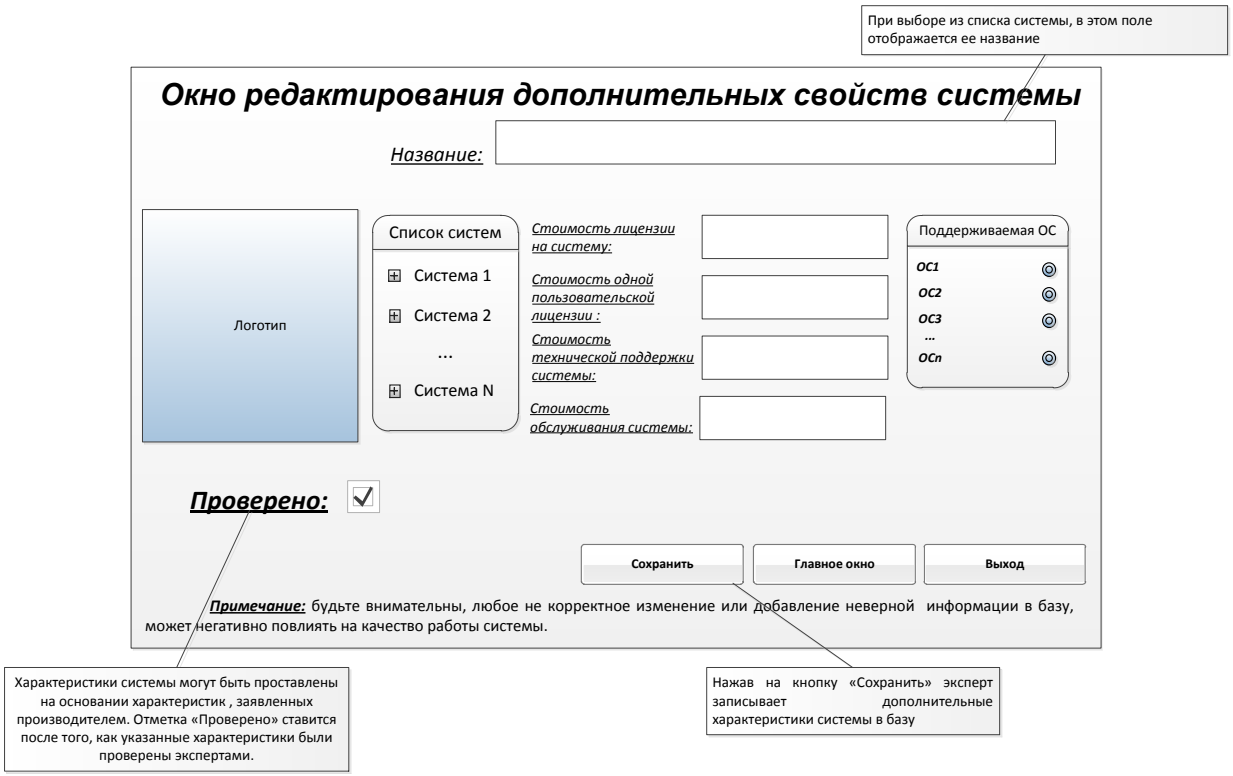

Рис. 24 – Редактирование /добавление дополнительных характеристик системы

После описания характеристик СФК эксперт выполнят итоговую бальную оценку ее потребительских свойств, выбрав функцию «Бальная оценка свойств СФК» (рис. 25).

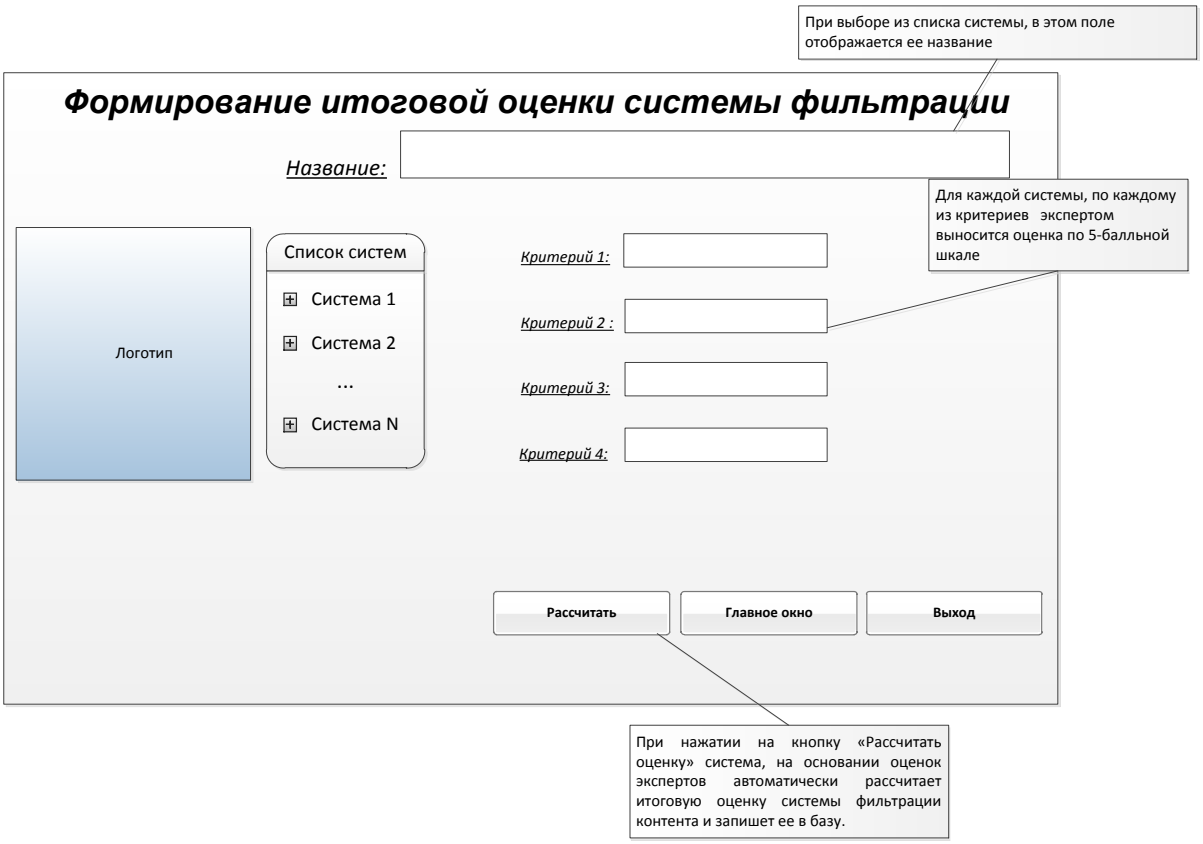

Рис. 25 – Окно формирования итоговой бальной оценки системы

Литература

1. OpenNet Initiative Access Denied: The Practice and Policy of Global Internet Filtering — Cambridge: MIT Press, 2008.
2. James Hookway. Vietnam Convicts 3 Bloggers Over Posts. The Wall Street Journal
3. Reporters Without Borders, “Internet Enemies Report 2012,” 2012.
4. Derek E. Bambauer Cybersieves // Duke Law Journal. — 2009.
5. The Berkman Center for Internet and Society, “Circumvention Landscape Report Methods, Uses, and Tools,” 2007.
6. OpenNet Initiative Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace — Cambridge: MIT Press, 2010.
7. OpenNet Initiative Access Contested: Security, identity, and resistance in Asian cyberspace — Cambridge: MIT Press, 2011.
8. The Berkman Center for Internet and Society, “2011 Circumvention Tool Evaluation,” 2011.
9. How To Bypass Internet Censorship // [http://www.howtobypassinternetcensorship.org/].
10. Freedom House, “Freedom on the Net 2012 ,” 2012.
11. Claudio Squarcella, Emile Aben Alberto Dainotti Analysis of Country-wide Internet Outages Caused by Censorship // Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference. — 2011.
12. William H. Dutton и др., “Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet,” 2011.

13. Tim Wu Jack Goldsmith Who Controls the Internet: Illusions of a Borderless World USA — s.l.: Oxford University Press, 2008.
14. A Look at Twitter in Iran (2009). Sysomos Blog.
15. Al Jazeera (2012). Facts and figures. Al Jazeera official web page.
16. Blogs and Bullets: New Media in Contentious Politics. (2010). Peaceworks.
17. Burns, A. & Eltham, B. (2009). Twitter Free Iran: an Evaluation of Twitter's Role in Public Diplomacy and Information Operations in Iran's 2009 Election Crisis. Communications Policy & Research Forum.
18. Clinton, H.R. (2010). Remarks on Internet Freedom.
19. Desouza, K.C. & Lysenko, V.V. (2012). Moldova's internet revolution: analyzing the role of technologies in various phases of the confrontation. Technological forecasting & social change: an international journal. Vol. 79.
20. Duffy, M. (2011). Smartphones in the Arab Spring. International Press Institute.
21. Dunn, A. Unplugging a Nation: State Media Strategy During Egypt's January 25 Uprising. (2011). Fletcher Forum of World Affairs.
22. Google Transparency Report (2011).
23. Franceschi-Bicchierai, L. (2013). What Happens to Social Media After a Twitter Revolution Mashable.
24. Freedom on the Net (2012). Freedom House.
25. www.entensys.ru/products/usergate_web_filter
26. www2.pineapp.com/products/2/web-filtering
27. www.barracuda.com/products/webfilter
28. www.websense.com/content/web-filter-features.aspx
29. www.entensys.ru Сравнение DNS-фильтрации и технологии обработки трафика на базе DCI
30. http://xserver.a-real.ru/support/useful/tipy-kontent-filtrov.php
31. http://compress.ru/article.aspx?id=17262 *Александр Прохоров* «Приличный» Интернет в школе и дома
32. http://www.anti-malware.ru/parental_control_test_2012
33. http://www.ixbt.com/soft/kinder-gate.shtml Защита детей от угроз Интернета с помощью «KinderGate Родительский Контроль»

Приложение А

Существующие системы фильтрации контента

Таблица А.1 – Существующие средства фильтрации контента

№	Сервис Интернет			Служба локальной сети			ПО клиентского хоста			Платное	Название	Ссылка
	Поисковая система	DNS	Сервис фильтрации	DNS	Proxy	Межсетевой экран	Настройки сети ОС	ПО хоста	Веб -клиент			
1	+										Google Search Engine for Kids	www.safesearchkids.com/
2	+										KidRex	www.kidrex.org/
3	+								+		Google	www.google.com
4	+								+		Bing	www.bing.com/account/general
5	+								+		Yahoo!	Yahoo.com/
6	+								+		Lycos	search.lycos.com/
7	+								+		Яндекс	yandex.com/support/search/beware/adult-filter.xml
8	+										KINDER.RU	kinder.ru/
9	+										Quintura для детей	kids.quintura.ru/
10	+										Agakids	www.agakids.ru/
11	+								+		YouTube	www.youtube.com
12		+				+	+				Rejector	http://rejector.ru адреса DNS серверов: – 95.154.128.32 – 78.46.36.8
13		+				+	+			+	SkyDNS	www.skydns.ru/ адрес DNS сервера: 193.58.251.251
14		+				+	+				Яндекс.DNS	адреса DNS серверов: – 77.88.8.7 – 77.88.8.3

Продолжение таблицы А.1

15		+		+		+	+			+ -	Open DNS	www.opendns.com/ адреса DNS серверов: – 208.67.222.222 – 208.67.220.220
16		+					+			+	SafeDNS	www.safedns.com/ адреса DNS серверов: – 195.46.39.39 – 195.46.39.40
17			+								Blocksi Manager	www.blocksi.net/ chromebook-filtering.php
18			+								Mobicip	www.mobicip.com/
19			+								Cloudacl WebFilter	www.cloudacl.com/api/
20			+					+		+	Norton Online Family	onlinefamily.norton.com /familysafety/loginStart.fs
21			-		-						SurfProtect	http://www.surfprotect.co.uk/
22						+		+		+	Kaspersky Internet Security	www.kaspersky.ua/multi-device-security
23								+		+	Dr.Web Security Space	products.drweb.ru/box/ss/
24						+		+		+	McAfee Parental Controls	Для дома: home.mcafee.com/?CID=MFEru-ruMHP001 Бизнес-решения: www.mcafee.com/ru/business-home.aspx?view=legacy&CID=MFEru-ruMHP002
25					+	+				+	Интернет Контроль Сервер	xserver.a-real.ru/
26						+				+	NetPolice UNIX	www.netpolice.ru/
27								+		+	NetPolice Pro Windows	www.netpolice.ru/
28								+		+	NetPolice Linux	www.netpolice.ru/
29								+		+	KinderGate	www.kindergate-parental-control.com/ru
30			Cloudacl						+		Плагин WebFilter Pro Chrome FireFox	ww.cloudacl.com/webfilter/
31			Cloudacl						+		Плагин Anti-Porn Pro Chrome FireFox	http://www.cloudacl.com/antiporn/
32									+	+ -	Плагин FoxFilter Chrome FireFox	http://inspiredeffect.com/FoxFilter/
33									+		Плагин Parental Control App	parentalcontrol-app.com
34									+		Плагин tinyFilter Chrome	https://github.com/hpaolini/tinyFilter-chrome/wiki
35			Blocksi						+		Плагин Blocksi Web Filter Chrome FireFox Opera	http://www.blocksi.net/
36									+		Плагин BlockSite Chrome	http://www.wips.com/support/block-site-extension

Окончание таблицы А.1

37			good.media						+		Плагин good.media Chrome Opera	http://good.media/ru/roditelskij_kontrol
38									+		Плагин Adult Blocker Chrome FireFox Opera	adult-blocker.com
39			metacert						+		Плагин Parental Controls & Web Filter from metacert.com Chrome FireFox	https://metacert.com/
40									+		Плагин StopItKids parental control Chrome FireFox MS IE	http://stopitkids.com/
41					+						rejik.ru	rejik.ru/
42					+						Dansguardian	dansguardian.org/
43								+		+	Kindergate	www.kindergate-parental-control.com/ru
44			+							+	UserGate Web Filter	www.entensys.com/ru/products
45					+	+					TrafficInspector	www.smart-soft.ru/ru/products/ Traffic-Inspector/
46					+						Nginx	nginx.org/ru/
47	+				+	+					Ideco	ideco.ru/
48					+						HandyCache	handycache.ru/
49				+							ORF	www.orf-filter.ru/
50						+					CS MIMEsweeper for Web	www.clearswift.com/products/msw/web.aspx
51						+					SurfControl Web Filter	www.surfcontrol.ru/web_filter.shtml
52								+			KidsWatch	www.kidswatch.com
53								+			CyberPatrol	www.cyberpatrol.com/
54								+		+	ContentProtect Pro	www.contentwatch.com/
56								+			Net Nanny	www.netnanny.com
57								+		+	ProblemPoker	www.problempoker.com/
58					+					+	SafeSquid	www.safesquid.com/content-filtering/downloads
59					+						squidGuard	www.squidguard.org/
60								+		+	ChildWebGuardian PRO	www.childwebguardian.ru/purchase/index.html
61								+		+	X3watch	x3watch.com/
62								+			Интернет Администратор для Дома	www.iadmin.ru/products/
63								+		+	Norton Family Premier	onlinefamily.norton.com/familysafety/basicpremium.fs
64					+					+	Wingate	www.wingate.com/

Таблица А.2 – Плагины Веб-клиента их описание и классификация

№	Название	Служба	Тип архитектуры: L, NC, ND	Контроль времени работы: TC, TNC	Объект фильтрации: SHF, HRF, KWF, TCF	Способ фильтрации: MLF, ALF, FT	Фильтрация шифрованных данных: HSS, NHS	Тип реакции: BS, RS	Цена	Описание
1	2	3	4	5	6	7	8	9	10	11
29	WebFilter Pro	Cloudacl WebFilter	ND	TNC	HRF KWF TCF	ALF	HSS	RS	-	Плагин браузера для фильтрации веб контента.
30	Anti-Porn Pro	Cloudacl WebFilter	ND	TNC	HRF KWF TCF	ALF	HSS	RS	-	Плагин браузера для фильтрации порно
31	FoxFilter		L	TNC	KWF TCF	MLF	HSS	BS	-/	Персональный контент-фильтр, позволяющий блокировать порно и др. нежелательный веб контент. Все опции - бесплатны. Premium опції - за небольшую плату.
32	Parental Control App ("PC app")		L	TNC	HRF KWF TCF	MLF	HSS	BS	-	Бесплатный плагин для безопасной работы в Интернет. Дает отчет активности на email. Блокирует нежелательные сайты. Возможность конфигурирования по категориям мониторинга.
33	tinyFilter		L	TNC	KWF TCF	FT	HSS	BS	-	Использует предопределенные правила для фильтрации различных веб-сайтов. Обеспечивает фильтр ненормативной лексики, маскируя слова, которые могут быть оскорбительными для пользователя.

Продолжение таблицы А.2

1	2	3	4	5	6	7	8	9	10	11
34	Blocksi Web Filter	Blocksi	L	TC	HRF KWF TCF	MLF ALF FT	HSS	RS	-	Плагин фильтрации веб-контента и URL. Выбирает для блокирования: -79 категорий Web страниц; -создает черне и белые URL –списки; -создает и конфигурирует списки, содержащие слова или их шаблоны; - категоризация и фильтрация Youtube – видео; -контроль по времени суток; -защита настроек паролем;
35	BlockSite		L	TNC	SHF	FT	HSS	RS	-	Расширение, которое блокирует сайты по выбраному шаблону гиперссылки. Отключает гиперссылки на этих сайтах и показывает текст ссылки.
36	Website Blocker		L	TC	TCF	FT	HSS	BS	-	Позволяет блокировать URL, включающий заданую пользователем подстроку. Позволяет выполнять блокирование в определенное время дня
37	Adult Blocker (Родительский контроль)		L	TC	KWF TCF	MLF FT	HSS	BS	-	морфологический анализ веб-страниц на наличие "плохих" слов и словосочетаний. Реализована функция «черных» и «белых» списков настроек фильтрации. - блокировка страниц с нежелательной информацией; - отключение плагина на определенное время; - защита паролем; - вывод количества заблокированных запросов;

Окончание таблицы А.2

1	2	3	4	5	6	7	8	9	10	11
38	Parental Controls & Web Filter from metacert.com	metacert	L	TC	HRF KWF TCF	MLF ALF	HSS	RS	-	Защита по 20 категориям. Режимы фильтра: **Сильный для детей** - Настройки для 20 наиболее важных категорий **Для взрослых** **Для самых маленьких детей** Выбор настройки "Just for Kids" блокирует все кроме рекомендованх експертами MetaCert для детей до 12 лет. родитель может добавлять разрешенные сайты.
39	StopItKids parental control	stopitkids.com	L	TC	HRF KWF	ALF	HSS	RS	-	Позволяет блокировать и разблокировать сайт, веб-страницу или браузер дистанционно в режиме реального времени Управлять количеством времени работы в Интернет Вести отчетность и контролировать: - по списоку посещенных вебсайтов -получать сообщения о просмотре запрещенных веб - сайтов. - отправлять сообщения в браузер с напоминанием - создавать ежедневный отчет о посещенных веб-сайтах. Работодатели могут следить за работой в сети сотрудников.

Таблица А.3 – Безопасные поисковые системы их описание и классификация

№	Поисковая система	тип архитектуры: L, NC, ND	контроль времени работы: TC, TNC	объект фильтрации: SHF, HRF, KWF, TCF	способ фильтрации: MLF, ALF, FT	фильтрация шифрованных данных: HSS, NHS	тип реакции: BS, RS	Цена	Описание
1	2	3	4	5	6	7	8	9	10
3	Google	NC	TNC	HRF KWF	ALF	HSS	BS	-	Функция безопасного поиска: – регистрация пользователя в Google – включение настройки безопасного поиска в браузере
1	Google Search Engine for Kids	NC	TNC	HRF	ALF	HSS	BS	-	Безопасная поисковая система для детей и родителей. Позволяет: Информирование родителей про: - возможности организации безопасного доступа для ПК и мобильных устройств; - мерах безопасности использования детьми социальных сетей; - обеспечение безопасности мобильных устройств; - противодействие кибер- запугиванию Использовать каталог интернет ресурсов , интересных для детей Осуществлять: - безопасный поиск по веб сайтам; – безопасный поиск фотографий в Интернет; – безопасный поиск видео Пользоваться Википедией для детей

Продолжение таблицы А.3

2	KidRex	NC	TNC	HRF	ALF	HSS	BS	-	Сайт KidRex предоставляет: - детям: безопасную поисковую систему; - родителям: советы по безопасности и форму для отправки данных о запрещенных страницах. Поисковая система KidRex использует: - API Google Custom Search технологии Google Safe Search фильтрации сайтов, использующих проверки по ключевым словам, фразам и URL-адресам. - собственную базу данных нежелательных веб-сайтов на основе белых, черных списков и ключевых слов.
5	Yahoo!	NC	TNC	HRF	ALF	HSS	BS	-	Поисковая система, реализующая функцию безопасного поиска: – регистрация пользователя в Yahoo! – включение настройки безопасного поиска в браузере Yahoo SafeSearch позволяет: - заблокировать содержание для взрослых в результатах поиска. - изменять для каждого браузера и устройства пользователя свой состав фильтров - защитить настройки паролем.
6	Lycos	NC	TNC	HRF	ALF	HSS	BS	-	Lycos SearchGuard (LycosZone) - поисковая система, реализующая функцию безопасного поиска. Требует включение настройки безопасного поиска в браузере

Продолжение таблицы А.3

4	Bing	NC	TNC	HRF	ALF	HSS	BS	-	Поисковая система, реализующая функцию безопасного поиска: – регистрация пользователя в Bing – включение настройки безопасного поиска в браузере. Предоставляет 4 уровня безопасности: - безопасный поиск: не показывать в результатах поиска содержимое для взрослых. - строгий: отфильтровывать текст, изображения и видео в результатах поиска. - умеренный: отфильтровывать только изображения и видео (но не текст) в результатах поиска. - отключен: не фильтровывать содержимое для взрослых в результатах поиска.
14	Яндекс	NC	TNC	HRF	ALF	HSS	BS	-	Поисковая система, реализующая функцию безопасного поиска: Регистрация в Яндекс и включение настройки «Семейный поиск» в браузере Предоставляет 3 уровня безопасности: - семейный поиск - умеренный фильтр - без ограничений
8	KINDER.RU	NC	TNC	HRF	ALF	HSS	RS	-	Каталог Детских ресурсов (>2000 ссылок): - каждая зарегистрированная страница имеет краткую характеристику. - ведется рейтинг популярности; - осуществляет мониторинг ресурсов. - содержит разделы новостей, интерактивные игры, конкурсы, книга друзей, детский чат, - форум для детей и их родителей. Недостатки: - не имеет механизмов поиска вне зарегистрированных на нем ресурсов. - проблема актуальности ссылок на зарегистрированные ресурсы.

Окончание таблицы А.3

1	2	3	4	5	6	7	8	9	10
9	Quintura для детей	NC	TNC	HRF	ALF	HSS	RS	-	Безопасная визуальная поисковая система для детей младших или средних классов школы. Реализует концепцию «Увидеть и Найти» — визуально находить в Рунете документы на русском языке и картинки с учетом морфологии русского языка. Предоставляет возможность разработчикам подключить поисковик на веб странице сайта.
10	Agakids	NC	TNC	HRF	ALF	HSS	RS	-	Безопасная поисковая система для детей и родителей. На Agakids индексируются: - сайты с детской и около-детской тематики - сайты помощи родителям по вопросам здоровья, психологии и учёбы детей. Данные проходит проверку модераторами.
11	YouTube	NC	TNC	HRF	ALF	HSS	RS	-	Видеосервис, предоставляющий функцию поиска хранимых видеофайлов. Настройка Безопасный поиск в сеансе пользователя похожа на функцию родительского контроля: при включении из результатов запроса удаляется контент, нежелательный для детей и членов семьи. Недостаток: не защищен паролем

Таблица А.4 – Интернет службы фильтрации их описание и классификация

№	Название	тип архитектуры: L, NC, ND	контроль времени работы: TC, TNC	объект фильтрации: SHF, HRF, KWF, TCF	способ фильтрации: MLF, ALF, FT	фильтрация шифрованных данных: HSS, NHS	тип реакции: BS, RS	Цена	Описание
1	2	3	4	5	6	7	8	9	10
17	Blocksi Manager	NC	TC	HRF KWF TCF	ALF MLF	HSS	BS	$20/польз/год	Облачное приложение, реализующее интернет – фильтрацию. Осужествляет фильтрацию сайтов по протоколам HTTP и HTTPS. Предоставляет пользователю: - безопасный поиск - блокирование нежелательных изображений. - возможнсть для пользователя создавать фильтры по URL, категориям YouTube, белым и черным списков пользователя - централизованный контроль за временем доступа ребенка к сети и статистика посещенных ресурсов. - централизованный контроль за рабочей средой защищаемого устройства - централизованный контроль руководителя за использованием рабочего времени сотрудниками Blocksi Manager интегрировано с приложениями Google: Gmail, Drive, Docs и Sheets Blocksi Manager бесплатно при использовании плагина для браузеров Chrome, FireFox, Opera

Продолжение таблицы А.4

20	Norton Online Family	NC	TC	KWF TCF	ALF	HSS	BS	- /1240 руб./год	Интернет – приложение, реализующее: - контроль Интернет - ресурсов - контроль использования социальных сетей - контроль результатов поиска - защиту личной информации пользователя - контроль за временем использования компьютера - оповещения о нарушениях по эл. почте - запрос доступа к родителю на разблокирование ресурса Позволяет отслеживать информацию о действиях детей в Интернете с мобильных устройств и управлять настройками фильтрации. **Версия Premier(платная) дополнительно:** - контроль просмотра видео (YouTube) - контроль местоположения мобильного устройства - контроль мобильных приложений - контроль SMS-сообщений - журнал действий пользователя - ежемесячные и еженедельные отчеты - контроль времени использования устройства для Android)
18	Mobicip	NC	TC	HRF KWF	ALF	HSS	BS	- / $40 / 5 устр / год	2 уровня сервиса фильтрации: BASIC (бесплатно) - предустановленные уровни фильтрации - расширенная фильтрация контента PREMIUM (платная - до 5 устройств) То же, что в BASIC, а также: - онлайн управление пользователями и устройcnвами - пользовательские фильтры контента - запрос на доступ к веб-ресурсам - мониторинг за приложениями - просмотр отчетов посещенных страниц - ограничение времени работы в сети

Продолжение таблицы А.4

19	Cloudacl WebFilter & AntiPorn	NC	TNC	HRF KWF	ALF	HSS	BS	-	защита по категориям: - порно-сайты и сайты для взрослых - употребление наркотиков - блокирование сайтов онлайн игр - сайты или блоги о насилии или оружии - социальные сети, в том числе facebook и twitter. - сайты с шпионскими программами и вирусами - сайты анонимных прокси для обхода родительского контроля - сайты спама Для использования сервиса предлагаются: - Safe Browser - безопасный браузер для мобильных устройств - плагины WebFilter и AntiPorn для браузеров
47	Ideco СКИФ	NC	TNC	SHF HRF KWF TCF	MLF ALF FT	HSS	BS	800 руб/ год/чел	Высокоскоростная фильтрация трафика в сетях с пропускной способностью до 10 Гбит/сек. При этом возможны: - URL-фильтрация с использованием облачной базы данных Ideco Cloud WebFilter – больше 140 категорий сайтов -DNS-фильтрация по облачной базе данных, разбитых на 50 категорий. -выполнение морфологического анализа веб-страниц по словарю с категориями. - блокировка загрузки файлов по расширениям и MIME-типам. - фильтрация поисковых запросов с возможностью принудительного включения безопасного поиска на поисковых машинах. - фильтрация HTTP и HTTPS-трафика. - фильтрация распространяющих вирусы, фишинговых и потенциально опасных сайтов. - блокировка IP, сетей, протоколов с помощью встроенного брандмауэра.

Окончание таблицы А.4

21	SurfProtect	ND	TNC	HRF KWF TCF	MLF ALF	HSS	BS	/ Для провайдеров Интернет - £500/ год.	- решение, фильтрующее контент при перехвате веб-страницы до попадания в сеть пользователя. - возможность классифицировать сайты с помощьювеб-интерфейса пользователя. - фильтрация по категориям посредством базы данных категорий SurfProtect. - возможность для руководителя быстро блокировать или разрешить фильтрацию в категории согласно политике организации. - перенос фильтрации на устройство (BYOD): вне зависимости от вида подключения пользователь получит к Интернет безопасный доступ. - возможность родителя измененить политики фильтрации при любых условий подключенни к Интернет - фильтрация протоколаHTTPS - установка разных профилей фильтрации для разных компьютеров основе их IP-адресов. Эти профили управляются через единый веб-интерфейс. - отдельные сайты могут быть разблокированы руководителем. - использование ресурсов YouTube для образования - использование индивидуальных фильтров пользователей сети с серверами Active Directory - разрешение посещать конкретные страницы сайта при запрет на посещение других его страниц. Условие использования - настройка в браузере, прокси – сервере или брандмауере на прокси - службу SurfProtect Бесплатное использование службы - включено во все продукты и сервисы EXA.

Таблица А.5 – DNS–серверы фильтрации их описание и классификация

№	Название	тип архитектуры: L, NC, ND	контроль времени работы: TC, TNC	объект фильтрации: SHF, HRF, KWF, TCF	способ фильтрации: MLF, ALF, FT	фильтрация шифрованных данных: HSS, NHS	Тип реакции: BS, RS	Цена	Описание
1	2	3	4	5	6	7	8	9	10
12	Rejector	NC	NC	KWF TCF	ALF	HSS	RS	-	DNS-служба фильтрации. Реализует: - блокирование по категориям веб-ресурсов; - ведение списки доступа пользователя; - ведение статистики запросов; - защиту от атак и вирусов; - работу с динамическими IP - адресами; - настраиваемую страницу запрета - защиту настроек паролем
13	SkyDNS	ND	TNC	KWF	ALF	HSS	BS	Домашний: 395 руб/год Корпоративный: 300 - 360 руб/год	Облачная DNS-служба, осуществляющая фильтрацию. Настраивается на клиентском компьютере, домашнем маршрутизаторе или шлюзе ЛС

Продолжение таблицы А.5

1	2	3	4	5	6	7	8	9	10
14	Яндекс.DNS	NC	TNC	TCF	ALF	HSS	BS	-	Бесплатный рекурсивный DNS-сервис родительского контроля и безопасного интернет для домашнего пользователя. Сервера Яндекс.DNS находятся в России, странах СНГ и Западной Европе. Обеспечивает высокую скорость выполнения запросов. Для IPv4 существуют 3 группы серверов: Базовая - 77.88.8.8, 77.88.8.1 Безопасная - 77.88.8.88, 77.88.8.2 Семейная - 77.88.8.7, 77.88.8.3 Базовая - не предусмотрена фильтрация трафика. Безопасная - обеспечивается защита от заражённых и мошеннических сайтов. Семейная - включает защиту от опасных сайтов и блокировку сайтов для взрослых. Алгоритмы Яндекса определяют эротический и порнографический контент в проиндексированных страницах. При этом выполняется: - анализ текста и изображений в документе, ссылочное окружение. - данные обновляются 2-3 раза в неделю. - в Семейном режиме блокируется реклама эротического и порнографического характера на всех сайтах, а объявления и баннеры не загружаются. Для домашних роутеров Asus, D-Link, TP-Link и ZyXEL выпущены версии прошивки с интегрированными адресами Яндекс.DNS. Для каждого устройства в домашней сети или сети школы можно выбрать свою группу Яндекс.DNS.

Окончание таблицы А.5

1	2	3	4	5	6	7	8	9	10
15	Open DNS	NC	TNC	TCF KWF	MLF ALF	HSS	BS	- / $19.95/год	Бесплатная для некоммерческого применения и домашней сети быстрая служба DNS. Реализована в 3 вариантах.: OPENDNS FAMILY SHIELD (бесплатно) Реализует: - защиту от мошенничества и фишинга - родительский контроль, для всех устройств в доме. - настроен на блокирование контента для взрослых OPENDNS HOME (бесплатно) - то же, что и в FAMILY SHIELD - настраиваемые пользователем категории фильтрации и безопасности OPENDNS VIP HOME - $19.95/year - то же, что и в OPENDNS HOME - статистику работы в Интернет: детальные данные о сайтах, посещаемых в домашней сети - доступ клиентам к службе піддержки
16	SafeDNS	NC	TNC	TCF KWF	ALF FT	HSS	BS	$16-9/год	Сервис DNS фильтрации для Windows, Linux и MacOS на ПК, нетбуках, iOS и Android планшетах и смартфонах В 4 разделах: - незаконная деятельность - сайты для взрослых - занимающие полосу пропускания - сайты общей тематики сгруппированы фильтры по 56 категориям. Реализованы режимы фильтрации: - использование только белых списков - блокирование неизвестных сайтов - усиленный безопасный поиск

Таблица А.6 – DNS- и SMTP-серверы локальной сети предприятия их описание и классификация

№	Название	Тип архитектуры: L, NC, ND	Контроль времени работы: TC, TNC	Объект фильтрации: SHF, HRF, KWF, TCF	Способ фильтрации: MLF, ALF, FT	Фильтрация шифрованных данных: HSS, NHS	Тип реакции: BS, RS	Цена	Описание
15	Open DNS	NC	TNC	SHF KWF	MLF FT	HSS	BS	$28/usr/year	Сервер фильтрации для DNS и ISP серверов. (Windows 2008 R2 Server, Windows Server 2012)
48	ORF	NC	TNC	SHF TCF	MLF FT	HSS	BS	$11/usr	ORF Fusion - эффективный спам фильтр для Microsoft IIS SMTP сервиса и Microsoft Exchange сервера.

Таблица А.7 – Интернет – шлюзы локальной сети их описание и классификация

№	Название	Тип архитектуры: L, NC, ND	Контроль времени работы: TC, TNC	Объект фильтрации: SHF, HRF, KWF, TCF	Способ фильтрации: MLF, ALF, FT	Фильтрация шифрованных данных: HSS, NHS	Тип реакции: BS, RS	Цена	Описание
24	Интернет Контроль Сервер	NC DS	TNC	HRF KWF	MLF ALF FT	HSS	BS	618 руб/ польз	Комплексное решение для локальной сети предприятия, включающее: - маршрутизатор с поддержкой NAT - управление DMZ-сетью - фаервол с прокси-сервером - защиту сети и ограничение доступа, в том числе: - различные типы авторизации пользователей, - фильтрация https трафика, - контентная фильтрация с помощью службы SkyDNS, - антивирус для трафика - собственный контент-фильтр) - средства учёта трафика - почтовый сервер - Jabber-сервер (ICQ) - сервер IP-телефонии - DNS-сервер с поддержкой SkyDNS, OpenDNS и GoogleDNS - файловый сервер с разграничением прав доступа - Веб-сервер - OwnCloud - система организации хранения, синхронизации и обмена данными, размещёнными на внешних серверах Реализован для ОС: FreeBSD 9.3

Продолжение таблицы А.7

1	2	3	4	5	6	7	8	9	10
25	NetPolice UNIX	NC	TNC	KWF	MLF FT	NHS	BS	480 руб/ год	NetPolice UNIX – версия программы NetPolice для операционных систем AltLinux, Ubuntu Linux (32 и 64 бит), FreeBSD 8.X и 9.X (32 и 64 бит). Предназначен для использования в локальных сетях компаний, компьютерных классах школ и т.п. Реализует эффективную систему контентной фильтрации различной производительности.
44	TrafficInspector	NC	TNC	SHF KWF TCF	MLF FT	HSS	BS	500 руб /польз	Комплексное решение ЛС предприятия: - шлюз доступа в Интернет. - NAT, - прокси-сервер, VPN, AD сервер. - сертифицированнаую защиту сети. - межсетевой экран, - антивирус. - средства контроля интернет-трафика. - средства мониторинга и статистики доступа. - средства блокировки сайтов, контентная и URL-фильтрация. - правила фиьтрации по типам, группам и категориям. - средства блокирования баннеров и кэширование. - средства управления скоростью интернет-доступа. Динамический шейпер, распределение загрузки канала, приоритеты использования канала, - средства настройки и управления маршрутизацией, - средство Advanced Routing. Сертифицированная биллинговая система. Подсчет, лимиты, автоматизация.- Почтовый шлюз с реализацией антиспама и антивируса для почты.- средства удаленного администрирования с использованием консоли и доступом через веб-интерфейс сервера.

Окончание таблицы А.7

47	Ideco	NC	TNC	SHF KWF TCF	MLF FT	HSS	BS	645 руб /комп	Комплексное решение для локальной сети предприятия, включающее средствазащиты пользователей и корпоративной сети от внешних угроз: - система предотвращения вторжений, - контентная фильтрация веб-трафика (включая HTTPS-трафик), - антивирус и антиспам Касперского, - модуль DLP, - межсетевой экран. - почтовый сервер с многоуровневой фильтрацией спама, защитой от вирусов и фишинговых ссылок, возможностью фильтрации в качестве релея, управляемый через веб-интерфейс. - средста безопасного подключения удаленных пользователей филиалов через VPN с использованием PPTP, OpenVPN, IPsec и ГОСТ-шифрования - использование нескольких подключений к провайдерам и маршрутизація - интеграция с Active Directory.
49	CS MIMEsweeper for Web	NC	TNC	SHF TCF	MLF FT	NHS	BS	По заказу	Средство контроля и разграничения доступа к Web CS MIMEsweeper for Web — обеспечивает защиту от утечки конфиденциальных материалов через бесплатные Интернет-сервисы — Web-почту, чаты и доски объявлений. Эта программа защищает от: - распространения вирусов через Web-ресурсы - потери конфиденциальной информации - запрещенного серфінга по Интернет-сайтам - нецелевых скачиваний файлов - помещения нелегальной информации на внешние Web-ресурсы.

Таблица А.8 – Прокси-серверы локальной сети их описание и классификация

№	Название	Тип архитектуры: L, NC, ND	Контроль времени работы: TC, TNC	Объект фильтрации: SHF, HRF, KWF, TCF	Способ фильтрации: MLF, ALF, FT	Фильтрация шифрованных данных: HSS, NHS	Тип реакции: BS, RS	Цена	Описание
1	2	3	4	5	6	7	8	9	10
25	Интернет Контроль Сервер	NC DS	TNC	HRF KWF	MLF ALF FT	HSS	BS	618 руб/ польз	Описан в разделе Шлюзы локальной сети
41	rejik	NC	TNC	KWF	MLF	NHS	BS	-	Прокси сервер SQUID Позволяет: - блокирование рекламы, порно-сайтов, видео и.т.д. Предоставляет: - обновляемые списки блокировок (бан-листы) - редиректор - инструкции по установке и настройке.
42	Dansguardian	NC	TNC	SHF TCF	MLF FT	NHS	BS	-	Служба фильтром веб-контента с открытым исходным кодом и в настоящее время работает на Linux, FreeBSD, OpenBSD, NetBSD, Mac OS X, HP-UX, Solaris. Реализует - фильтрацию содержания страниц на основании совпадение фраз, - фильтрацию изображений - фильтрацию URL. Позволяет адаптировать фильтрацию от строгой до полностью разрешающей. Настройки по умолчанию ориентированы на требования начальной школы.
45	TrafficInspector	NC	TNC	SHF KWF TCF	MLF FT	HSS	BS	500 руб /польз	Описан в разделе Шлюзы локальной сети

Продолжение таблицы А.8

46	Nginx	NC	TNC	SHF	MLF	HSS	BS	-	HTTP-сервер и обратный прокси-сервер, почтовый прокси-сервер, а также TCP прокси-сервер общего назначения
47	Ideco	NC	TNC	SHF KWF TCF	MLF FT	HSS	BS	645 руб/комп	Описан в разделе Шлюзы локальной сети
48	HandyCache	L NC	TNC	KWF TCF	MLF FT	NHS	BS	- / 246 грн. (коммерч. или более 5 польз.)	Прокси-сервер для локальной сети дома, учебного заведения или предприятия. - может работать на компьютере пользователя. - позволяет писать расширения на языке lua, расширяющие поведение прокси в соответствии с требованиями пользователя.
58	SafeSquid	NC	TNC	SHF KWF TCF	MLF FT	NHS	BS	$15/ подкл/год / $10-$8	Веб-шлюз для серверов на основе x86_64 архитектуры для ОС Linux или Windows. **SafeSquid SWG** - для любого провайдера облачных услуг может быть создан в облаке безопасный веб-шлюз предприятия. - позволяет полностью контролировать фильтрацию контента Веб 2.0-приложений. **SafeSquid Composite Edition,** многопоточная архитектура, обеспечивает: - высокую пропускную способность фильтрации и -высококачественный контент-анализ веб-страниц - безопасность данных. - интеллектуальный кэш DNS-службы, - управляемую систему кэш-контента - предвыборку для быстрого просмотра часто посещаемых веб-сайтов. - создание неограниченное числа Политик фильтрации в зависимости от пользователя сети, веб-сайта, MIME-типа, раз мера, времени. - проверку подлинности пользователей удаленными серверами Windows ADS или / OpenLDAP. - создание и анализ отчетов активности пользователей.

Окончание таблицы А.7

59	squidGuard	NC	TC	SHF KWF TCF	MLF FT	NHS	RS	-	Плагин для проки-сервера Squid, соединяющий фильтрацию контента, переадресацию и контроль доступа к ресурсам Интернет. Не являясь специализированным фильтром или блокатором порно и баннеров, хорошо подходит для этих целей при соответствующей настройке. Позволяет: - ограничить доступ для отдельных пользователей тоько к списку разрешенных веб-серверов и URL-адресов. - блокировать доступ к черному списоку веб-серверов и URL-адресов для отдельных пользователей. - блокировать доступ к URL, соответствующих списоку регулярных выражений или слов. - обеспечить использование domainnames, запретив IP-адреса в URL. - перенаправить заблокированные адреса к «умной» информационной странице. - перенаправить незарегистрированного пользователя в регистрационной форме. - разные правила доступа в зависимости от времени суток, дня недели, дата и т.д. - разные правила для разных групп пользователей.
64	Wingate	NC	TNC	SHF KWF TCF	MLF FT	HSS	BS	$15/польз + $30 /польз/ год - Kaspersky + $15 /польз/ год - PureSight + $24 /польз/год - Wingate VPN	Прокси-сервер многих протоколов, включая HTTPS, сервер электронной почты и система управления интернет-шлюза для ОС Windows. Реализует: - сканирование трафика на наличие вредоносных программ с использованием антивируса Kaspersky Labs - классификацию веб-контента посредством плагина PureSight. - управление администратором политики доступа в зависимости от типа сайта. - простое и гибкое решение VPN – сети для удаленных офисов и рабочих мест используя плагин Wingate VPN .

Таблица А.9 – Антивирусные программы, включающие средства ограничения доступа к нецелевому контенту для клиентских, серверных и мобильных устройств их описание и классификация

№	Название	Тип архитектуры: L, NC, ND	Контроль времени работы: TC, TNC	Объект фильтрации: SHF, HRF, KWF, TCF	Способ фильтрации: MLF, ALF, FT	Фильтрация шифрованных данных: HSS, NHS	Тип реакции: BS, RS	Цена	Описание
21	Kaspersky Internet Security для всех устройств 2016	L	TNC	HRF	ALF	HSS	BS	980 грн./ год/ 2 устр	Антивирусная программа, реализующая защиту ПК или мобильного устройства. Реализует: - оптимальный набор защитных функций - безопасность и защиту денежных средств в Интернет - защиту детей в Интернете - конфиденциальность данных пользователя и защиту общения детей
22	Dr.Web Security Space	L ND	TNC	HRF TCF	ALF	HSS	BS	1290 руб. 1ПК + 1моб.устр./ 1 год	Комплексная защита ПК под управлением Windows.Реализует: - защиту в режиме онлайн. - защиту данных от повреждения. - детектирование и нейтрализация сложных вирусов. - проверка «на лету» трафика по всем портам. - безопасный интернет-серфинг в поисковых системах Google, Yandex, Yahoo!, Bing, Rambler активацией в поисковиках функции «Безопасный поиск» - фильтрацию трафика в мгновенных сообщениях. - эффективную защиту детей от нежелательного контента. Использует облачный сервис Dr.Web Cloud — проверяющий URL на серверах компании «Доктор Веб».

Продолжение таблицы А.9

23	McAfee Internet Security	L	TNC	HRF TCF	ALF FT	HSS	BS	1899 руб./год	Антивирусная программа и управление данными для всех устройств. Реализует: - защиту от вирусов и интернет-угроз - защиту от рискованных веб-сайтов и предотвращает загрузку опасных файлов - защиту от попадания нежелательной почты в почтовый ящик - комплексную защиту мобильных устройств
62	Norton Family Premier	L	TC	SHF HRF TCF	ALF FT	HSS	BS	1240 руб. /год	Антивирусная программа, защиту ПК или мобильного устройства. Функции: **Контроль использования Интернет** – информирунт о посещенных сайтах и предоставляет средства избежать неприемлемого содержимого. **Контроль социальных сетей** - анализ использования социальных сетей: частоту подключения, данные профилей. **Контроль поиска** – поисковые слова, словосочетания и фразы **Защита личной информации** - помогает избежать случайной публикации данных **Контроль за временем использования компьютера** **Оповещения по эл. почте** о попытках посещения заблокированных сайтов. **Мобильное приложение для родителей** - контроль действий детей. **Контроль просмотра видео** - журнал просмотра видеоматериалов YouTube и Hulu **Контроль мобильных приложений** - список загруженных Android приложений **Контроль SMS-сообщений** **Ежемесячные и еженедельные отчеты** **Контроль за временем использования устройства Android**

Таблица А.10 – Программы блокирования доступа к нецелевому контенту их описание и классификация

№	Название	Тип архитектуры: L, NC, ND	Контроль времени работы: TC, TNC	Объект фильтрации: SHF, HRF, KWF, TCF	Способ фильтрации: MLF, ALF, FT	Фильтрация шифрованных данных: HSS, NHS	Тип реакции: BS, RS	Цена	Описание
27, 28	NetPolice Pro (Windows), NetPolice Linux	L	TC	SHF HRF TCF	MLF ALF FT	HSS	BS	480 руб/ лиц/год, 400 руб/ лиц/год	Программа фильтрации и блокирования доступа к нецелевому контенту. URL-фильтрация и динамическая фильтрация (анализ содержимого страниц). Функциональные возможности фильтра - категории фильтрации; -блокирование сервисов обмена сообщениями -гибкая настройка блокировки загрузки файлов (Видео, Аудио, Архивы, Торрент-файлы, Программы) Функции работы фильтра: -предустановленные профили фильтрации - создание профилей пользователя -установка активации профиля по времени -скрытый режим работы -журнал подключения к сайтам -доступ к настройкам по единому паролю -отмена блокировки ресурса на определённый промежуток времени (30 мин., 1 час) -настраиваемая страница блокировки с возможностью переадресации на определенный пользователем адрес -управление локальными и доменными пользователями -информационные отчеты (удаленные, итоговые, детализированные) -еженедельные отчеты на адрес электронной почты

Продолжение таблицы А.10

1	2	3	4	5	6	7	8	9	10
29	KinderGate Родительский Контроль	L ND	TNC	SHF KWF TCF	MLF ALF FT	HSS	BS	490 руб/ год	Программа фильтрации и блокирования доступа к нецелевому контенту. Реализует: -блокировку опасных сайтов -контентную фильтрацию по технологии DCI - блокировку, используя черные и белые списки -блокировку контекстной рекламы -контроль загрузки файлов -безопасный поиск -фильтрацию HTTPS-трафика -поддреживает кластеризацию ОС -статистику блокированных ресурсов Версии для MAC OS 10.7.5, ALT LINUX/UBUNTU, Windows 8.1/8/7/Vista/XP
52	KidsWatch	L	TC	SHF KWF TCF	MLF ALF FT	HSS	BS	15 дней безплатно $ 49,95.	Программа фильтрации нецелевому контенту, обеспечивающая управление временем доступа и блокирование интернет с помощью таких ключевых функций: – ограничение доступ ва Интернет и использования ПК на основе настраиваемого графика доступа и ограничений по времени. -ограничение обмена мгновенными сообщениями по расписанию. -автоматизированный фильтр порно, незаконных, вульгарных и других нежелательных веб-сайтов. - вожможность создания родителями белого и черного списков Веб-ресурсов. - блокирование неуместных баннеров на веб-страницах. -автоматическое уведомление по электронной почте при появлении запрещенных слов или фраз в чате.

Продолжение таблицы А.10

56	Net Nanny							$30 / год	Программа фильтрации Реализует: - защиту от порнографии на компьютере. - маскировку ненормативной лексики до появленияя на экране. - управление ограниченем времени использования Интернет. -отправку уведомления и отчеты в окно программы или на адрес электронной почты. - создание профилей пользователей для адаптации потребностей защиты для отдельных членов семьи. Версии для Windows, Mac, Android, IPhone, IPod Touch, и IPad
53	CyberPatrol	L	TC	SHF KWF TCF	MLF ALF FT	HSS	BS	$40 / год / 3 комп	Программа фильтрации. Реализует: - 3 профиля (дети, подростки и взрослые) -ивидуальные уровни фильтрации -блокирование веб-сайтов, их содержания и изображений -черный список сайтов, обновляемый при каждом подключении -блокирование программ для взрослых -контроль за использованием игр, чата и социальных приложений -блокирование загрузки опасных данных -управление временем онлайн-доступа -управление как Интернет так и использованием приложений - отчеты о посещенных веб-страницах, времени и продолжительности просмотра -просмотр и хранение ежедневных или еженедельных сводок -блокирование слов и фраз ненормативной лексики -ограничение доступа к сайтам Facebook и YouTube -интеграция с учетными записями пользователей на XP, Vista и Windows 7

Окончание таблицы А.10

1	2	3	4	5	6	7	8	9	10
54	ContentProtect Pro	L	TC	SHF KWF TCF	MLF ALF FT	HSS	BS	$40	Программа фильтрации и нецелевого контента для ПК Политика использования Интернет применяется к, подключенным и отключен от сети устройствам Включает: -возможность веб-администрирования и отчетность о обращении к нецелевому контенту -инструменты пользовательских правил и контроля времени использования Интернет -уведомления по электронной почте о нарушения политик и запросов изменения фильтров -индивидуальные для каждого пользователя параметры политик и правил

Приложение Б
Вопросы для определения класса пользователя

I. *Новичок*:

1. Что такое веб-браузер?
   А. Устройство обеспечения работы сети Интернет
   Б. **Программное обеспечение для просмотра содержимого веб-страниц**
   В. Центральный элемент обеспечивающий работу компьютера
2. Процессор это?
   А. Центральный элемент сети Интернет
   Б. **Центральный элемент обеспечивающий работу компьютера**
   В. Системный блок компьютера
3. Для отправки электронной почты используют:
   А. Google Chrome
   Б. **Gmail**
   В. Google Drive
4. Ресурсы в сети Интернет размещаются на:
   А. **Сервере**
   Б. Маршрутизаторе
   В. Коммутаторе
5. Google Chrome это -
   А. почтовый клиент
   Б. антивирусная программа
   В. **веб-браузер**

II. *Пользователь*:

1. Для защиты от внешних угроз (атак) используют?
   А. Антивирус
   Б. **брандмауер**
   В. диспетчер задач
2. Для просмотра запущенных на компьютере процессов используют:
   А. **диспетчер задач/монитор процессов**
   Б. командную строку
   В. системный реестр
3. Для осуществления видео звонка применяют:
   А. Google Chrome
   Б. Youtube
   В. **Skype**
4. Пиринговая сеть файлового обмена это:
   А. **Сетевой сервис, предоставляющий возможность пользователям обмениваться фалами на прямую без использования сервера**
   Б. Сетевой сервис, предоставляющий пользователям возможность просматривать видео в режиме реального времени
   В. Почтовая программа
5. Глобальная информационная система, созданная для обмена информацией между различными сетевыми устройствами по всему миру:
   А. **Интернет**
   Б. Skype
   В. Сайт

III. *Опытный пользователь*:

1. Для защиты ребенка от негативного влияния сети Интернет используют:
   А. Антивирусы
   Б. **Родительский контроль**
   В. Веб фильтр
2. Беспроводные сети WI-FI работают на базе стандарта:
   А. **IEEE 802.11**
   Б. 3 GPP
   В. CDMA
3. Для отправки электронной почты используют протокол:
   А. SMTP
   Б. TCP
   В. **POP3** +
4. Для идентификации процесса получателя пакета используется:
   А. MAC адрес
   Б. HTML-код
   В. **номер порта**
5. Для определения соответствия между символьным и числовым адресом ресурса используется:
   А. протокол IP
   Б. протокол FTP
   В. **протокол DNS**

IV. *Технический специалист*:

1. Технология, позволяющая создавать безопасное сетевое соединение между двумя устройствами (клиентом и сервером) в сети Интернет это:
   А. **VPN**.
   Б. Ethernet
   В. MPLS
2. Процесс проверки подлинности личности объекта это:
   А. Авторизация
   Б. **Идентификация**
   В. Аутентификация
3. Для работы протокола SSH необходимо открыть:
   А. 20 порт
   Б. 21 порт
   В. **22 порт**
4. Маршрутизацию между автономными системами сети Интернет осуществляют по протоколу:
   А. **BGP4**
   Б. OSPF
   В. IGMP
5. Для организации сервиса «Видео по запросу» необходимо обеспечить возможность передачи в сети трафика в режиме:
   А. multicast
   Б. broadcast
   В. **Unicast**

V. *Эксперт*:

1.При создании безопасного канала протокол SSL:

А. **обязательно аутентифицирует серверную сторону и опционально клиентскую;**

Б. обязательно аутентифицирует клиентскую сторону и опционально серверную;

В. обязательно аутентифицирует и клиентскую сторону и серверную сторону;

2. Перехват данных, которые передаются в сети это:

А. Фишинг

Б. Сайдджекинг

В. **Сниффинг**

3. Что не относится к информационной инфекции:

А. Троянский конь

Б. **Фальсификация данных**

В. Логическая бомба

4. Создание копии публичной сети с целью перехвата траффика пользователей и получения доступа к конфиденциальным данным это:

А. Фишинг

Б. Сниффинг

В. **Сетевая ловушка**

5. Перенаправление пользователя на другой адрес (ресурс) отличный от того, что он запросил это:

А. Фишинг

Б. Сайдджекинг

В. **Редирект**

Приложение В
Расчёт общей стоимости сети и системы фильтрации

В.1 Метод приближенного расчета стоимости монтажа локальной кабельной компьютерной сети

Методы проектирования компьютерных сетей достаточно подробно описаны в различных источниках. Несмотря на это, проектирование представляет собой сильно упрощенную модель сети, так как не представляется возможным учесть все факторы и все требования которые могут возникнуть в будущем.

Однако общие подходы к проектированию локальных компьютерных сетей все-таки могут быть сформулированы. На рис. В.1 приведена примерная последовательность этапов проектирования локальной сети.

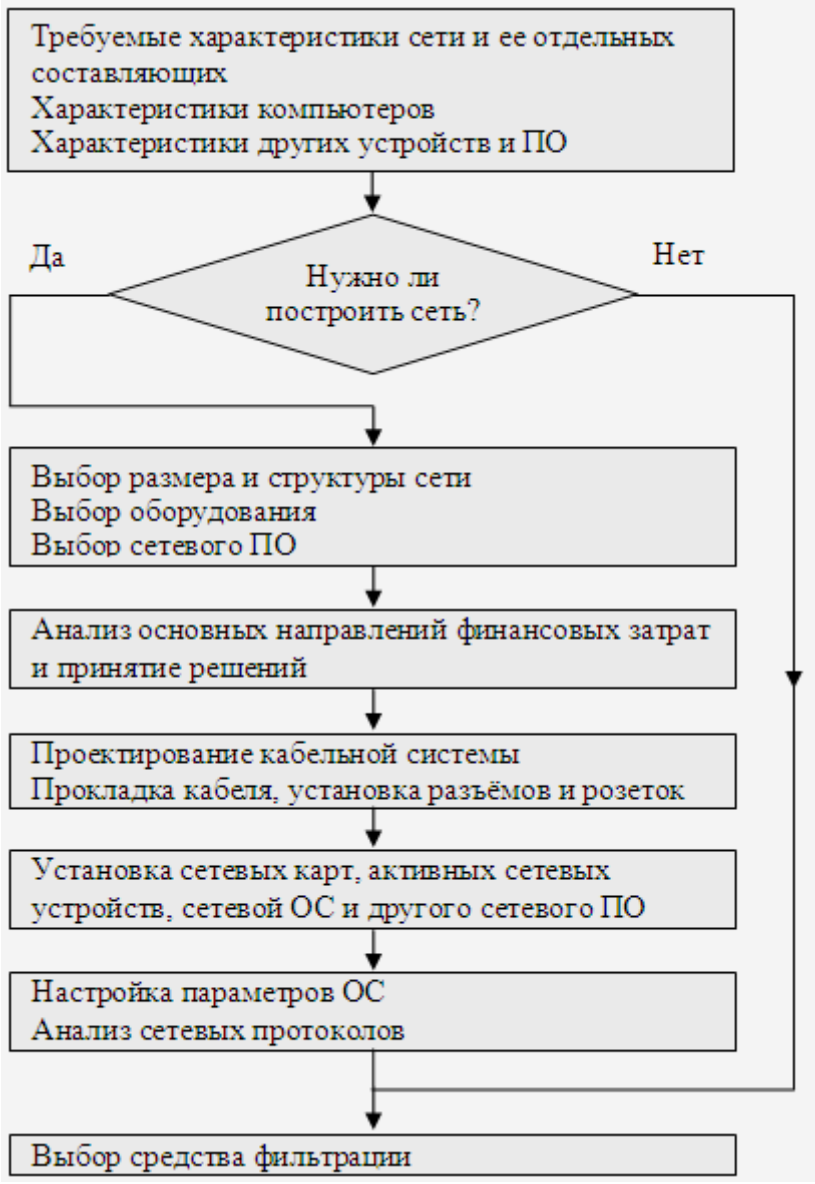

Рисунок В.1 – Этапы проектирования локальной сети

Даже в таком виде проектирование сети, с учетом того, что данные для проекта будут поступать в режиме онлайн, требует существенного упрощения. Проиллюстрируем это на примере вычисления длины кабеля.

Расчет длины кабеля при известных планировке помещений, количестве рабочих мест и их расположения выполняется по формуле

$$D_k = K_{tz} \sum_{i=1}^{K_{wp}} d_i \,, \qquad \text{(В.1)}$$

где d_i – длина сегмента кабеля; $K_{tz} = 1{,}13$ – коэффициент технологического запаса, который учитывает особенности его прокладки, а также запас для разделки кабеля.

Так как, приведенные выше данные невозможно получить в онлайн режиме воспользуемся приближенным методом вычисления D_k.

Для получения приближенных формул по расчету длины кабеля воспользуемся результатами, которые заимствованы из реальных проектов (табл. В.1)

Таблица В.1 – Данные расчетов реальных проектов кабельных систем

K_{wp}	S	K_h	K_{ir}	D_k	D_{kr}
15	60	3	1	220	42
20	80	4	1	338	57
25	80	4	1	408	59
30	85	5	2	768	65
35	100	7	2	1095	84
40	130	7	1	1117	84
45	150	8	2	1715	110
50	175	9	1	2171	126
60	190	9	2	2700	132
70	200	10	1	2088	143
80	230	11	2	4393	160
90	250	9	1	2888	151
100	400	20	2	9516	286
110	350	12	1	4476	207
120	450	14	1	10111	253

В этой таблице: K_{wp} – количество рабочих мест; S – общая площадь помещений; K_h – количество комнат; K_{ir} – количество информационных розеток на одно рабочее место; D_{kr} – длина короба.

Зададим блочную матрицу

$$\mathrm{X} = \left(\mathrm{K}_{wp} \; \mathrm{S} \; \mathrm{K}_h \; \mathrm{K}_{ir} \right), \qquad \text{(В.2)}$$

где матрицы $\mathrm{K}_{wp}, \mathrm{S}, \mathrm{K}_h, \mathrm{K}_{ir}$ – матрицы-столбцы соответствующих эмпирических значений, а $\mathrm{e} = \left(1 1 \ldots 1\right)^T$; матрицы D_k и D_{kr} – матрицы-столбцы эмпирических значений длин кабеля и короба; $\mathrm{A} = \left(a_0 \; a_1 \; a_2 \; a_3 \; a_4\right)^T$ – матрица-столбец коэффициентов множественной линейной регрессии.

Тогда, в соответствии с методом наименьших квадратов, для вычисления коэффициентов A, получим следующие матричные уравнения:

– для кабеля

$$A_k = (X^T X)^{-1} X^T D_k ; \quad \text{(В.3)}$$

–для короба

$$A_{kr} = (X^T X)^{-1} X^T D_{kr} . \quad \text{(В.4)}$$

Тогда, для расчета длины кабеля получим уравнение

$$D_k = 46{,}45S - 79{,}896K_{wp} - 18{,}77K_h + 841{,}89K_{ir} - 2412{,}8 ; \quad \text{(В.5)}$$

а для короба

$$D_{kr} = 0{,}33S + 0{,}02K_{wp} + 7{,}56K_h + 1{,}33K_{ir} - 3{,}516 . \quad \text{(В.6)}$$

Введем обозначения:

– стоимость прокладки кабеля заданной категории, за 1 м. – C_{pk} ;

– стоимость монтажа короба заданного сечения, за 1 м. – C_{mkr};

– стоимость монтажа информационной розетки, за 1 шт. – C_{mir} ;

– стоимость расшивки кросс/патч панели, за 1 порт – C_{pkp} ;

– стоимость установки и монтажа стойки/шкафа, за 1 шт. – C_{mssh};

– стоимость кабеля, за 1 м. – C_k ;

– стоимость короба, за 1 м. – C_{kr} ;

– стоимость информационной розетки, за 1 шт. – C_{ir} ;

– стоимость стойки/шкафа, за 1 шт. – C_{ssh}.

С учетом принятых обозначений стоимость монтажа ЛКС будет вычисляться по формуле

$$C_{MLKN} = C_{mk}D_k + C_{mkr}D_{kr} + C_{mir}K_{ir} + C_{pkp}K_{ir}K_{wp} + C_{mssh}K_{ssh} , \quad \text{(В.7)}$$

а стоимость материалов

$$C_{KMP} = C_k D_k + C_{kr} D_{kr} + C_{ir} K_{ir} K_{wp} + C_{ssh} K_{ssh} , \quad \text{(В.8)}$$

где K_{ssh} – количество стоек/шкафов.

Общая стоимость

$$C_{CKC} = C_{MLKN} + C_{KMP} . \quad \text{(В.9)}$$

В.2 Метод приближенного расчета стоимости монтажа или модернизации беспроводной сети

Для приближенного расчёта стоимости монтажа или модернизации беспроводной сети предположим, что помещение имеет прямоугольную форму. В таком случае для покрытия можно использовать зоны в форме квадрата. Опишем вокруг квадрата окружность с радиусом r , равным радиусу действия точки доступа, и определим характеристики квадрата.

Диагонали квадрата точкой пересечения делятся пополам и образуют на его сторонах 4 равнобедренных прямоугольных треугольника с катетами $a = b = r$. Сторона квадрата c является гипотенузой и следовательно $c = r\sqrt{2}$.

Поскольку необходимо предусмотреть возможность роуминга между зонами, обеспечим минимальное пересечение всех зон. Для этого учтём пересечение зон на величину t , указанную производителем. Тогда, сторона квадрата –

$$c = \sqrt{2}(r - t), \quad \text{(В.10)}$$

а его площадь –

$$S_c = 2(r - t)^2. \quad \text{(В.11)}$$

В результате минимально необходимое количество точек доступа N_{rou} для покрытия площади помещения прямоугольной формы вычисляется по формуле:

$$N_{rou} = \left\lceil \frac{S}{S_c} \right\rceil = \left\lceil \frac{S}{2(r - t)^2} \right\rceil. \quad \text{(В.12)}$$

Для определения длины соединительного кабеля воспользуемся приближенной формулой

$$D_{kwf} = 2(N_{rou} + 1)\sqrt{S}\ . \quad \text{(В.13)}$$

Будем считать, что длина короба $D_{kr,wf} \approx D_{kwf}$

Введем обозначения:

– стоимость монтажа точки доступа, за 1 шт. – C_{mrou};

– стоимость точки доступа, за 1 шт. – C_{rou};

Тогда общая стоимость беспроводной сети будет вычисляться по формуле:

$$C_{WIFI} = (C_{mrou} + C_{rou})N_{rou} + 2C_{pkp}N + (C_{mk} + C_{mkr})D_{krwf} + (C_k + C_{kr})D_{kwf}. \quad \text{(В.14)}$$

В.3 Выбор сетевого программного обеспечения

Выбор сетевого программного обеспечения выполняется с учетом следующих факторов:

– какой тип сети поддерживает сетевое ПО;
– максимальное количество пользователей;
– количество серверов и их типы;
– совместимость с разными операционными системами и компьютерами, а также с другими сетевыми средствами;
– уровень производительности программных средств в различных режимах работы;
– степень надежности работы, разрешенные режимы доступа и степень защиты данных;
– какие сетевые службы необходимо поддерживать;
– стоимость программного обеспечения, его эксплуатации и модернизации.

Алгоритм расчёта стоимости системы фильтрации с учётом стоимости материалов и монтажа ЛВС представлен на рис. В.2

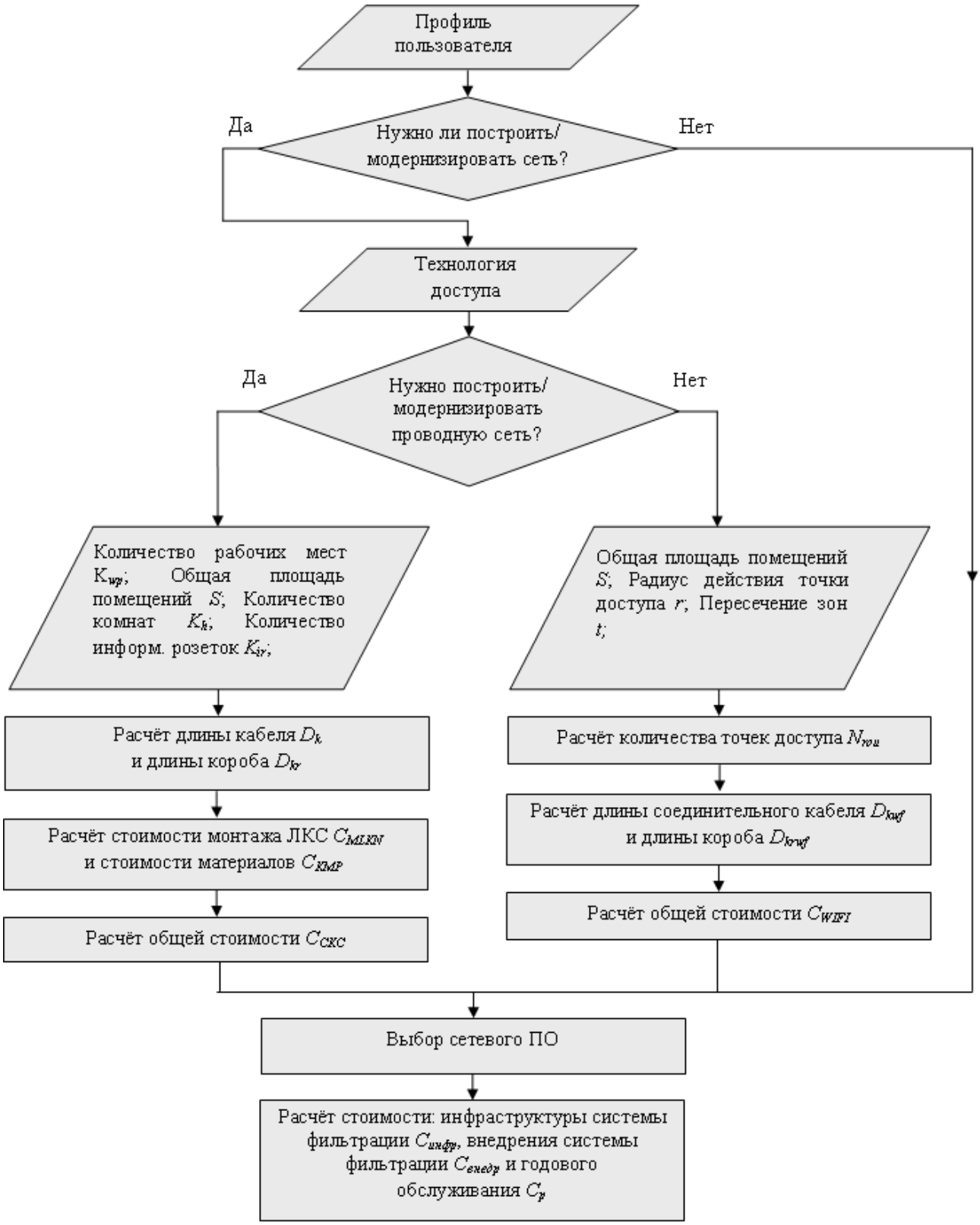

Рисунок В.2 – Расчёт стоимости системы фильтрации

Приложение Г

Инструкция по проведению экспертизы существующих технических решений фильтрации контента и наполнению единой базы данных систем фильтрации контента

Работа по эксперта по оценке существующих технических решений фильтрации контента и наполнению единой базы данных систем фильтрации контента состоит из следующих этапов. Для каждого решения необходимо:

1 проанализировать заявленное производителем описание решения и внести в базу функциональные характеристики решения, согласно детализированной классификационной модели систем фильтрации контента в сети Интернет (разд.2, рис.1):

1.1 **базовые характеристики**: *тип реализации, совместимость с операционными системами, тип операционной системы, тип сопровождения (поддержки), тип управления, тип внутренней безопасности;*

1.2 **специфические характеристики**: *тип архитектуры, возможность контроля времени работы, объект фильтрации, способ фильтрации, возможность фильтрации шифрованных данных, тип реакции (способ работы)*;

1.3 **заявленный производителем список функций, с общим количеством заявленных функций** N_{f,x_i} ;

1.4 **список и технические характеристики необходимого аппаратного обеспечения (серверов);**

1.5 **список необходимого программного обеспечения;**

2 проанализировать и внести в базу **ценовые характеристики** решения (разд.3, п.3.4): *общая стоимость лицензии, стоимость часа работы по инсталляции необходимого аппаратного и программного обеспечения, время настройки необходимого оборудования, стоимость услуг (например, командировки сотрудников) обслуживающей компании, стоимость лицензии одного пользователя, стоимость обслуживания системы, стоимость технической поддержки системы;*

3 установить и настроить решение;

4 провести, путём тестирования, экспертизу заявленного в описании функционала, посчитать **количество функций** N_{zr,x_i} **, которые в процессе тестирования дали заявленный результат**, и дать **бальную оценку функциональности** решения (разд.3, п.3.6);

5 сформировать и внести в базу бальные оценки уровня защиты и простоты использования решения (разд.3, п.3.6).

Для каждой СФК эксперту предлагается заполнить Акт обследования СФК.

АКТ

обследования СФК

1. Общие сведения:

Название СФК

Описание СФК

Разработчик СФК

Веб-сайт СФК

2. Анализ заявленного производителем описания решения

2.1 Базовые характеристики СФК*:*

Тип реализации:

☐ Программные (S)

☐ Аппаратные (H)

Совместимость с ОС:

☐ Одноплатформенные (SP)

☐ Кроссплатформенные (CP)

Тип ОС:

☐ *Windows x86*

☐ *Windowsx x64*

☐ *Unix*

☐ *Linux*

☐ *Mac OS*

☐ *Android*

☐ *iOS*

Тип сопровождения (поддержки):

☐ Полностью сопровождаемые системы (FS)

☐ Частично сопровождаемые системы (PS)

☐ Несопровождаемые системы (US)

Тип управления:

☐ Системы локального управления (LM)

☐ Системы удаленного управления (RM)

Тип внутренней безопасности:

☐ Защищенные системы (SS)

☐ Незащищенные системы (NSS).

2.2 Специфические характеристики

Тип архитектуры:

- Локальные (L)
- Сетевые (N):
  - Централизованные (NC)
  - Децентрализованные (ND).

Контроль времени работы:

- Обеспечивающие контроль времени работы в сети Интернет (TC)
- Не обеспечивающие контроль времени работы в сети Интернет (TNC)

Объект фильтрации:

- По служебным заголовкам (полям) (SHF)
- По запросам к поисковым системам (HRF)
- По ключевым словам (морфологический анализ) (KWF)
- По типу контента (TCF)

Способ фильтрации:

- по шаблонам (FT)
- по спискам (LF):
  - ручное формирование списков (MLF)
  - автоматическое формирование списков (ALF)

Фильтрация шифрованных данных:

- Позволяющие фильтровать шифрованные данные (HSS)
- Не позволяющие фильтровать шифрованные данные (NHS)

Тип реакции (способ работы):

- Блокирующие (BS)
- Перенаправляющие (RS)

2.3 Заявленный производителем список функций подлежащих оцениванию:

Название функции	**Соответствует заявленному результату (да/нет)**

3. Ценовые характеристики:

Общая стоимость лицензии, $C_{лиц}$ = _____, ден.ед. /год;

Стоимость часа работы по инсталляции необходимого аппаратного и программного обеспечения, $C_{час}$ = _____, ден.ед/ час;.

Время настройки необходимого оборудования, $T_{настр}$ = _____, часы.

Стоимость услуг (например, командировки сотрудников) обслуживающей компании, $C_{ком}$ = _____, ден.ед.;

Стоимость лицензии одного пользователя, $C_{польз.лиц}$ = _____, ден.ед. /год;

Стоимость обслуживания системы, $C_{обслсист}$ = _____, ден.ед. /год;

Стоимость технической поддержки системы, $C_{поддержс}$ = _____, ден.ед. /год.

4. Бальная оценка уровня защиты:

☐ Новичок, $B_{f_1} = 1$

☐ Пользователь, $B_{f_1} = 2$

☐ Опытный пользователь, $B_{f_1} = 3$

☐ Технический специалист, $B_{f_1} = 4$

☐ Эксперт, $B_{f_1} = 5$

5. Бальная оценка простоты использования решения:

☐ Новичок, $B_{f_1} = 5$

☐ Пользователь, $B_{f_1} = 4$

☐ Опытный пользователь, $B_{f_1} = 3$

☐ Технический специалист, $B_{f_1} = 2$

☐ Эксперт, $B_{f_1} = 1$.

В качестве примера рассмотрим экспертизу плагина Веб-клиента Adult Blocker.

АКТ

обследования СФК

1. Общие сведения:

Название СФК

Adult Blocker

Описание СФК

Плагин Веб-клиента. Сетевой фильтр, который ограничивает доступ детей и подростков к нежелательным сайтам, например, порно-сайтам и сайтам, где присутствует пропаганда насилия. Adult Blocker проводит глубокий анализ контента и фильтрует страницы по загружаемому содержимому, позволяя блокировать нецензурные выражения, обеспечивая лучшую защиту детей.

Разработчик СФК

Adult Blocker

Веб-сайт СФК

https://adult-blocker.com

2. Анализ заявленного производителем описания решения

2.1 Базовые характеристики СФК*:*

Тип реализации:

☑ Программные (S)

☐ Аппаратные (H)

(Adult Blocker реализован в виде плагина Веб-клиента – программного продукта, который устанавливается непосредственно на устройство пользователя)

Совместимость с ОС:

☐ Одноплатформенные (SP)

☑ Кроссплатформенные (CP)

(*Adult Blocker* поддерживают работу с несколькими ОС)

Тип ОС:

☑ *Windows x86*

☑ *Windowsx x64*

☐ *Unix*

☑ *Linux*

☑ *Mac OS*

☑ *Android*

☐ *iOS*

Тип сопровождения (поддержки):

☐ Полностью сопровождаемые системы (FS)

☐ Частично сопровождаемые системы (PS)

☑ Несопровождаемые системы (US)

(Централизованное обновление *Adult Blocker* не проводится)

Тип управления:

☑ Системы локального управления (LM)

☐ Системы удаленного управления (RM)

*(*управление *Adult Blocker* осуществляется «локально» изнутри защищаемого браузера*)*

Тип внутренней безопасности:

☑ Защищенные системы (SS)

☐ Незащищенные системы (NSS).

(у *Adult Blocker* настройки системы (параметры фильтрации) защищены паролем, не каждый пользователь, который имеет доступ к системе, может изменять режим ее работы)

2.2 Специфические характеристики

Тип архитектуры:

☑ Локальные (L)

☐ Сетевые (N):

- ☐ Централизованные (NC)
- ☐ Децентрализованные (ND).

(*Adult Blocker* предназначен для организации фильтрации контента только на одном устройстве (компьютер, смартфон, планшет))

Контроль времени работы:

☐ Обеспечивающие контроль времени работы в сети Интернет (TC)

☑ Не обеспечивающие контроль времени работы в сети Интернет (TNC)

(*Adult Blocker* не обеспечивает контроль времени работы в Интернет)

Объект фильтрации:

☐ По служебным заголовкам (полям) (SHF)

☐ По запросам к поисковым системам (HRF)

☑ По ключевым словам (морфологический анализ) (KWF)

☐ По типу контента (TCF)

(*Adult Blocker* осуществляет морфологический анализ веб-страниц)

Способ фильтрации:

☑ по шаблонам (FT)

☑ по спискам (LF):

- ☑ ручное формирование списков (MLF)

☐ автоматическое формирование списков (ALF)

(В *Adult Blocker* реализована функция «черных» и «белых» списков для интернет ресурсов – при внесении сайтов в данные наборы, доступ к ним блокируется/разрешается)

Фильтрация шифрованных данных:

☐ Позволяющие фильтровать шифрованные данные (HSS)

☑ Не позволяющие фильтровать шифрованные данные (NHS)

(*Adult Blocker* не позволяет фильтровать шифрованные данные)

Тип реакции (способ работы):

☑ Блокирующие (BS)

☐ Перенаправляющие (RS)

(*Adult Blocker* осуществляет блокировкуа страниц с нежелательной информацией)

2.3 Заявленный производителем список функций подлежащих оцениванию:

Название функции	**Соответствует заявленному результату (да/нет)**
1. блокировка страниц с нежелательной информацией;	**да**
2. анализ контента –морфологический анализ веб-страниц;	**да**
3. функция «черных» и «белых» списков;	**да**
4. защита настроек паролем;	**да**
5. вывод количества заблокированных запросов;	**да**
6. возможность скрыть иконку с панели;	**да**
7. отключение плагина на определенное время.	**да**

3. Ценовые характеристики:

Общая стоимость лицензии, $C_{лиц}$ = 0 грн/год

(*Adult Blocker* – свободно распространяемое ПО).

Стоимость часа работы по инсталляции необходимого аппаратного и программного обеспечения, $C_{час}$ = 50 грн / час.

(стоимость часа работы по инасталляции и настройке *Adult Blocker* – работа с данным приложеним не требует высокой квалификации).

Время настройки необходимого оборудования, $T_{настр}$ = 0.5 часа

(Время для инсталляции и настройки *Adult Blocker*).

Стоимость услуг (например, командировки сотрудников) обслуживающей компании, $C_{ком}$ = 50 грн

(Работа с данным приложеним не требует высокой квалификации – командировка в пределах населеного пункта).

Стоимость лицензии одного пользователя, $C_{польз.\ лиц}$ = 0 грн/год

(*Adult Blocker* – свободно распространяемое ПО).

Стоимость обслуживания системы, $C_{обслсист}$ = 600 грн/год;

(Обслуживания *Adult Blocker* не требует высокой квалификации и время настройки $T_{настр}$ = 0.5 часа)

Стоимость технической поддержки системы, $C_{поддерж}$ = 0 грн/год.

4. Бальная оценка уровня защиты:

☐ Новичок, $B_{f_1} = 1$

☑ Пользователь, $B_{f_1} = 2$

☐ Опытный пользователь, $B_{f_1} = 3$

☐ Технический специалист, $B_{f_1} = 4$

☐ Эксперт, $B_{f_1} = 5$

(Для обхода *Adult Blocker* достаточно воспользоваться приложением не из стандартной поставки ОС или офисного пакета, например альтернативным браузером или торрент-клиентом, отыскать без использования специальных терминов несложную инструкцию в Интернет и т.д.)

5. Бальная оценка простоты использования решения:

☐ Новичок, $B_{f_1} = 5$

☑ Пользователь, $B_{f_1} = 4$

☐ Опытный пользователь, $B_{f_1} = 3$

☐ Технический специалист, $B_{f_1} = 2$

☐ Эксперт, $B_{f_1} = 1$.

(Требуется установка, несложная настройка приложения с использованием графического интуитивно понятного интерфейса)