СОГЛАСОВАНО
Министр образования и науки
Российской Федерации

_____ Д.В. Ливанов

УТВЕРЖДАЮ
Министр связи и массовых
коммуникаций Российской Федерации

_____ Н.А. Никифоров

# РЕКОМЕНДАЦИИ
## по организации системы ограничения в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования

Москва, 2014

## ОГЛАВЛЕНИЕ

## ТЕРМИНЫ И СОКРАЩЕНИЯ

| Термин или сокращение | Описание |
|---|---|
| АС | Автоматизированная система |
| База данных категоризированных ресурсов | Специализированные справочники, либо информационные системы, содержащие информацию, разделенную на категории, о ресурсах сети Интернет, не совместимых с задачами образования. |
| Специализированные организации и внешние базы данных | Специализированные организации, в том числе зарубежные, осуществляющие функции поиска и анализа информации в сети Интернет. Внешние базы данных категоризированных Интернет-ресурсов. |
| Единый реестр | Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено. |
| Интернет-ресурс, информационный ресурс Интернет | Уникально адресуемый в сети Интернет и доступный через сеть Интернет блок информации. |
| Контент | Информация, размещенная в сети Интернет |
| Контентная фильтрация | Метод ограничения доступа к Интернет-ресурсам или услугам сети Интернет по их содержимому. Позволяет ограничить доступ к информации, размещенной в сети Интернет, определенных категорий, не предназначенных для просмотра. |
| Методические материалы | Методические и справочные материалы для реализации комплексных мер по внедрению и использованию программно-технических средств, обеспечивающих ограничение доступа обучающихся образовательных учреждений к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания. — Минобрнауки |

| | |
|---|---|
| | России, 2006 г. |
| ОО | Образовательные организации |
| Оператор Единого реестра | Организация, привлекаемая для ведения Единого реестра |
| Реестр НСОР | Реестр Не Совместимых с Образованием Ресурсов – База данных, хранящая актуальный список Интернет-ресурсов, содержащих информацию, причиняющую вред здоровью и (или) развитию детей, а также не соответствующую задачам образования |
| Оператора Реестра НСОР | Организация, привлекаемая для ведения Реестра НСОР |
| Пользователь Интернет (потребитель информации) | Физическое лицо или организация, обращающиеся к Интернет-ресурсам с целью получения информации |
| Интернет-провайдер | Оператор связи, предоставляющий услуги доступа к сети Интернет и иные связанные с Интернетом услуги |
| СКФ | Система контентной фильтрации. Система, обеспечивающая ограничение доступа пользователей Интернет к Интернет-ресурсам в соответствии с определенными правилами. |
| АСОР | Автоматизированная система Оператора Реестра НСОР |
| DPI | Deep Packet Inspection. Технология накопления статистических данных, проверки и фильтрации сетевых пакетов по их содержимому |

# 1. ВВЕДЕНИЕ

## 1.1.Постановка задачи и состав документа

Необходимо разработать комплекс организационных, нормативных и технических рекомендаций, обеспечивающих построение эффективной системы защиты детей от нежелательной информации при доступе к сети Интернет из образовательной организации в рамках образовательного процесса.

При разработке рекомендаций необходимо учесть результаты и опыт реализации единой системы контент-фильтрации доступа к сети Интернет, реализованной Министерством образования и науки Российской Федерации.

Для всесторонней проработки вопроса, необходимо в дальнейшем детализировать требования к организации ограничения доступа к информации, распространяемой посредством сети Интернет, включая:

- Перечень видов информации, структурированный по категориям, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, доступ к которой из ОО должен быть ограничен;
- Функциональные требования к системам контентной фильтрации;
- Технические требования к системам контентной фильтрации.
- Функциональные и технические требования к реализации централизованного контроля за использованием средств фильтрации сети Интернет и их взаимодействия.
- Требования к операторам связи по установке системы контентной фильтрации.

Также для выработки эффективного решения поставленной задачи необходимо учитывать общие задачи и существующие механизмы контроля распространения информации в сети Интернет, включая контроль распространения запрещенной информации и защиту детей от нежелательной информации.

В настоящем документе дается краткий обзор текущей ситуации в рамках поставленной задачи, проводится анализ существующей СКФ с соответствующими рекомендациями, и приводится вариант модернизации СКФ с учетом этих рекомендаций. Для предлагаемой реализации даны схемы и временной регламент взаимодействия основных участников.

## 1.2.Обзор текущей ситуации

Обзор текущей ситуации дан в Приложении №1 к настоящему документу, в котором описана общая постановка задачи в контексте общей ситуации с ограничением доступа к информации в Интернет, а также кратко описываются действующие практические механизмы обеспечения таких ограничений.

Следует сразу отметить, что базовые принципы организации СКФ в образовательных организациях были отражены в документе «Методические и справочные материалы для реализации комплексных мер по внедрению и использованию программно-технических средств, обеспечивающих исключение доступа обучающихся образовательных

учреждений к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания», подготовленном Минобрнауки России в 2006 году.

Основные выводы по текущей ситуации, в связи с поставленной задачей, следующие:

- Не все образовательные организации способны внедрить и поддерживать у себя локальные фильтры. Еще сложнее это делать для детей, обучающихся на дому.
- Контроль доступа к Интернет-ресурсам, содержащим информацию, запрещенную на территории Российской Федерации, обеспечивается федеральной службой по надзору в сфере связи.
- Механизм актуализации списка ограничения доступа не отвечает современным требованиям по оперативности.
- Система изолирована и не взаимодействует с внутригосударственными системами и иными организациями, и базами данных Интернет-ресурсов.
- Отсутствует описание современных технических требований к системам фильтрации, которые могли бы обеспечивать качество фильтрации контента в соответствии с действующим законодательством Российской Федерации
- Осуществление ограничения доступа описано как ограничение доступа к Интернет-ресурсам, а не информации (контенту), размещенному в сети Интернет, как этого требует Федеральный Закон Российской Федерации.
- Отсутствуют технологические инструменты адресного контроля за осуществлением фильтрации Интернет-контента при использовании сети Интернет в образовательных организациях.

На основе данных выводов разработана возможная модель развития СКФ в рамках образовательного процесса, которая отражена в Приложении №2 к настоящему документу. При разработке учитывались как результаты анализа текущей ситуации, так и существующие нормативно-правовые акты:

- Федеральный закон 436-ФЗ от 29 декабря 2010 г. «О защите детей от информации, причиняющей вред их здоровью и развитию».
- Федеральный закон 114-ФЗ от 25 июля 2002 г. "О противодействии экстремистской деятельности".
- Федеральный закон 187-ФЗ от2 июля 2013 г. «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях».
- Методические материалы.
- «Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Министерством образования и науки Российской Федерации», Минобрнауки России, 2011 г.

В разделе 2 настоящего документа описан сценарий взаимодействия основных участников в рамках организации работы СКФ, разработанный на основе предложенной модели.

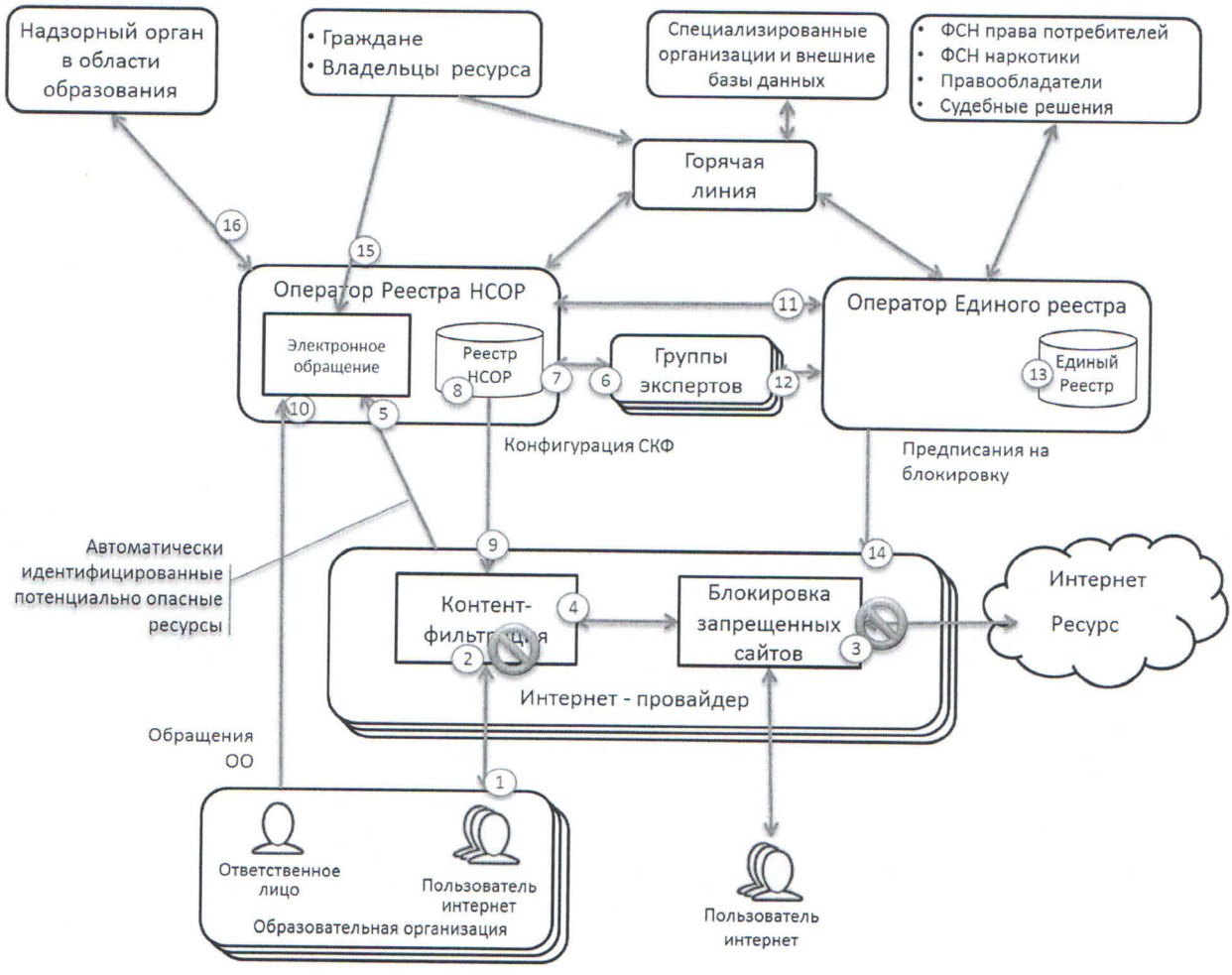
# 2. РЕГЛАМЕНТ ВЗАИМОДЕЙСТВИЯ УЧАСТНИКОВ ПРОЦЕССА ОГРАНИЧЕНИЯ ДОСТУПА УЧАЩИХСЯ К ИНТЕРНЕТ

В данном разделе дается краткое описание решения и схемы взаимодействия участников. Подробное описание дано в Приложении 2 данного документа.

## 2.1.Схема предлагаемого решения

Общая схема взаимодействия участников процесса в предлагаемом решении приведена на рисунке.

Рисунок 1. Схема процесса взаимодействия




Система обеспечивает следующие возможности ограничения доступа к информации при доступе в Интернет из ОО:

- Запрет доступа к запрещенной в России информации и информации, запрещенной к распространению среди детей;
- Запрет доступа к информации, не соответствующей задачам образования;
- Ограничение доступа к информации, не соответствующей возрастной категории учащегося, осуществляющего доступ в Интернет.

Идентификация Образовательной Организации, подключаемой к провайдеру Интернет, осуществляется по статическому внешнему IP адресу (адресам), выделенному Организации ( "белые" IP-адреса), либо путем регистрации соответствия ОО внутренним статическим IP адресам ( серые адреса) при других способах подключения.

Варианты решения для идентификации возрастной категории учащегося представлены в Приложении 2.

В Таблице 1 представлены роли участников процесса и перечислены их основные задачи:

Таблица 1. Роли и задачи участников взаимодействия

| Участник процесса | Задачи участника |
|---|---|
| Оператор Единого реестра | Задачи Оператора Единого реестра:<br>• Создание, формирование и ведение "Единого реестра» сайтов в сети Интернет, содержащих информацию, распространение которой в Российской Федерации запрещено<br>• Организация проведения экспертизы информационной продукции в целях обеспечения информационной безопасности детей;<br>• Определение порядка взаимодействия Оператора Единого реестра с Интернет-провайдерами с целью физического ограничения доступа к запрещенным Интернет-ресурсам;<br>В настоящее время данные функции выполняет Роскомнадзор. «Единый реестр» - официальное название реестра ресурсов запрещенной информации |
| Оператор Реестра НСОР | Оператор Реестра НСОР осуществляет:<br>• формирование и ведение реестра Интернет-ресурсов, содержащих информацию, запрещенную для распространения среди детей, и информацию, не совместимую с задачами образования;<br>• взаимодействие с экспертами и агрегация результатов проведения экспертиз;<br>• взаимодействие с компетентными органами государственной власти;<br>• контроль обновлений настроек систем СКФ в соответствии с Реестром НСОР;<br>• координация обработки Обращений и Нотификаций о потенциально опасных Интернет-ресурсах;<br>• осуществление приема обращений граждан и образовательных организаций по фактам обнаружения нарушений в распространении или доступе к информации в сети Интернет и координация их обработки;<br>• взаимодействие со специализированными организациями и внешними базами данных;<br>• сбор и агрегация статистики использования интернет в |

| | |
|---|---|
| | образовательных организациях;<br>• подключение СКФ Интернет-провайдеров.<br>В настоящее время централизованно данные функции не выполняются.<br>Задачи Оператора Реестра НСОР должны преимущественно осуществляться посредством автоматизированной системы, осуществляющей следующие функции:<br>• взаимодействие с системами фильтрации, используемыми для ОО;<br>• сбор статистических данных использования сети Интернет в ОО;<br>• передача на экспертизу Интернет-ресурсов, содержащих контент, не соответствующий образовательному процессу;<br>• ведение базы данных URL-адресов, содержащих контент, не соответствующий образовательному процессу;<br>• взаимодействие с внешними базами данных Интернет-ресурсов и специализированными организациями;<br>• автоматизированный прием заявлений об обнаружении Интернет-контента, не соответствующего образовательному процессу;<br>• взаимодействие с компетентными органами государственной власти. |
| Эксперты | Специалисты, обеспечивающие анализ информационных Интернет-ресурсов на соответствие требованиям законодательных и нормативных актов.<br>В настоящее время эксперты привлекаются Оператором Единого реестра для осуществления экспертизы информационных Интернет-ресурсов на предмет отнесения к запрещенным.<br>Задачи экспертов:<br>• Подготовка рекомендаций по формированию правил автоматической идентификации нежелательного контента;<br>• Осуществление экспертизы Интернет-ресурсов по запросам Оператора Реестра НСОР. |
| Автоматизированный прием сообщений | АС Оператора Реестра НСОР в автоматическом режиме обеспечивает прием заявлений граждан об обнаруженных запрещенных Интернет-ресурсах, запрещенных среди детей, несовместимых с образованием или необоснованно заблокированных Интернет-ресурсов из установленных СКФ, либо формы ручной подачи заявления.<br>В настоящее время «горячая линия» функционирует при Роскомнадзоре и принимает заявления об обнаруженных запрещенных Интернет-ресурсах. |

| | |
|---|---|
| Образовательная организация (ОО) | • Предоставление обучающимся доступа к сети Интернет;<br>• Информирование Оператора Реестра НСОР о фактах доступа обучающихся через Интернет из ОО к информации из не разрешенной для данного обучающегося категории. . |
| Интернет-провайдер | • Ввод в эксплуатацию системы СКФ;<br>• Предоставление образовательным организациям доступа в Интернет;<br>• Эксплуатация системы СКФ;<br>• Обеспечение фильтрации (блокировки) трафика в соответствии с Единым реестром;<br>• Обеспечение фильтрации (блокировки) трафика в соответствии с Реестром НСОР информации;<br>• Сбор и предоставление Оператору Реестра НСОР деперсонифицированной статистики использования образовательными организациям доступа в Интернет. |
| Специализированные организации и внешние базы данных | Базы данных Интернет-ресурсов, в том числе международные, содержащие реестры противоправного или не соответствующего целям образования контента.<br>Специализированные организации, осуществляющие поиск и анализ информации в сети Интернет, носящей противоправный или не соответствующий целям образования контент. |
| ФОИВ в области образования (на схеме не показан) | • Формирование политики использования сети Интернет в рамках образовательного процесса;<br>• Анализ результатов реализации политики. |
| Федеральная служба по надзору в области образования (на схеме не показана) | • Контроль за соблюдением требований законодательства и нормативных актов в области использования Интернет в рамках учебного процесса;<br>• Устранение выявленных нарушений. |

## 2.2.Основные сценарии ограничения доступа к Интернет

Взаимодействие участников процесса ограничения доступа обучающихся из образовательных организаций к информации в сети Интернет обеспечивает поддержку следующих основных сценариев:

1. Обращение учащегося из образовательной организации к Интернет-ресурсу, содержащему информацию, запрещенную на территории Российской Федерации;
2. Обращение учащегося из образовательной организации к Интернет-ресурсу, содержащему информацию, не совместимую с задачами образования;
3. Обращение учащегося из образовательной организации к Интернет-ресурсу, содержащему потенциально опасную информацию;
4. Обращение учащегося из образовательной организации к Интернет-ресурсу, содержащему информацию не совместимую с задачами образования, но не

включенному в Реестр НСОР и автоматически не идентифицируемому как потенциально опасному;

5. Обращение учащегося из образовательной организации к Интернет-ресурсу, содержащему информацию, запрещенную на территории Российской Федерации, но не включенному в Единый реестр и автоматически не идентифицируемому как потенциально опасному.
6. Оспаривание гражданином или владельцем Интернет-ресурса правомочности блокировки Интернет-ресурса, признанного не совместимым с задачами образования.

В таблице 2 представлено описание взаимодействия участников при реализации основных сценариев работы СКФ:

Таблица 2. Сценарии взаимодействия

| № | Участник | Действия (номер на схеме) | Результат |
|---|---|---|---|
| **1** | **Обращение учащегося из образовательной организации к Интернет-ресурсу, содержащему информацию, запрещенную на территории Российской Федерации** | | |
| 1.1 | Учащийся образовательной организации | • Обращается к ресурсу сети Интернет (1) | Запрос отправляется к Интернет-провайдеру |
| 1.2 | Интернет-провайдер | • Система СКФ проверяет адрес Интернет-ресурса по Реестру НСОР (2) | Интернет-ресурс не включен в Реестр НСОР. Запрос пропускается к Интернет-ресурсу |
| 1.3 | Интернет-провайдер | • Средства Интернет-провайдера проверяют адрес Интернет-ресурса по Единому реестру (3) | Интернет-ресурс включен в Единый реестр.<br>Доступ к Интернет-ресурсу блокируется |
| 1.4 | Интернет-провайдер | • Система СКФ регистрирует обращение к запрещенному Интернет-ресурсу и передает в АС Оператора Реестра НСОР | Обновляется статистика в АС Оператора Реестра НСОР |
| **2** | **Обращение учащегося из образовательной организации к Интернет-ресурсу, содержащему информацию, не совместимую с задачами образования** | | |
| 2.1 | Учащийся образовательной организации | • Обращается к ресурсу сети Интернет (1) | Запрос направляется к Интернет-провайдеру |
| 2.2 | Интернет-провайдер | • Система СКФ проверяет адрес Интернет-ресурса по Реестру НСОР (2) | Интернет-ресурс включен в «черный список» Реестра НСОР. Доступ к Интернет-ресурсу блокируется |
| 2.3 | Интернет-провайдер | • Система СКФ регистрирует обращение к запрещенному Интернет-ресурсу и передает в АС Оператора | Обновляется статистика в АС Оператора Реестра НСОР |

| | | | |
|---|---|---|---|
| | | Реестра НСОР | |
| **3** | **Обращение учащегося из образовательной организации к Интернет-ресурсу, содержащему потенциально опасную информацию** | | |
| 3.1 | Учащийся образовательной организации | • Обращается к ресурсу сети Интернет (1) | Запрос направляется к Интернет-провайдеру |
| 3.2 | Интернет-провайдер | • Система СКФ проверяет адрес Интернет-ресурса по Реестру НСОР (2) | Интернет-ресурс не включен в Реестр НСОР. Запрос пропускается к Интернет-ресурсу |
| 3.3. | Интернет-провайдер | • Средства Интернет-провайдера проверяют адрес Интернет-ресурса по Единому реестру (3) | Интернет-ресурс не включен в Единый реестр. Запрос пропускается к Интернет-ресурсу |
| 3.4 | Интернет-провайдер | • Система СКФ анализирует содержимое Интернет-ресурса (4) | Обнаружены признаки потенциально опасного контента.<br>Пользователю отображается предупреждение СКФ о потенциально опасном контенте. Пользователь может получить доступ к контенту или отказаться от просмотра.<br>Система СКФ передает в АС Оператора Реестра НСОР электронное Обращение об обнаружении потенциально опасного контента |
| 3.5 | Оператор Реестра НСОР | • Получает обращение от СКФ Интернет-провайдера (5)<br>• Направляет запрос эксперту на анализ Интернет-ресурса (6) | Обновляется статистика в АС Оператора Реестра НСОР.<br>Запрос в АС Оператора Реестра НСОР назначен на эксперта для рассмотрения |
| 3.6 | Эксперт | • Проводит экспертизу Интернет-ресурса<br>• Регистрирует заключение в запросе<br>• Направляет запрос Оператору Реестра НСОР (7) | Результат экспертизы фиксируется Оператором Реестра НСОР |
| 3.7 | Оператор Реестра НСОР | По результатам экспертизы:<br>• В случае контента несовместимого с задачами образования, Интернет- | В обращении регистрируется решение.<br>В «черный» список Реестра НСОР вносится адрес |

| | | | |
|---|---|---|---|
| | | ресурс включается в «черный» список Реестра НСОР (список Интернет-ресурсов, не совместимых с задачами образования (8)<br>• В случае отнесения контента к запрещенному на территории Российской Федерации, запрос перенаправляется Оператору Единого реестра(11) (Шаг 5.9). | Интернет-ресурса.<br>Обновляется статистика обработки обращений |
| 3.8 | Интернет-провайдер | • Система СКФ обновляет конфигурацию в соответствии с обновленным Реестром НСОР (9) | Новые запросы к данному Интернет-ресурсу будут блокироваться на втором шаге сценария. |
| **4** | **Обращение учащегося из образовательной организации к Интернет-ресурсу, содержащему информацию не совместимую с задачами образования, но не включенному в Реестр НСОР и автоматически не идентифицируемому как потенциально опасному** | | |
| 4.1 | Учащийся образовательной организации | • Обращается к ресурсу сети Интернет (1) | Запрос направляется к Интернет-провайдеру |
| 4.2 | Интернет-провайдер | • Система СКФ проверяет адрес Интернет-ресурса по Реестру НСОР (2) | Интернет-ресурс не включен в Реестр НСОР. Запрос пропускается к Интернет-ресурсу |
| 4.3. | Интернет-провайдер | • Средства Интернет-провайдера проверяют адрес Интернет-ресурса по Единому реестру (3) | Интернет-ресурс не включен в Единый реестр. Запрос пропускается к Интернет-ресурсу |
| 4.4 | Интернет-провайдер | • Система СКФ анализирует содержимое Интернет-ресурса (4) | Не обнаружено признаков потенциально опасного контента.<br>Учащийся образовательной организации получает доступ к Интернет-ресурсу. |
| 4.5 | Образовательная организация | • Работник ОО регистрирует получение доступа к информации, не совместимой с задачами образования<br>• Работник ОО передает информацию о Интернет-ресурсе через электронное | |

| | | | |
|---|---|---|---|
| | | обращение (10) | |
| 4.6 | Оператор Реестра НСОР | • В автоматическом порядке регистрирует обращение и отправляет на экспертизу. (6) | Обращение зарегистрировано и передано на экспертизу |
| 4.7 | Эксперт | • Проводит экспертизу Интернет-ресурса<br>• Регистрирует заключение в запросе<br>• Направляет запрос Оператору Реестра НСОР (7) | Результат экспертизы фиксируется Оператором Реестра НСОР. |
| 4.8 | Оператор Реестра НСОР | • Интернет-ресурс включается в список Интернет-ресурсов, не совместимых с задачами образования (8) | В обращении регистрируется решение<br>В Реестр НСОР вносится адрес Интернет-ресурса<br>Обновляется статистика обработки обращений в АС Оператора Реестра НСОР |
| 4.9 | Интернет-провайдер | • Система СКФ обновляет конфигурацию в соответствии с обновленным Реестром НСОР (9) | Новые запросы к данному Интернет-ресурсу будут блокироваться на втором шаге сценария |
| **5** | **Обращение учащегося из образовательной организации к Интернет-ресурсу, содержащему информацию, запрещенную на территории Российской Федерации, но не включенному в Единый реестр и автоматически не идентифицируемому как потенциально опасному** | | |
| 5.1 | Учащийся образовательной организации | • Обращается к ресурсу сети Интернет (1) | Запрос направляется к Интернет-провайдеру |
| 5.2 | Интернет-провайдер | • Система СКФ проверяет адрес Интернет-ресурса по Реестру НСОР (2) | Интернет-ресурс не включен в Реестр НСОР. Запрос пропускается к Интернет-ресурсу |
| 5.3 | Интернет-провайдер | • Средства Интернет-провайдера проверяют адрес Интернет-ресурса по Единому реестру (3) | Интернет-ресурс не включен в Единый реестр. Запрос пропускается к Интернет-ресурсу |
| 5.4 | Интернет-провайдер | • Система СКФ анализирует содержимое Интернет-ресурса (4) | Не обнаружено признаков потенциально опасного контента.<br>Учащийся образовательной организации получает доступ |

| | | | |
|---|---|---|---|
| | | | к Интернет-ресурсу |
| 5.5 | Образовательная организация | • Работник ОО регистрирует получение доступа к информации, не совместимой с задачами образования<br>• Работник ОО обращается на горячую линию | |
| 5.6 | Горячая линия | • Специалист горячей линии регистрирует Обращение (или обращение регистрируется автоматически в зависимости от канала) | Обращение зарегистрировано |
| 5.7 | Горячая линия | • Специалист горячей линии проверяет данные Обращения и классифицирует его | Данные из Обращения подтверждаются.<br>Обращение относится к информации, запрещенной на территории Российской Федерации |
| 5.8 | Горячая линия | • Специалист горячей линии направляет обращение Оператору Единого реестра | Обращение передано Оператору Единого реестра.<br>Статистика обработки обращений обновлена |
| 5.9 | Оператор Единого реестра (вне процесса ограничения доступа учащихся в Интернет) | • Направляет запрос эксперту на анализ Интернет-ресурса (12)<br>• В случае положительного заключения эксперта Интернет-ресурс включается в Единый реестр (13)<br>• Интернет-провайдеру, предоставляющему подключение Интернет-ресурса направляется предписание о блокировке Интернет-ресурса (14)<br>• Интернет-провайдер блокирует Интернет-ресурс. | Новые запросы к данному Интернет-ресурсу будут блокироваться на третьем шаге сценария |
| **6** | **Оспаривание гражданином или владельцем Интернет-ресурса правомочности блокировки Интернет-ресурса, признанного не совместимым с задачами образования** | | |
| 6.1 | Гражданин или владелец Интернет- | • Регистрирует Электронное обращение (15) | Система формирует Запрос эксперту |

| | | | |
|---|---|---|---|
| | ресурса | | |
| 6.2 | Эксперт | • Проводит экспертизу Интернет-ресурса<br>• Регистрирует заключение в запросе<br>• Направляет запрос Оператору Реестра НСОР (7) | Оператор Реестра НСОР получает заключение эксперта |
| 6.3 | Оператор Реестра НСОР | • Если решение эксперта положительное, то принимается решение об исключении Интернет-ресурса из реестра несовместимых с образованием. (8) | Решение регистрируется в обращении<br>Из «черного списка» Реестра НСОР исключается Интернет-ресурс<br>Далее шаг 6.5 |
| 6.4 | Оператор Реестра НСОР | • Если решение эксперта отрицательное, то Реестр НСОР остается без изменений | Решение регистрируется в обращении.<br>Обработка завершается.<br>Гражданин или владелец Интернет-ресурса может подать письменную жалобу Оператору Реестра НСОР, которая будет рассмотрена в порядке, устанавливаемом надзорным органном в области образования. (16) |
| 6.5 | Интернет-провайдер | • Система СКФ обновляет конфигурацию в соответствии с обновленным Реестром НСОР (9) | Новые запросы к данному Интернет-ресурсу не будут блокироваться на втором шаге сценария |

# 3. ПРИЛОЖЕНИЕ №1 АНАЛИЗ СУЩЕСТВУЮЩЕГО ОПЫТА И ДЕЙСТВУЮЩИХ НПА

## 3.1.Предпосылки проведения работ

С целью организации работы по ограничению доступа обучающихся образовательных учреждений к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования, Министерством образования и науки Российской Федерации в 2006 году были разработаны базовые принципы организации работы систем контентной фильтрации доступа к сети Интернет в образовательных организациях, которые легли в основу документа «Методические и справочные материалы для реализации комплексных мер по внедрению и использованию программно-технических средств обеспечивающих ограничение доступа обучающихся образовательных учреждений к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания».

Вместе с этим Минобрнауки России разработало единую систему контент-фильтрации доступа к сети Интернет и «Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Министерством образования и науки Российской Федерации.

Однако, в настоящее время задача ограничения доступа обучающихся ОО к ресурсам сети Интернет в полной мере не решена.

В этой связи можно выделить следующий ряд причин:

- не все ОО имеют возможность обеспечить приобретение, настройку и эксплуатацию персональных контентных фильтров. Еще сложнее это сделать для детей, обучающихся на дому;
- отсутствуют технологические инструменты адресного контроля за осуществлением фильтрации Интернет-контента при использовании сети Интернет в ОО;
- СКФ изолирована и не взаимодействует с внутригосударственными системами и иными организациями, и базами данных Интернет-ресурсов;
- отсутствует описание современных технических требований к СКФ, которые могли бы обеспечивать качество фильтрации контента в соответствии с действующим законодательством Российской Федерации;
- порядок актуализации Перечня категорий Интернет-контента, не совместимого с задачами образования обучающихся, доступ к которому для ОО должен быть ограничен, разработанного Минобрнауки России, не отвечает современным требованиям по оперативности реагирования на изменения, происходящие в сети Интернет (далее – Перечень категорий Интернет-контента);
- контроль за ограничением доступа к Интернет-ресурсам, содержащим информацию, запрещенную на территории Российской Федерации, обеспечивается Федеральной службой по надзору в сфере связи (в соответствие со ст.15.1 и 15.2 Федерального закона № 149-ФЗ).

Вместе с этим в связи с вступлением в силу Федеральных законов № 436-ФЗ, № 139-ФЗ и № 187-ФЗ Минобрнауки России необходимо провести работу по актуализации Перечня видов информации, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, структурированной по категориям. При этом предусматривается его последующая доработка, например, в случае изменения законодательства Российской Федерации.

Учитывая изложенное, для решения поставленной задачи необходимо разработать комплекс организационных, нормативных и технических рекомендаций, обеспечивающих построение эффективной системы защиты детей от нежелательной информации (контента), размещенной в сети Интернет, носящей противоправный или несоответствующий целям обучения учащихся ОО характер (далее – Рекомендации).

При разработке Рекомендаций также следует учесть опыт функционирования единой системы контент-фильтрации доступа к сети Интернет, реализованной Министерством образования и науки Российской Федерации.

Для всесторонней проработки указанного вопроса, необходимо в дальнейшем детализировать требования к организации ограничения доступа к информации (контенту), размещенной в сети Интернет, носящей противоправный или несоответствующий целям обучения учащихся ОО характер, а именно:

- функциональные и технические требования к СКФ;
- унифицированные требования к операторам связи (Интернет-провайдерам) по обеспечению организации работы СКФ;
- функциональные и технические требования к реализации централизованного ведения реестра информации, носящей противоправный или несоответствующий целям обучения учащихся ОО характер;

## 3.2.Система контентной фильтрации Минобрнауки России

Базовые принципы организации СКФ в ОО, изложенные в Методических материалах, закрепляют следующие основные принципы:

- Минобрнауки России формирует рекомендации по организации системы ограничения доступа к сети Интернет в образовательных организациях в виде набора методических материалов, образцов нормативных документов и Классификатора информации (перечня Интернет-ресурсов, доступ к которым должен быть закрыт). При этом на региональном и муниципальном уровнях материалы и Классификатор могут быть доработаны с учетом особенностей региона и учебных заведений в муниципальном образовании;
- Классификация информации осуществляется, как правило, специальными экспертно-консультативными органами (советами) при органах управления образованием разных уровней;
- Классификатор информации состоит из двух разделов: 1) классификатор информации, запрещенной законодательством Российской Федерации к распространению. Данный классификатор обязателен к применению без изменений; 2) Классификатор информации, не имеющей отношения к образовательному процессу может состоять из общей части, применяемой без изменений на всей территории Российской Федерации, и части, рекомендуемой к использованию в данном регионе или муниципальном образовании;
- Образовательные организации являются уровнем практической реализации мероприятий по ограничению доступа учащихся к Интернет-ресурсам, не имеющим отношения к образовательному процессу. При этом основанием для внедрения соответствующих программно-технических средств является утверждение образовательными организациями правил использования сети Интернет, имеющих статус локальных правовых актов;
- Политика доступа в Интернет определяется образовательной организацией самостоятельно. При этом образовательная организация должна руководствоваться:

- законодательством Российской Федерации;
- специальными познаниями, в том числе полученными в результате профессиональной деятельности по рассматриваемой тематике;
- интересами обучающихся, целями образовательного процесса;
- рекомендациями профильных органов и организаций в сфере классификации ресурсов сети Интернет;
- образовательная организация несет ответственность за невыполнение функций в рамках своей компетенции;

- Техническое ограничение доступа пользователей к нежелательной информации (фильтрация) осуществляется непосредственно на клиентских рабочих местах, для чего используются специальные программные решения фильтрации, рекомендованные Минобрнауки России;
- Информация об обнаруженных информационных Интернет-ресурсах передается на специальную «горячую линию»

Достоинствами реализованной системы ограничения доступа к информации являются:

- Самостоятельность образовательных организаций в формировании политики доступа в Интернет. Данный подход позволяет максимально полно (в рамках образовательной организации) реализовывать принцип права и конечной ответственности родителей за защиту детей от нежелательной информации;
- Установка СКФ на конечные пользовательские компьютеры обеспечивает максимальную простоту развертывания: не требуется создания, внедрения и поддержки централизованных систем и инфраструктуры, не требуется дополнительного оборудования в школах;
- Данная система позволяет легко реализовать дифференцированный доступ учащихся к информации в зависимости от их возрастной категории, так как идентификация пользователя и применение политик доступа в Интернет осуществляются непосредственно на рабочем месте пользователя.
- Относительная простота всего комплекса мер, что упрощает внедрение.

Среди недостатков следует отметить:

- Создание многоуровневой системы экспертно-консультативных советов представляется избыточным. Результат работы каждого из этих уровней носит рекомендательный характер, при том, что окончательное решение принимается в образовательной организации. При этом доступ образовательных организаций к квалифицированным экспертам не описан, поэтому реализовать в полной мере свои права на определение политики доступа организации не в состоянии;
- Предоставление возможности учесть региональные особенности при формировании политики доступа к сетевым ресурсам требует экспертизы. Данный механизм может оказывать деструктивное влияние на целостность федерации. При этом наличие таких региональных особенностей, которые могут отразиться в различиях политики доступа детей к информации, не очевидно;
- Не определено, какие именно изменения могут быть внесены в Классификатор информации на каждом уровне. Ужесточение политики на нижних уровнях не является проблемой, но ослабление политики представляет собой проблему администрирования и контроля;

- Не описана схема обновления Классификатора информации на региональном уровне. Процедура обратной связи построена на обобщении опыта образовательных организаций на муниципальном и региональном уровнях, при этом не закладываются средства автоматизации. Такой механизм не отвечает требованиям оперативного реагирования на вновь возникающие угрозы;
- Система не рассматривает наличие иных государственных механизмов контроля доступа к сетевым ресурсам. Поэтому, ограничение доступа к Интернет-ресурсам, запрещенным на территории России, должно осуществляться наряду с Интернет-ресурсами, закрытыми для детей. Такое дублирование фильтрации не усиливает защиту, а только снижает скорость доступа в сеть за счет дополнительной нагрузки на СКФ. Также, такой механизм предполагает постоянное обновление Классификатора Минобрнауки России от Единого реестра, что увеличивает время реакции и вводит дополнительные точки взаимодействия;
- Отсутствует механизм «реабилитации» страниц, которые блокируются СКФ на основе правил автоматического анализа контента, но при этом являются легальными.
- Не предусмотрены точки интеграции системы в мировую систему контроля за распространением запрещенной информации, что снижает уровень защиты от нежелательного контента, размещенного за рубежом и увеличивает объем анализа зарубежных Интернет-ресурсов на соответствие политике, при том, что такой анализ мог быть уже сделан другими организациями.
- Ответственность образовательной организации за доступ к Интернет-контенту не соответствующего целя образования, а также за неиспользование системы контент-фильтрации при организации доступа в информационно-телекоммуникационную сеть Интернет.
- Не все образовательные организации способны внедрить и поддерживать у себя локальные фильтры. Еще сложнее это делать для детей, обучающихся на дому. Кроме того, разнообразие средств доступа в сеть Интернет и ПО, установленного на них, усложняет задачу разработки универсального локального фильтра.
- Существующие методические рекомендации не соответствуют требованиям действующего законодательства Российской Федерации в области защиты детей от информации, причиняющей вред их здоровью и духовному развитию.
- Осуществление ограничения доступа описано как ограничение доступа к Интернет-ресурсам, а не информации (контенту), размещенному в сети Интернет, как этого требует Федеральный Закон Российской Федерации.
- Отсутствуют технологические инструменты мониторинга на уровне адресов URL за результатами фильтрации Интернет-контента в образовательных организациях.

В 2011 году были утверждены «Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Министерством образования и науки Российской Федерации».

В целом, данные правила не изменяют принципов, заложенных в Методических рекомендациях 2006 года.

Исключением является предоставленная образовательным организациям возможность использовать СКФ не только рекомендованные Минобрнауки, но и приобретенные самостоятельно при соблюдении требований, которым должны соответствовать СКФ.

При этом правила подчеркивают, что СКФ должны реализовывать единую политику исключения доступа к Интернет-ресурсам для всех образовательных организаций.

Если это предполагает, что Классификатор стал единым для всех учебных заведений и не предполагает изменений классификаторов на региональном и муниципальном уровнях, то этот факт можно рассматривать как позитивный шаг к повышению эффективности системы в целом.

## 3.3.Категоризация информации

В настоящее время определены следующие категории информации, доступ к которой должен быть закрыт или ограничен при работе в сети Интернет:

- Информация, распространение которой запрещено на территории России. Виды данной информации определяются, первую очередь, законом 114-ФЗ "О противодействии экстремистской деятельности", а также рядом других законов. Сводный перечень категорий информации, запрещенных к распространению, дан в документе «Методические и справочные материалы для реализации комплексных мер по внедрению и использованию программно-технических средств, обеспечивающих исключение доступа обучающихся образовательных учреждений к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, Приложение № 8, Минобрнауки России, 2006 год»;
- Информация, являющаяся предметом интеллектуальной собственности, которая распространяется без разрешения правообладателя. Перечень такой информации определен законом 187-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях;
- Информация, запрещенная к распространению среди детей. Виды данной информации определены в законе 436-ФЗ «О защите детей от информации, причиняющей вред здоровью или развитию»;
- Информация, ограниченная к распространению среди детей определенных Возрастных категорий. Возрастные категории и перечень видов информации определяются тем же законом 436-ФЗ;
- Информация, не имеющая отношения к образовательному процессу при доступе к Интернет из образовательной организации. Сводный перечень категорий информации, не имеющих отношения к образовательному процессу, дан в том же Приложении 8 документа Методических материалов Минобрнауки России от 2006 года. При этом следует учитывать, что в настоящее время образовательные организации России не подразделяют доступ учащихся к Интернет на доступ в рамках учебного процесса и вне учебного процесса.

## 3.4.Ограничение доступа к запрещенной информации

Согласно закону ограничение доступа к информации, запрещенной к распространению на территории Российской Федерации, и незаконно распространяемой информации, являющейся интеллектуальной собственностью, должно быть обеспечено для всех граждан на всей территории Российской Федерации.

Для реализации данных законов созданы механизмы физического ограничения доступа к незаконной информации на территории Российской Федерации.

Поскольку данные механизмы единообразно применяются ко всем пользователям Интернет в Российской Федерации, то дублирование защиты от данных категорий информации в системе ограничения доступа к информации при работе в образовательной организации представляется не целесообразным. При этом задачи ограничения доступа к информации из образовательных организаций концентрируются на ограничении доступа к информации детей.

Механизмы ограничения доступа к запрещенной на территории Российской Федерации информации подробно рассмотрены в следующем разделе данного документа.

## 3.5. Ограничение доступа к информации для детей

Закон 436-ФЗ, включая последующие изменения, определяет меры по защите детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе информации, распространяемой через Интернет.

Указанный кон также определяет перечень запрещенной для детей информации, возрастные категории детей и виды информации, разрешенной для той или иной категории, а также требования к обороту информационной продукции.

Согласно закону, при предоставлении доступа к информации через Интернет в местах, доступных для детей, закон обязывает применять административные, организационные и технические меры по защите детей от запрещенной информации.

Однако данная норма не относится к операторам связи, предоставляющим доступ в интернет на основании письменных договоров, что перекладывает ответственность за выполнение норм закона на конечных потребителей: родителей, при доступе детей к интернет из дома, публичные библиотеки, владельцев публичных точек доступа к Интернет (ст. 14. часть 1 (в ред. Федерального закона от 28.07.2012 г. N 139-ФЗ)).

При этом закон никак не помогает и не стимулирует перечисленные категории пользователей Интернет применять средства защиты детей от нежелательной информации. В связи с этим представляется целесообразным обязать операторов связи предлагать своим клиентам возможности безопасного для детей доступа к Интернет, а клиентов, то есть лиц, заключающих договора доступа к Интернет с оператором связи, обязать обеспечивать защиту детей при доступе в Интернет, с использованием средств оператора связи или иными средствами.

При этом необходимо формирование технических требований к системам фильтрации, используемым для образовательных организациях Российской Федерации.

## 3.6. Ограничение доступа к информации, распространение которой запрещено

Закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» определяет механизм физического ограничения доступа к запрещенной информации в сети Интернет.

Данный механизм предусматривает создание федерального реестра сетевых адресов, доменных имен и указателей страниц, содержащих информацию, распространение которой в России запрещено. Доступ к Интернет-ресурсу, внесенному в Единый реестр, блокируется оператором связи, предоставляющим доступ к сети Интернет данному ресурсу.

Решение о включении в Единый реестр может быть принято, как в судебном порядке, при признании информации запрещенной к распространению на территории России, так и в внесудебном порядке на основании решения уполномоченных федеральных органов исполнительной власти. Внесудебный порядок может быть принят в отношении следующих видов информации:

- Материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;
- Информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений;
- Информации о способах совершения самоубийства, а также призывов к совершению самоубийства;
- Информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами.

Данный механизм, в целом, универсален и может быть применен к информации различного рода.

Перечень запрещенной информации определяется данным законом и может быть расширен дополнительными законами. В настоящее время принят один закон, расширяющий перечень запрещенной информации: Закон 114-ФЗ "О противодействии экстремистской деятельности".

Перечень информации, для которой применим внесудебный порядок, определен данным законом. Закон 187-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях" расширяет применение блокировки информационного Интернет-ресурса по решению федерального органа исполнительной власти, но в этом случае решение принимается на основании решения суда о применении обеспечительных мер.

Необходимо отметить недостатки существующей реализации данного механизма. Операторы связи без больших затрат могут реализовать блокировку по IP адресам и доменным именам. Однако при использовании таких средств заблокированными могут оказаться большое число законных Интернет-ресурсов. Точную блокировку может обеспечить блокировка по URL, однако реализация такого механизма может потребовать более существенных затрат от операторов связи. Также осуществление фильтрации по URL уменьшает скорость доступа к информации, что является негативным факторов развития интернет индустрии и экономики в целом.

Также указанный механизм не обеспечивает надежного ограничения доступа к информационным Интернет-ресурсам, размещённым за пределами Российской Федерации. Ограничение доступа к зарубежным информационным Интернет-ресурсам требует организации международного взаимодействия по вопросам борьбы с распространением запрещенной информации, а также путем введения практики фильтрации в точке подключения пользователей к сети Интернет.

Представляется целесообразным реализовать универсальный механизм блокировки информационных Интернет-ресурсов на уровне URL, обеспечивающий блокировку как входящего, так и исходящего потоков запросов, при этом обеспечивающего минимальную дополнительную задержку для легального трафика.

## 3.7.Противодействие экстремизму

Закон 114-ФЗ "О противодействии экстремистской деятельности" определяет, в частности, перечень видов экстремистской информации, распространение которой на территории России запрещено, включая и распространение через Интернет.

Информационные материалы, признанные решением суда экстремистскими, подлежат государственной регистрации и внесению в федеральный список экстремистских материалов. Материалы, признанные экстремистскими подлежат конфискации.

В случае, если для распространения экстремистской информации используется сеть Интернет, то меры, предусмотренные настоящим Федеральным законом, применяются с учетом особенностей отношений, регулируемых законодательством Российской Федерации в области связи. То есть для предотвращения распространения запрещенной информации может быть применен механизм блокировки доступа к материалам посредством федерального реестра сетевых адресов, доменных имен и указателей страниц.

Необходимо отметить, что если в решении суда не указан адрес размещения информации в сети Интернет, то механизм блокировки применен быть не может.

## 3.8.Защита интеллектуальной собственности

Закон 187-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях" определяет механизм защиты от распространения нелицензионного контента в сети Интернет. На данный момент закон распространяется исключительно на кино и видео продукцию.

Механизм предусматривает возможность блокировку Интернет-ресурса, на котором размещен нелицензионный контент, по заявлению правообладателя. Решение о блокировке принимается федеральным органом исполнительной власти, при предоставлении заявителем определения суда о принятии обеспечительных мер. При этом заявитель должен в течение установленного срока подать иск в суд о признании незаконным размещение данного материала

Блокировка осуществляется через механизм федерального реестра сетевых адресов, доменных имен и указателей страниц.

## 3.9.Зарубежный опыт борьбы с запрещенной информацией в Интернет и межгосударственного взаимодействия

На сегодняшний день большинство развитых стран мира прибегают к фильтрации интернет-контента и другим ограничениям свободы в Сети. При этом применяются различные технические решения: блокирование интернет-ресурсов по IP-адресу, искажение DNS-записей, блокирование сайтов по URL, пакетная фильтрация, фильтрация через HTTP прокси-сервер.

Следует отдельно отметить фильтрацию контента на основании возрастной маркировки ( по аналогии с видео и аудио продукцией средств массовой информации). В США и странах Евросоюза разрабатывались проекты возрастной маркировки контента в Интернет. Однако с развитием Интернета стало очевидно, что маркировка контента не решает поставленных задач.

По результатам специального исследования было указано, что контент в Интернете, в отличии от других форм контента (фильмов на CD/DVD, телепередач и видеоигр), распределен в пространстве и во времени, и не имеет единого источника. Это делает невозможным внедрение национальной или международной системы маркировки контента, поскольку сроки внедрения с учетом возможных законодательных и этических проблем делают саму систему классификации неэффективной.

Более того, исследования показали, что в большинстве случаев родители предпочитают сами делать индивидуальный выбор в отношении собственных детей. При этом часто родители не считают маркировку справедливой и подходящей для их ребенка.

В результате было принято решение отказаться от маркировки контента в интернете в странах Евросоюза.

Одной из наиболее эффективных моделей регулирования Интернета, по мнению международного сообщества, является принцип саморегулирования

В основе принципов лежат три базовых положения:

- Интернет-компании и интернет-платформы, позволяющие размещать пользовательский контент (социальные медиа), берут на себя обязательства разрабатывать и встраивать настройки безопасности, позволяющие родителям ограничить доступ ребенка к нежелательному контенту. При этом речь идет не о навязанной пользователю контентной фильтрации на уровне магистрального провайдера, а именно о пользовательских настройках безопасности, которые являются добровольным выбором пользователя и не ограничивают его права на доступ к информации;
- Интернет-компании предоставляют пользователям возможность сообщить о неприемлемом контенте и реагируют на жалобы пользователей;
- Настоящий механизм уведомления интернет-платформы пользователем основывается на четких и прозрачных правилах и политиках размещения пользовательского контента, его удаления и ограничения доступа к нему, которые разрабатываются и публикуются интернет-компаниями.

Примерами реализации саморегулирования являются специальные безопасные режимы работы поисковых систем (google), систем хостинга пользовательского контента (youtube)

Наиболее распространенным в мире инструментом сбора информации о нелегальном контенте в Интернет является организация «горячих линий» с пользователями. Работа «горячих линий» осуществляется в сотрудничестве с правоохранительными и иными государственными органами, операторами систем технического ограничения доступа к информации, общественными и образовательными организациями, экспертами.

«Горячие линии» работают, как правило, в рамках страны пребывания. В рамках Евросоюза успешно реализуется механизм борьбы с противозаконным контентом, размещенным вне страны обнаружения. Собранная информация передается в страну размещения контента по линии общественных организаций, поддерживающих «горячие линии». Такие организации объединены в единую сеть INHOPE, а операторы национальных «горячих линий» являются национальными узлами этой сети. «Сигнал» передается в страну размещения противозаконного Интернет-ресурса на национальный узел, который направляет информацию правоохранительным или иным уполномоченным органам своей страны.

Как показала практика INHOPE такой обмен информацией намного эффективнее и реализуется быстрее прямого полицейского взаимодействия.

Представляется целесообразным Оператору Реестра НСОР обеспечить взаимодействие со специализированными организациями, осуществляющими свою деятельность в сфере выявления противоправного и не соответствующего целям образования контента. Взаимодействие должно носить технический характер обмена базами данных.

## 3.10. Общественный контроль

Общественные организации принимают непосредственное участие в процессах борьбы с нежелательным контентом в большинстве западных стран. Общественным организациям делегируется самый широкий спектр функций, от сбора информации о противоправных Интернет-ресурсах и классификации Интернет-ресурсов, до контроля процессов ограничения доступа и даже непосредственно до физического управления ограничением доступа к Интернет-ресурсам.

В РФ на настоящий момент нет широкой практики привлечения общественных организаций к данным вопросам. Хотя закон предусматривает привлечение для управления Единым реестром сторонней организации, на данный момент эта функция выполняется надзорным органом.

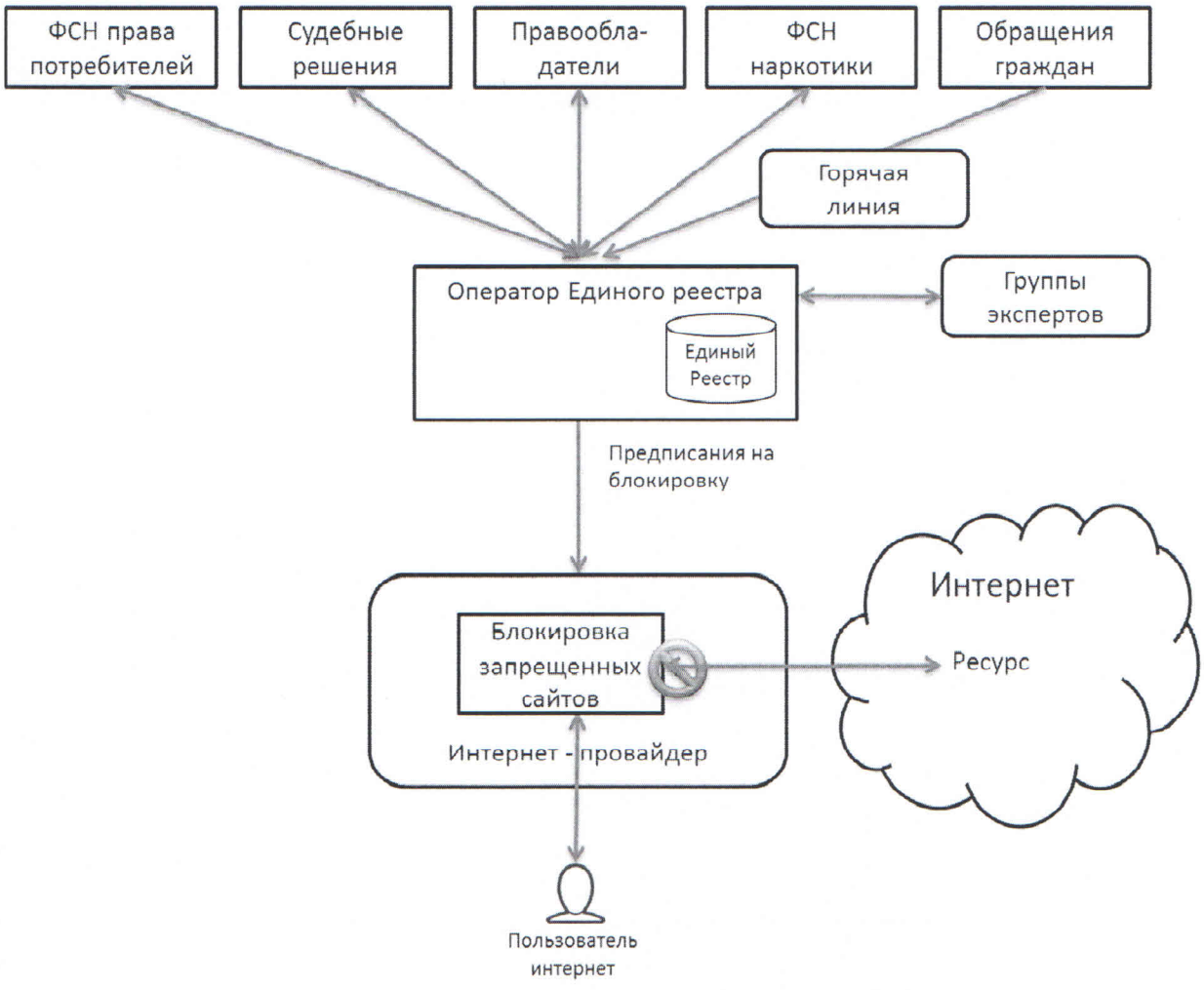
Решение должно предусматривать возможность привлечения общественности как с целью непосредственного исполнения отдельных функций, так и с целью контроля процессов.

## 3.11. Схема существующей системы ограничения доступа к информации в интернет в Российской Федерации

На диаграмме представлена существующая схема организации ограничения доступа к информации в Российской Федерации на основе принципов, изложенных в разделе выше. Государственным надзорным органом является Роскомнадзор:

Рисунок № 2. Существующая в РФ схема организации ограничения доступа к запрещенной информации в Интернет

Рисунок 2. Схема ограничения доступа к запрещенной информации в Интернет


ФСН права потребителей
Судебные решения
Правообла-датели
ФСН наркотики
Обращения граждан
Горячая линия
Оператор Единого реестра
Единый Реестр
Группы экспертов
Предписания на блокировку
Интернет
Блокировка запрещенных сайтов
Ресурс
Интернет - провайдер
Пользователь интернет

# 4. ПРИЛОЖЕНИЕ №2. ОПИСАНИЕ ВАРИАНТА РЕАЛИЗАЦИИ

## 4.1. Цели и задачи развития системы ограничения доступа к информации в Интернет

Целями предлагаемой модернизации системы являются:

- Максимальное повышение оперативности и прозрачности процесса актуализации Реестра НСОР;
- Исключение образовательных организаций из процессов установки, поддержания работоспособности и настройки контент фильтров и передача этих процессов в сферу ответственности операторов связи;
- Исключение дублирования функций системой Минобрнауки России и другими государственными механизмами ограничения доступа к информации в сети Интернет;
- Повышение эффективности работы СКФ и уровня защиты от незаконного контента, в том числе размещенного за рубежом.

Задачами модернизации системы являются:

- Максимальная автоматизация процессов обнаружения нежелательных Интернет-ресурсов, передачи на экспертизу, обновления настроек систем контент-фильтрации, повышение эффективности работы СКФ, возможность анализа результатов фильтрации Интернет-контента для использования в дальнейшем взаимодействии с образовательными организациями;
- Интеграция системы Минобрнауки России с существующими процессами и механизмами ограничения доступа к контенту в Интернет;
- Интеграция со специализированными организациями, деятельность которых направлена на выявление противоправного и несоответствующего задачам образования контента.

## 4.2. Системы контентной фильтрации

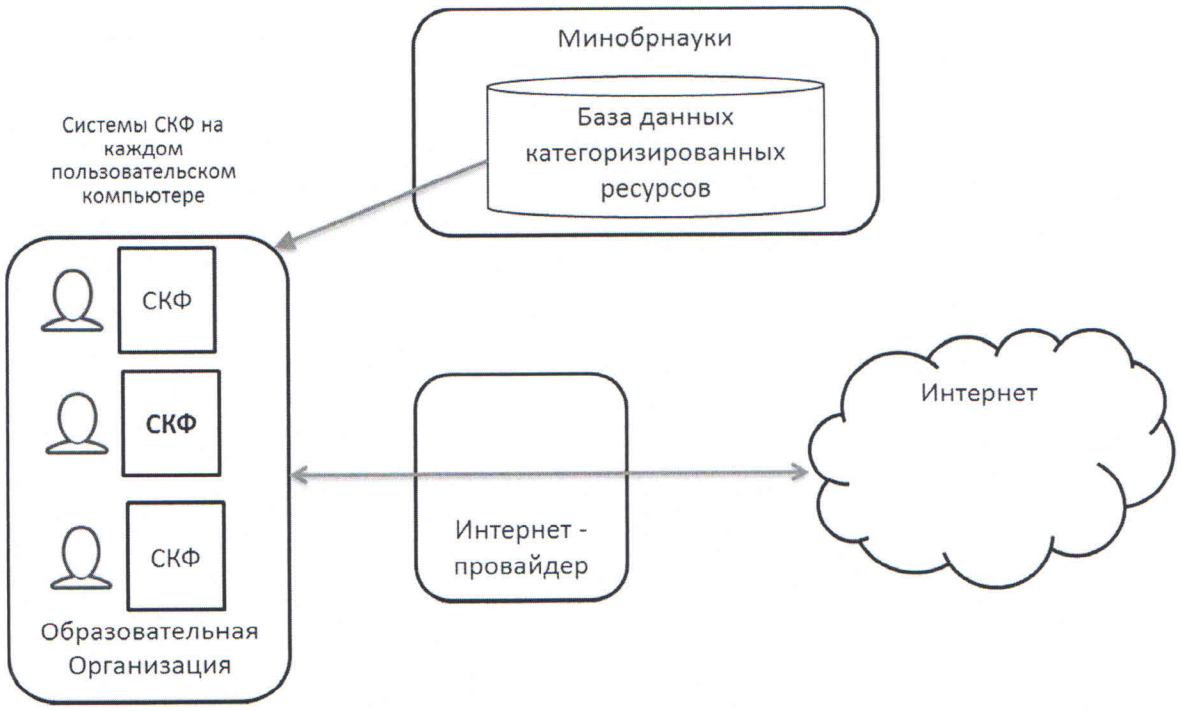
Схема размещения контентных фильтров на клиентских станциях, применяемая в существующем решении Минобрнауки России, имеет свои ограничения:

- Отсутствие в образовательной организации персонала или наличие сторонних организаций, способных обеспечить оперативную настройку систем контент-фильтрации. Наиболее актуально данное ограничение для небольших образовательных организаций и организаций в удаленных населенных пунктах;
- Большое число точек настройки. Настраивать контент-фильтр необходимо на каждом компьютере. Ограничение снимается, если контент-фильтры поддерживают массовое автоматическое обновление. Однако, в любом случае, увеличение количества настраиваемых элементов повышает сложность и снижает надежность системы в целом;
- Затруднено оперативное автоматическое обновление настроек всех СКФ на территории страны при изменениях в Классификаторе. Это связано и с качеством и скоростью каналов подключения, и с разницей часовых поясов, и режимами работы

организаций, и другими факторами. Кроме того, для автоматического обновления все типы СКФ должны поддерживать единый формат приема Базы данных категоризированных ресурсов;

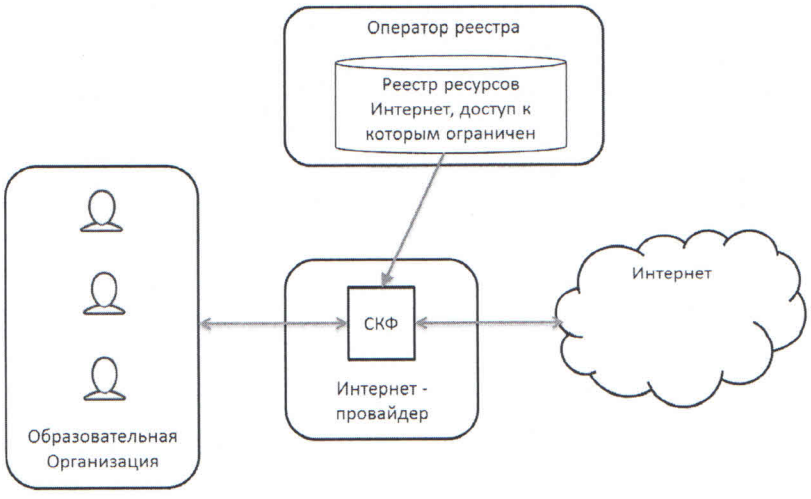
- При увеличении числа клиентских компьютеров до определенного уровня суммарная стоимость лицензий локальных СКФ может превысить стоимость централизованного решения.

Рисунок 3. Схема работы контент-фильтрации при размещении в ОО.




Для снятия данного ограничения рекомендуется внедрить систему контентной фильтрации на стороне Интернет-провайдера либо специализированной организации, обеспечивающей доступ в сеть Интернет для ОО. При этом необходимо обязать Интернет-провайдеров иметь СКФ и предоставлять услугу контентной фильтрации при заключении договоров с целью доступа к сети Интернет образовательных организаций. В этом случае образовательные организации будут подключаться Интернет-провайдером к сети Интернет через данную СКФ. Небольшим Интернет-провайдерам, которые не могут обеспечить полноценное развертывание системы СКФ на своих каналах, достаточно будет пропустить трафик от образовательных организаций на Интернет-провайдера, развернувшего такую систему.

Рисунок 4. Схема работы контент-фильтрации при размещении у Интернет-провайдера.




Такое решение обеспечивает следующие преимущества:

- Упрощается задача унификации интерфейсов обновления настроек систем СКФ, что позволяет полностью автоматизировать процесс обновления;
- СКФ будут всегда доступны для обновления, что повышает оперативность внесения изменений в настройки;
- При определенном количестве обслуживаемых подключений стоимость такого решения будет меньше стоимости локальных установок;
- У Интернет-провайдера появляется инструмент URL фильтрации, который может быть использован и в общих задачах ограничения доступа к информации вместо блокировки по IP и DNS.

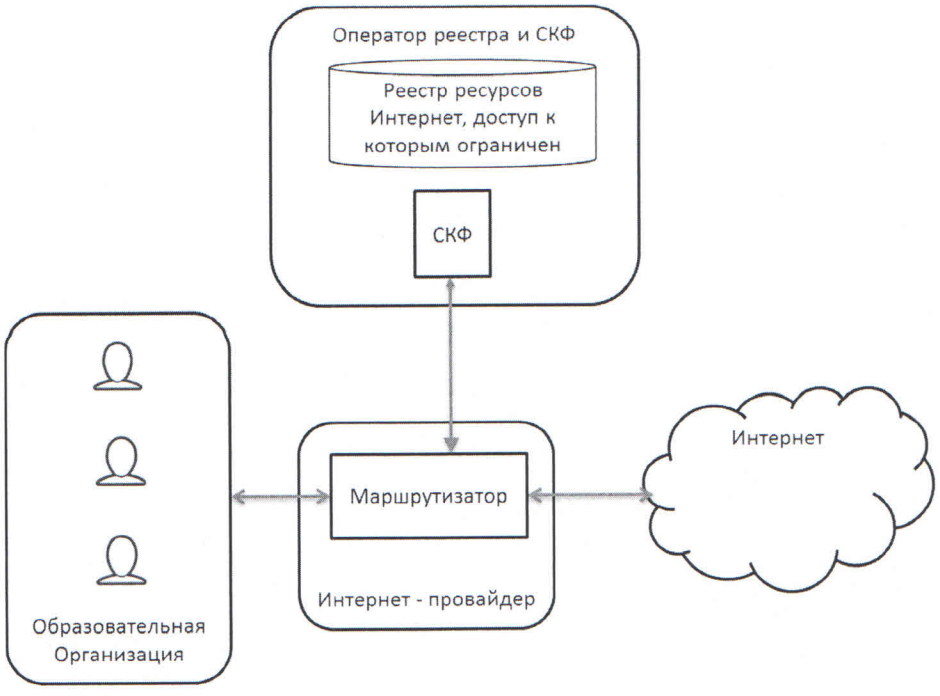
## 4.3. Альтернативный вариант размещения СКФ

Система СКФ может быть реализована как единое решение, распределенное или централизованное, эксплуатируемое уполномоченным органом.

В этом случае, при желании клиента получать услуги фильтрации, Интернет-провайдер должен транслировать, трафик данного клиента на систему фильтрации. К минусам такого решения можно отнести увеличение загрузки каналов, если трафик направлен на локальные Интернет-ресурсы, а также невозможность использовать ресурсы системы фильтрации для блокировки локальных Интернет-ресурсов по URL.

Плюсами решения являются полная централизация и унификация решения, что упростит организационные и технически задачи внедрения системы.

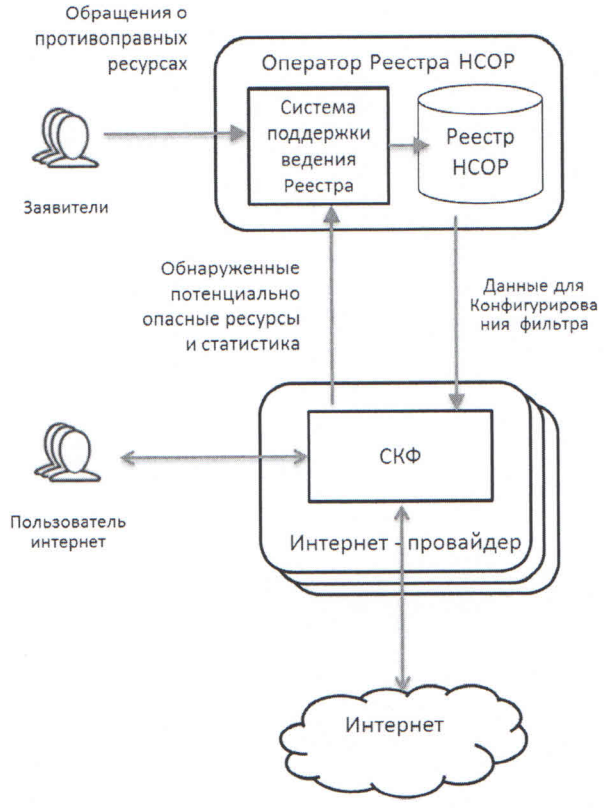
Рисунок 5. Схема работы контент-фильтрации при едином решении.




## 4.4. Принцип управления ограничением доступа обучающихся к информации в Интернет

Схема управления ограничением доступа обучающихся ОО к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования схематично изображена на рисунке № 6.

Рисунок 6. Принцип контроля доступа через Реестр НСОР



Информация о Интернет-ресурсах, доступ к которым должен быть ограничен, заносится в специальную единую базу данных – Реестр НСОР, формируемый в АС Оператора Реестра НСОР.

Из АС Оператора Реестра НСОР данные о Интернет-ресурсах, преобразованные в соответствующий формат (Реестра НСОР), передаются в системы СКФ, установленные у Интернет-провайдеров.

СКФ осуществляет фильтрацию трафика в соответствии с информацией Реестра НСОР. Информацию об обнаруженных на основе семантического анализа потенциально опасных Интернет-ресурсах, а также статистику обращений к Интернет-ресурсам СКФ передает в систему поддержки работы Оператора Реестра НСОР.

Оператор Реестра НСОР обрабатывает информацию от СКФ, а также обращения от граждан и других источников и обновляет содержание Реестра НСОР.

## 4.5. Идентификация трафика Образовательной Организации

Идентификация Образовательной Организации, подключаемой к провайдеру Интернет, осуществляется по статическому внешнему IP адресу (адресам), выделенному Организации ( "белые" IP-адреса), либо путем регистрации соответствия ОО внутренним статическим IP адресам ( серые адреса) при других способах подключения.

## 4.6.Идентификация пользователей для возрастной категоризации

Для того, чтобы СКФ могла обеспечить фильтрацию ресурсов в соответствие с возрастной категорией каждого пользователя необходимо обеспечить идентификацию категории пользователя при доступе к Интернет из ОО. Без реализации такого механизма фильтрация ресурсов в соответствие с возрастной категорией невозможна

Возможно несколько технических решений, различающихся сложностью реализации и эффективностью:

- Индивидуальная идентификация;
- Групповая идентификация;
- Заявительная идентификация.

Первые два способа предполагают выполнение процедуры аутентификации пользователя в системе СКФ при осуществлении доступа к Интернет. Каждой учетной записи устанавливается возрастная категория. После прохождения авторизации СКФ использует данные категории из учетной записи для фильтрации трафика.

Авторизация может быть построена на стандартном механизма прокси-сервера. Следует учитывать, что в этом случае для доступа в Интернет с персональных устройств на них необходимо настраивать proxy-доступ.

Администрирование учетных записей должно осуществляться работником Образовательной Организации через web-интерфейс, предоставляемый СКФ.

***Индивидуальная идентификация***

Данный способ предполагает наличие персональных учетных записей для каждого ученика.

Плюсом данного варианта является возможность доступа в Интернет с персональных устройств. При доступе в Интернет пользователь указывает свои личные данные и тем самым идентифицирует свою категорию.

Однако, в реальности идентификационные данные учащихся с максимальной категорией быстро станут известны всем учащимся, что сведет на нет эффективность данного решения. Данная проблема может быть решена либо ограничением доступа с индивидуальных устройств, либо регистрация индивидуальных устройств и запрет доступа для незарегистрированных устройств.

Кроме того, индивидуальные логины предполагают большой объем администрирования. С другой стороны, наличие систем электронных журналов и дневников предполагает наличие возможности автоматизации администрирования доступа за счет интеграции СКФ с системами учета учеников.

***Групповая идентификация***

Данный способ предполагает использование групповых учетных записей, которые выдается учащимся на время занятий в классе. В этом случае все ученики класса могут использовать одну учетную запись. При этом доступ через эту запись возможен только на протяжении занятия. По завершению занятия доступ закрывается.

Данный вариант представляется достаточно оптимальным с точки зрения объемов администрирования. Однако, данный вариант исключает возможность доступа в Интернет с индивидуальных устройств учащихся.

***Заявительная идентификация***

Данный подход не предполагает аутентификации пользователя. При начале сеанса доступа пользователь направляется СКФ на специальную страницу, где он указывает свою возрастную группу. Далее система осуществляет фильтрацию контента в соответствие с указанной категорией.

Данное решение является достаточно простым, однако оно не будет работать без жесткого контроля доступа со стороны работников ОО.

## 4.7. Автоматическая эскалация

Если при автоматическом анализе системой СКФ контент будет признан потенциально опасным, система может автоматически сформировать и направить на рассмотрение сообщение о подозрительном Интернет-ресурсе. При этом специальная подсистема АС Оператора Реестра НСОР обеспечит группировку сообщений от различных СКФ в одно сообщение, что позволит сократить поток сообщений для анализа. Такие сообщения должны быть приоритезированы по количеству зарегистрированных обращений к данному контенту.

Обработка сообщений о потенциально опасном контенте может координироваться специальными администраторами. На первом этапе осуществляется экспертиза контента. На втором этапе принимается решение о включении Интернет-ресурса в черный или белый список, а также формируются предложения по оптимизации правил анализа контента, чтобы исключить ошибочное отнесение Интернет-ресурса к потенциально опасным.

## 4.8. Актуализация Реестра НСОР

По результатам экспертиз информация о новых Интернет-ресурсах должна быть включена в Реестр НСОР. Данный процесс должен быть автоматизирован в части синхронизации этих изменений с ресурсом Единого реестра (черными и/или белыми списками).

Актуализация конфигурации систем СКФ осуществляется автоматически с необходимой периодичностью, вплоть до on-line актуализации при внесении изменений в Реестр НСОР.

## 4.9. Взаимодействие со специализированными организациями и внешними базами данных

Необходимо обеспечить взаимодействие со специализированными организациями (в том числе международными), осуществляющими свою деятельность в сфере выявления противоправного и не соответствующего целям образования контента. Взаимодействие должно носить технический характер обмена базами данных.

В том числе необходимо автоматизировать процесс приемки сообщений граждан об обнаруженном нелегальном контенте или о блокировке доступа к заведомо легальному контенту.

## 4.10. Общественный контроль

Оптимальным решением в части организации общественного контроля является привлечение общественной организации для выполнения следующих функций:

- Дополнительная экспертиза Интернет-ресурсов;
- Мониторинг решений об изменении Реестра НСОР;
- Сбор информации о незаконных Интернет-ресурсах.

При этом следует учитывать, что предоставление открытого доступа к Реестру НСОР является нежелательным, так как представляет собой, по сути, справочник нежелательного контента.

## 4.11. Функции Оператора Реестра НСОР

Функции Оператора Реестра НСОР:

- Автоматизированный прием сообщений;
- Предварительный анализ и передача на экспертизу обращений;
- Ведение Реестра НСОР;
- Передача Реестра НСОР в СКФ;
- Проверка причин блокировки Интернет-ресурсов и «реабилитации» Интернет-ресурсов;
- Осуществление адресного мониторинга использования сети Интернет в образовательных организациях;

- Взаимодействие с компетентными органами государственной власти в части предоставления им адресной статистики использования сети Интернет в образовательных организациях.

Отличием в ведении Реестра НСОР является дополнительная, к имеющейся, классификация ресурсов, и осуществление адресного мониторинга использования сети Интернет в образовательных организациях.

## 4.12. Профили организаций, подключаемых через СКФ

Фильтрация Интернет-контента необходима не только образовательным организациям, но и другим организациям, в случае наличия у них доступного для детей выхода в Интернет. Примерами таких организаций могут быть детские библиотеки, развивающие центры для детей, спортивные секции, детские оздоровительные лагеря и санатории и т.д. В таких организациях может не применяться ограничение доступа к контенту, не совместимому с задачами образования, но необходимо ограничение доступа детей к информации, причиняющей вред их здоровью и (или) развитию.

Для таких организаций могут быть так же определены и различные предельные возрастные категории посетителей. Для решения поставленных задач в Реестре НСОР возможно создание нескольких профилей фильтрации Интернет-контента, реализующих разный уровень защиты пользователей от нежелательного контента. Профиль фильтрации привязывается в зависимости от типа организации при заключении договора на оказание услуг с Интернет-провайдером.

## 4.13. Структура Реестра НСОР

Поскольку требования по ограничению доступа к сетевым ресурсам определяются различными нормативными документами, в которые по мере необходимости могут вноситься независимые изменения, то для удобства ведения Реестра НСОР целесообразно выделить следующие разделы:

- Интернет-ресурсы, запрещенные для детей и методические правила выявления потенциально опасных Интернет-ресурсов данной категории;
- Интернет-ресурсы, не совместимые с задачами образования и методические правила выявления потенциально опасных Интернет-ресурсов данной категории.

Реестр НСОР состоит из нескольких взаимосвязанных частей:

- Справочник категорий информации;
- «Черный» список Интернет-ресурсов по категориям информации;
- Правила контентной фильтрации Интернет-ресурсов по категориям информации
- «Белый» список Интернет-ресурсов (образовательные ресурсы, рекомендованные Минобрнауки России).

## 4.14. Борьба со средствами обхода защиты

Обеспечить 100%-ную защиту от нежелательного контента в Интернет невозможно. Существующие системы противодействия таким инструментам как тор, публичные прокси-сервера и т.д., так называемые системы DPI, дороги для массового применения и при этом не обеспечивают необходимого уровня защиты.

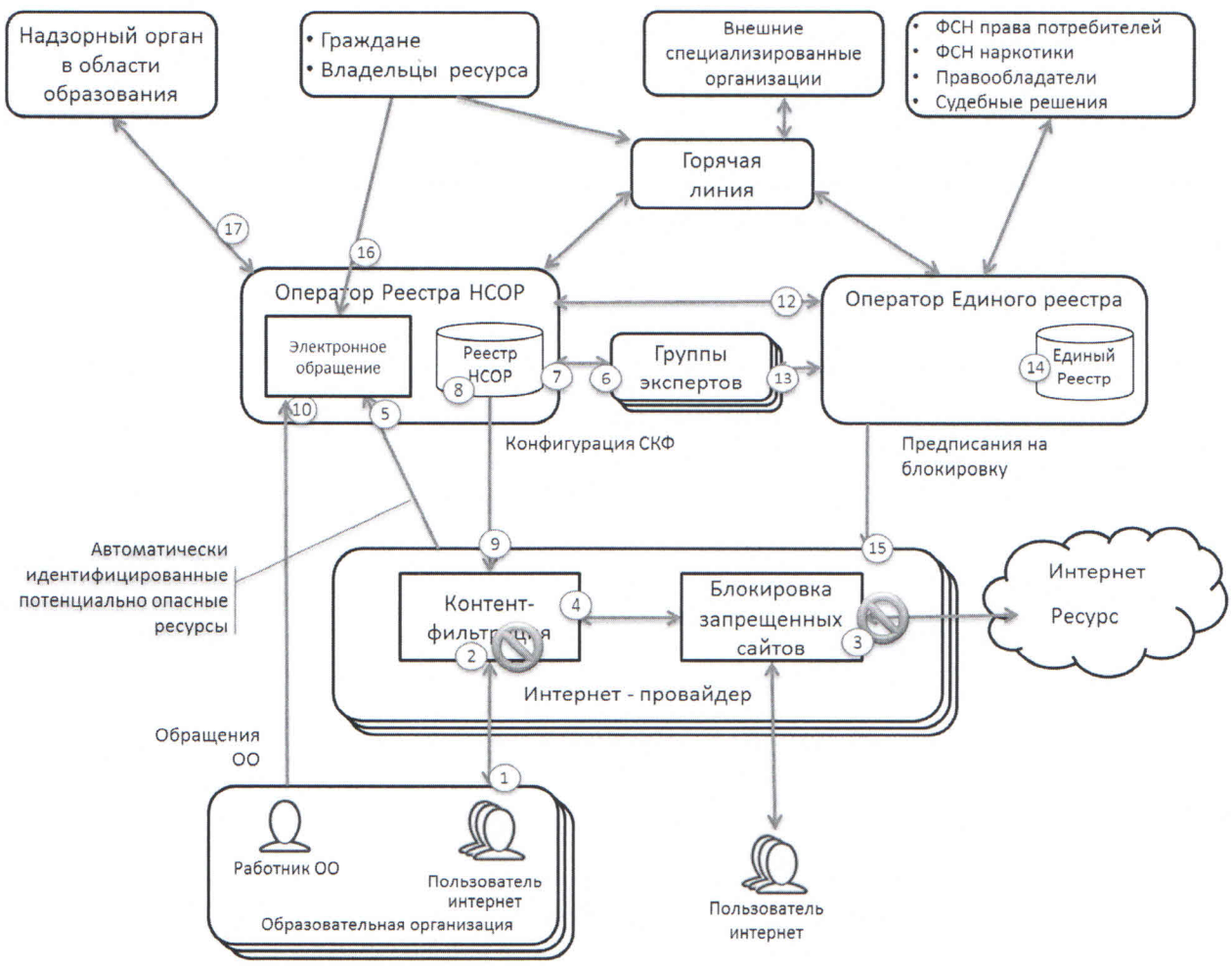
При правильной организации процесса доступа к интернет из образовательных организаций возможно свести риск доступа пользователей к нежелательному контенту практически к нулю.

Учитывая сказанное, предлагаемое решение не включает средства противодействия инструментам обхода защиты, а рассматривает их как возможные дополнения, усиливающие степень защиты, в случае если это необходимо.

## 4.15. Организационная схема построения решения СКФ

На Рисунке 7 представлена общая схема процесса ограничения доступа обучающихся из ОО к информации в Интернет, не соответствующей задачам образования, включая схему взаимодействия участников процесса ограничения доступа к сайтам сети Интернет, содержащим запрещенную информацию.

Рисунок 7. Схема процесса взаимодействия




## 4.16. Автоматизация процессов Оператора Реестра НСОР

С целью оптимизации исполнения задач Оператору Реестра НСОР целесообразно автоматизировать ряд функций. Автоматизации в первую очередь подлежат функции, позволяющие сократить время между обнаружением не корректного доступа к контенту и обновлением Реестра по результатам экспертизы ресурса. .

С учетом вышесказанного можно выдели функции, которые целесообразно исполнять посредством автоматизированной системы Оператора Реестра НСОР:

-взаимодействие с СКФ, используемыми для ОО;

- сбор статистических данных использования сети Интернет в ОО;

- передача на экспертизу Интернет-ресурсов, содержащих контент, не соответствующий образовательному процессу;

- ведение базы данных URL-адресов, содержащих контент, не соответствующий образовательному процессу;

- взаимодействие с внешними базами данных Интернет-ресурсов и специализированными организациями;

- автоматизированный прием заявлений об обнаружении Интернет-контента, не соответствующего образовательному процессу;

- взаимодействие с компетентными органами государственной власти;

Подробные функциональные требования к автоматизированной системе представлены в Приложении №4.

# 5. ПРИЛОЖЕНИЕ №3 ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К СКФ

В данном разделе представлены высокоуровневые функциональные и нефункциональные требования к СКФ.

Требования к СКФ устанавливаются для обеспечения возможности использования продуктов различных поставщиков. Требования должны обеспечить:

- единообразие результата фильтрации для всех пользователей, чей трафик подвергается фильтрации;
- для совместимости СКФ с системами поддержки работы Оператора Реестра НСОР и системами сбора статистики.

**Нефункциональные требования**

СКФ предназначены для размещения на базе Интернет-провайдеров или на базе специализированных организаций, обеспечивающих функции коллективной точки доступа к сети Интернет и предоставляющих телематические услуги связи образовательным организациям.

Система должна обеспечивать выполнение функций фильтрации на каналах со скоростью до 10 Гбит/с. Система должна обеспечивать линейную масштабируемость пропускной способности фильтруемых каналов.

Архитектура СКФ должна обеспечивать возможность применения современных методов обеспечения бесперебойности функционирования при сбоях и техническом обслуживании (кластеризация, резервирование) для обеспечения доступности системы не хуже 98%.

Архитектура и применяемые в системе и при ее разработке технологии должны соответствовать современным стандартам и тенденциям индустрии, включая платформо-независимость, использование свободно распространяемого ПО, масштабируемость, гибкость размещения (deployment) и другие.

Структура хранения данных СКФ должна быть открытой.

Применяемые при разработке и использовании интерфейсов технологии, стандарты и спецификации должны соответствовать нормативно установленным и общепринятым стандартам и требованиям в области информационных технологий и программного обеспечения.

При использовании сетевых протоколов передачи данных необходимо придерживаться следующих спецификаций:

- протокол передачи гипертекста версии 1.11 - RFC 2616;
- расширенный протокол передачи гипертекста версии 1.1 с обеспечением безопасности транспортного уровня;
- протокол защищенных соединений (SSL) версии 3 – RFC 5246;
- протоколы использования системы поддержки пространства имен - FC 1035.

При описании данных, а также информации о данных, их составе и структуре, содержании, формате представления, методах доступа и требуемых для этого полномочиях пользователей, о месте хранения, источнике, владельце и др. (далее – метаданные) и используемых наборах символов, применяемых в процессе информационного обмена, необходимо придерживаться следующих спецификаций:

- расширяемый язык разметки XML- набор стандартов Консорциума Всемирной паутины;
- расширяемый язык описания схем данных (XML Schema) версии не ниже 1.0.

Описания разрабатываемых электронных сервисов и описания схем данных, согласно базовому профилю интероперабельности версии 1.1, должны создаваться в кодировке UTF-8 или UTF-16 (с указанием этой кодировки в заголовке соответствующего описания).

Аутентификация должно строиться на основе сертификатов PKI в формате X.509.

**Функциональные требования**

Система должна обеспечивать следующие основные функции:

- осуществлять в режиме реального времени анализ Интернет-ресурсов, к которым обращаются пользователи;
- пропускать, блокировать или модифицировать информацию от Интернет-ресурса к пользователю в зависимости от результатов проверки;
- автоматически загружать правила фильтрации из внешнего источника (Реестра НСОР);
- автоматически передавать данные во внешнюю систему о Интернет-ресурсах, информация из которых удовлетворяет заданным правилам;
- собирать и передавать во внешние системы статистику фильтрации.

Анализ Интернет-ресурсов

Система должна обеспечивать определение категории Интернет-ресурса путем сопоставления URL-адреса с базой URL-адресов Реестра НСОР. Система должна поддерживать множество категорий Интернет-ресурсов.

Система должна обеспечивать возможность анализ поисковых HTTP-запросов путем разбора запроса, сформированного поисковыми машинами, и сравнением составных частей запроса со словарем слов, словосочетаний и словообразований, включенных в запрещенные категории в Реестре НСОР. Система должна поддерживать множество категорий запрещенных слов, словообразований и словосочетаний.

Если Интернет-ресурс не попадает ни под одну категорию, то система должна обеспечивать анализ с применением семантического и морфологического анализа.

Система должна обеспечивать возможность семантического и морфологического анализа информации Интернет-ресурсов, получаемых по HTTP протоколу, на основе списков запрещенных слов, словообразований и словосочетаний, сформированных в Реестре НСОР, а также сочетаний слов из разных категорий, образующие совокупности запрещенных выражения. Информация Интернет-ресурсов должна интерпретироваться строго согласно стандартам на протокол передачи гипертекста и язык разметки гипертекста, в том числе должна корректно определяться кодировка передаваемых данных.

Система должна обеспечивать сопоставление категории Интернет-ресурса с категорией пользователя и принимать решение о доступе пользователя к информации.

Действия по результату анализа

Система должна обеспечивать возможность по результатам анализа Интернет-ресурсов:

- отображение специальной страницы предупреждения с возможностью пропуска информации от Интернет-ресурса в случае подтверждения пользователя;
- блокировка URL-адреса Интернет-ресурса, запрашиваемой по HTTP протоколу, при совпадении URL-адреса с базой URL-адресов Реестра НСОР;
- отображение специальной страницы блокировки в случае блокировки URL-адреса Интернет-ресурса;
- блокировка части информации от Интернет-ресурса, запрашиваемой по HTTP протоколу, и пропуск только не заблокированных частей пользователю;
- перенаправление запроса по специальным адресам, в зависимости от категории, присвоенной Интернет-ресурсу по результатам анализа;

Система должна обеспечивать метод принудительного включения безопасного поиска в поисковых системах путем добавления аргумента «&family=yes&» или «&safe=yes&».

Ведение статистики фильтрации

Система должна обеспечивать сбор статистики фильтрации, включая:

- Время;
- IP-адрес, с которого произошло обращение;
- Образовательное учреждение (по соответствию IP адреса);
- URL Интернет-ресурса, к которому было произведено обращение;
- домен системы DNS, к которому было произведено обращение;
- вид фильтрации, согласно которому обращение было заблокировано, если обращение было заблокировано;
- категория, к которой был отнесен данный Интернет-ресурс;
- ключевые слова, по которым было заблокировано обращение, если обращение было заблокировано методом поисковой или контентной фильтрации;
- подтверждение пользователя, если он был предупрежден о потенциально опасной информации.

Система должна обеспечивать хранение статистики в течение срока, устанавливаемого соответствующими нормативными документами.

Система должна обеспечивать возможность передачи статистики во внешние системы в соответствии с установленными требованиями к взаимодействию.

Настройка параметров работы

Система должна обеспечивать автоматическое обновление конфигурации Системы при изменении параметров настойки Системы. Параметрами Системы являются:

- пороговая величина блокировки Интернет-ресурса на основе семантического и морфологического анализа;
- адрес специальной страницы блокировки;
- адрес специальной страницы блокировки поисковых HTTP-запросов;
- адрес специальной страницы предупреждения с возможностью пропуска информации от Интернет-ресурса;
- параметры взаимодействия с Реестром НСОР.

- параметры взаимодействия с внешней системой для передачи информации о потенциально опасных Интернет-ресурсах

Обновление правил фильтрации от внешней системы

Система должна обеспечивать автоматическое обновление конфигурации (правил) фильтрации при изменении информации в Реестре НСОР. Обновление должно осуществляться не более чем через 1 час после изменений в Реестр НСОР. Обновлению подлежат:

- списки новых категорий Интернет-ресурсов;
- списки URL адресов Интернет-ресурсов с присвоенными категориями;
- списка слов, словообразований и словосочетаний для выполнения фильтрации с присвоенными категориями.

Взаимодействие с внешней системой должно осуществляться в соответствии с установленными требованиями к взаимодействию.

Передача информации о потенциально опасных Интернет-ресурсах во внешнюю систему

Система должна обеспечивать автоматическую передачу во внешнюю систему информации об Интернет-ресурсе, соответствующем заданным правилам. Передаче подлежат URL Интернет-ресурсов, информация которых была определена как потенциально опасная по результатам морфологического и семантического анализа.

Взаимодействие с внешней системой должно осуществляться в соответствии с установленными требованиями к взаимодействию.

# 6. ПРИЛОЖЕНИЕ №4 ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К АСОР

Автоматизированная система Оператора Реестра НСОР (АСОР) (далее - Система) предназначена для автоматизации функций управления Реестром НСОР.

**Функциональные требования**

Система АСОР должна обеспечивать следующие основные функции:

- регистрацию и учет обращений граждан и образовательных организаций касательно Интернет-ресурсов (обнаруженная противоправная информация, доступ к информации не совместимой с задачами образования, некорректно заблокированных Интернет-ресурсах);
- регистрацию и учет уведомлений от систем СКФ об обнаруженных потенциально-опасных Интернет-ресурсах;
- автоматизацию процесса обработки зарегистрированных обращений и уведомлений;
- ведение Реестра НСОР;
- автоматическая передача данных Реестра НСОР в системы СКФ для обновления конфигурации (правил) фильтрации;
- автоматический сбор и агрегацию статистики работы ОО с Интернет, полученную от СКФ;
- взаимодействие с внешними базами данных Интернет-ресурсов и специализированными организациями, компетентными органами государственной власти;

Регистрация обращений

Система должна обеспечивать возможность регистрации обращений граждан, организаций и ОО касательно Интернет-ресурсов через электронную форму в сети Интернет. Форма должна быть доступна как минимум на русском и английском языке.

Система должна предоставлять API для автоматической регистрации обращений из внешних систем.

Система должна обеспечивать возможность ручной регистрации обращений пользователем системы.

Перечень регистрируемых для обращений данных должен, как минимум, включать:

- дату и время обращения;
- причину обращения по классификатору причин (нелегальный контент, информация не совместимая с задачами образования, необоснованно заблокированный Интернет-ресурс и т.д.);
- URL-адрес Интернет-ресурса;
- идентификационные данные ОО;
- идентификационные данные внешних систем;
- контактные данные обратившегося;
- комментарии.

Система должна обеспечивать хранение обращений и учет состояния их жизненного цикла в соответствии с процессом обработки.

Система должна автоматически исключать из процесса обработки повторяющихся обращений (по URL, домену, IP адресу). При этом система должна учитывать, как находящиеся в обработке обращения, так и обращения с принятым решением.

Регистрация уведомлений

Система должна обеспечивать автоматическую регистрацию уведомлений от систем СКФ об обнаруженных потенциально-опасных Интернет-ресурсах.

Система должна предоставлять аутентификацию систем СКФ на основе сертификатов PKI в формате X.509.

Перечень регистрируемых для обращений данных должен, как минимум, включать:

- дату и время уведомления;
- URL адрес Интернет-ресурса;
- набор данных Реестра НСОР по которым данный Интернет-ресурс был идентифицирован как потенциально-опасный (набор запрещенных слов, категория пользователя);
- идентификационные данные Интернет-провайдера;
- идентификационные данные ОО;
- идентификационные данные систем СКФ.

Система должна обеспечивать хранение обращений и учет состояния их жизненного цикла в соответствии с процессом обработки.

Система должна автоматически анализировать наличие уведомлений для данного URL-адреса от других систем СКФ и повышать приоритет обработки уведомления.

Система должна автоматически исключать из процесса обработки повторяющиеся уведомления. При этом система должна учитывать, как находящиеся в обработке уведомления, так и уведомления с принятым решением.

Система должна автоматически уведомлять администратора системы в случае поступления уведомления по Интернет-ресурсу, относительно которого уже было принято решение и в Реестр НСОР были внесены изменения, либо истекло время обновления конфигураций СКФ.

Взаимодействие с системами СКФ

Система должна предоставлять API для автоматической взаимодействия с системами СКФ.

Система должна предоставлять аутентификацию и регистрацию систем СКФ на основе сертификатов PKI в формате X.509.

Перечень методов взаимодействия систем СКФ должен, как минимум, включать:

- аутентификация СКФ;
- регистрация и отправка идентификационных данных систем СКФ;
- передача данных Реестра НСОР в СКФ;
- сбор статистики от СКФ.

Система должна обеспечивать аутентификацию систем СКФ в соответствие с

процессом обработки запросов.

Перечень параметров для аутентификации систем СКФ должен, как минимум, включать:

- идентификатор системы СКФ;
- ключ системы СКФ, зашифрованный открытым ключом, выданным системе СКФ, закодированный в Base64.

Система должна передавать системам СКФ токен аутентификации, действующий ограниченное время, для дальнейшего взаимодействия.

Система должна автоматически регистрировать системы СКФ в соответствие с процессом обработки запросов к Системе.

Перечень параметров для регистрации систем СКФ должен, как минимум, включать:

- идентификатор инсталляции системы СКФ;
- тип системы СКФ;
- производительность системы СКФ.

Автоматизация процесса обработки обращений и уведомлений;

Система должна обеспечивать автоматическое назначение обращений и уведомлений на исполнителей в соответствии с установленным регламентов обработки.

Как минимум регламент включает следующие шаги обработки:

- проведение экспертизы Интернет-ресурса;
- принятие решения по обращению или уведомлению по результатам экспертизы.

Система должна обеспечивать пользователям доступ к списку назначенных обращений и уведомлений в соответствии с ролью пользователя.

Система должна обеспечивать возможность регистрации результатов экспертизы Интернет-ресурса в обращении или уведомлении.

Система должна обеспечивать возможность регистрации принятого решения по обращению или уведомлению.

Система должна обеспечивать регистрацию времени начала и завершения обработки задачи пользователем.

Ведение Реестра НСОР

Система должна обеспечивать хранение данных Реестра НСОР. Как минимум данные должны включать:

- Справочник категорий информации;
- «Черный» список Интернет-ресурсов по категориям информации;
- «Черный» список слов, словосочетаний и словообразований по категориям информации;
- «Белый» список Интернет-ресурсов по категориям информации;
- Правила контентной фильтрации Интернет-ресурсов по категориям информации.

Система должна предоставлять администратору системы инструменты изменения данных Реестра НСОР.

Система должна предоставлять функции автоматического внесения изменений в Реестр НСОР по результатам принятого решения по обращениям и уведомлениям.

Передача данных Реестра НСОР в системы СКФ

Система должна обеспечивать автоматическую передачу данных (или обновлений данных) из Реестра НСОР системам СКФ.

Система должна предоставлять аутентификацию систем СКФ на основе сертификатов PKI в формате X.509.

Система должна обеспечивать контроль получения данных системами СКФ. В случае не получения данных системой СКФ в течение заданного времени система должна уведомлять администратора системы.

Взаимодействие с системами СКФ должно осуществляться в соответствии с установленными требованиями к взаимодействию.

Передача данных Оператору Единого реестра

Система должна обеспечивать автоматическую передачу обращения Оператору Единого реестра в случае признания, по результатам экспертизы, информации Интернет-ресурса запрещенной к распространению в РФ.

Сбор статистики

Система должна обеспечивать автоматический сбор и хранение статистики от систем СКФ.

Система должна обеспечивать контроль полноты статистики и уведомлять администратора в случае отсутствия данных по периодам.

Система должна обеспечивать автоматическое обнаружение всплесков обращений к Интернет-ресурсам на основании URL и формировать уведомление.

Система должна обеспечивать возможность доступа к данным статистики для внешних систем отчетности, а также обеспечивать выгрузку данных в установленном формате за заданный период.

# 7. ПРИЛОЖЕНИЕ №5 ТРЕБОВАНИЯ К ИНТЕРНЕТ-ПРОВАЙДЕРАМ

Интернет-провайдер имеет право на предоставление услуг доступа к Интернет Образовательным Организациям при условии соответствия требованиям, предъявляемым ФОИВ в области образования и связи.

Указанные требования, как минимум, включают:

- требование наличия системы СКФ, зарегистрированной Оператором Реестра НСОР. Технические условия регистрации определяются Оператором Реестра НСОР;
- требования к обеспечению доступности и качества услуги доступа к Интернет.
- идентификация Образовательной Организации, подключаемой к провайдеру Интернет, осуществляется по статическому внешнему IP адресу (адресам), выделенному Организации ("белые" IP-адреса), либо путем регистрации соответствия ОО внутренним статическим IP адресам ( серые адреса) при других способах подключения.

Контроль за соблюдением правил осуществляется региональным надзорным органом в области образования, а также иными органами власти в соответствии с их компетенцией.