Принято решением педагогического совета
МБОУ ПГО «Средняя общеобразовательная школа № 18»
Протокол № 1 от 31.08.2020 г.

Утверждаю: Тарасова Т.Г.,
директор МБОУ ПГО «Средняя общеобразовательная школа № 18»
Приказ от 31.08.2020 № 312-Д

ПОЛОЖЕНИЕ
по организации доступа к сети Интернет в МБОУ ПГО «Средняя общеобразовательная школа № 18»

1. Общие положения

1.1. В целях обеспечения учебного процесса и в соответствии с законодательством Российской Федерации в МБОУ ПГО «Средняя общеобразовательная школа № 18» (далее – ОО) предоставляется доступ к глобальной сети Интернет (далее - Интернет). В соответствии с Федеральным законом Российской Федерации от 29 декабря 2010 г. № 436-ФЗ (ред. от 14.10.2014 г.) «О защите детей от информации, причиняющей вред их здоровью и развитию» и ст. 3 Федерального закона от 25.07.2002 г. № 114-ФЗ (ред. от 21.07.2014 г.) «О противодействии экстремистской деятельности» доступ детей в образовательной организации ограничивается от информации, пропаганды и агитации, наносящих вред их здоровью, нравственному и духовному развитию (далее – Нежелательная информация).

1.2. Доступ к Интернету предоставляется сотрудникам и обучающимся ОО для осуществления учебной деятельности.

1.3. Доступ к Интернету осуществляется в минимальном объеме, необходимым для заявленных целей.

1.4. Целью данного Положения является формирование общих подходов к организации доступа к сети Интернет сотрудников и обучающихся ОО.

1.5. Настоящее Положение устанавливает:

- порядок организации доступа в Интернет;
- организацию защиты обучающихся от Нежелательной информации, распространяемой через сеть Интернет.

1.6. Настоящее Положение вступает в силу с момента подписания приказа директором ОО приказа об его утверждении.

1.7. Пересмотр Положения осуществляется при изменении действующего законодательства, по результатам инцидентов и других соответствующих обстоятельств.

1.8. Требования настоящего Положения распространяются на всех сотрудников ОО, использующих компьютеры и другие мультимедиа устройства в образовательной деятельности в помещении ОО.

1.9. Сотрудники ОО, использующие в своей работе ресурсы сети Интернет, должны быть ознакомлены с настоящим Положением.

2. Основные направления работ по защите учащихся от Нежелательной информации, распространяемой через сеть Интернет

2.1. ОО обеспечивает защиту обучающихся от Нежелательной информации, распространяемой через сеть Интернет, во время нахождения обучающихся в ОО.

2.2. Выделяются следующие основные направления работ по защите обучающихся от Нежелательно информации:

- определение Нежелательной информации;
- организация деятельности по защите учащихся от Нежелательной информации во время нахождения в ОО;
- определение обязанностей и установление персональной ответственности за нарушение безопасности при работе в сети Интернет.
- контроль за поддержанием безопасного доступа к ресурсам сети Интернет.

3. Определение Нежелательной информации

3.1. К Нежелательной информации относится информация определённая законодательством Российской Федерации:

- информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды – согласно Федеральному закону от 27.07.2006 № 149-ФЗ (ред. От 27.07.2014) «Об информации, информационных технологиях и о защите информации»;
- информация, наносящая вред нравственному и духовному развитию ребёнка – согласно Федеральному закону от 29 декабря 2010 г. №436-ФЗ (ред. от 14.10.2014г.) «О защите детей от информации, причиняющей вред их здоровью и развитию».

3.2. На основании вышеуказанных документов в ОО утвержден Классификатор информации, не совместимой с задачами образования и воспитания обучающихся в ОО. Каждый сотрудник ОО, использующий в своей работе ресурсы сети Интернет, должен быть ознакомлен с Классификатором и использовать его для определения Нежелательной информации.

4. Организация деятельности по защите учащихся от Нежелательной информации во время нахождения в Школе.

4.1. Защита обучающихся от Нежелательной информации в сети Интернет осуществляется методом ограничении доступа к Интернет-контенту.

4.2. Ограничение доступа осуществляется на двух уровнях:

- на стороне провайдера услуг доступа в сеть Интернет – общая фильтрация для всех компьютеров и мультимедиа устройств, подключаемых через сеть ОО. Ограничивает доступ Интернет-ресурсам, запрещенным соответствующими органами Российской Федерации (прокуратура, ФСКН, Роспортребнадзор и т.д.)
- на стороне конечного пользователя – программами, ограничивающими доступ к Интернет - содержимому (далее – контент-фильтр), средствами

комплексной антивирусной защиты (антивирусный мониторинг, проверка компьютера, контроль входящего Интернет-трафика, антифишинговый и антихакерский контроль), дополнительно средствами фильтрации на маршрутизаторе с использованием безопасных DNS-серверов.

4.3. На каждый компьютер, к которому возможен доступ обучающихся, устанавливается контент-фильтр, если не используются средства фильтрации на маршрутизаторе с использованием безопасных DNS-серверов.

4.4. Основным (постоянным) уровнем защиты контент-фильтра принимается уровень белых списков, который позволяет посещать только проверенные сайты.

4.5. Допускается добавление педагогом в контент-фильтр своего списка разрешенных сайтов, не входящих в перечень запрещенных сайтов.

4.6. Во время работы в сети Интернет сотрудники и обучающиеся обязаны соблюдать Правила работы в сети Интернет, утвержденные директором ОО.

4.7. Сотрудники ОО не несут ответственность за доступ обучающихся к Нежелательной информации с личных мобильных устройств обучающихся.

5. Определение обязанностей и установление персональных устройств ответственности за нарушение безопасности при работе в сети Интернет.

5.1. Сотрудник, на рабочем месте которого, установлен компьютер, несет персональную ответственность за его работоспособность и надлежащее состояние защиты. В кабинетах, где установлено несколько компьютеров, ответственное лицо закрепляется отдельным документом. В случае, когда сотрудник использует личный компьютер, он самостоятельно обеспечивает безопасность работы в сети Интернет и несет ответственность за защиту обучающихся от Нежелательной информации.

5.2. Каждый ответственный сотрудник обязан следить за текущим состоянием защиты компьютера.

5.3. В случае обнаружения сотрудником некорректной работы компьютера или неработоспособных компонентов защиты, необходимо незамедлительно сообщить об этом лицу, ответственному за информационную безопасность в ОО, для устранения.

5.4. Обучающимся ОО запрещен доступ к рабочим компьютерам сотрудников. Сотрудник, за которым закреплен компьютер, лично следит за недопущением обучающихся к данному компьютеру.

5.5. Во время работы обучающихся в сети Интернет, преподаватель осуществляет постоянный контроль за работой обучающегося в сети Интернет.

5.6. Ответственный за компьютер сотрудник периодически (не реже одного раза в месяц) самостоятельно проверяет добавленные в личный белый список контент-фильтра сайты на соответствие с перечнем запрещенных сайтов.

5.7. В случае обнаружения доступа к запрещенному сайту или при наличии Нежелательной информации на сайте из белого списка, а также в случае выхода на сайт, содержащий Нежелательную информацию, сотрудник вносит сайт в список «Запретить сайты».

5.8. При трансляции изображения на интерактивную доску (экран) контент-фильтр должен работать в основном режиме.

5.9. Сотрудник ОО для более широкого поиска информации в сети Интернет может временно понизить уровень защиты контент-фильтра или отключить его при условии отсутствия обучающихся в кабинете и отсутствии трансляции на интерактивную доску (экран).

5.10. Временное отключение контент-фильтра должно обеспечивать его автоматическое включение при следующей загрузке операционной системы компьютера.

5.11. Сотрудник после окончания работы в сети Интернет, а также после окончания работы обучающихся, вносит в Журнал регистрации работы в сети Интернет данные о посещенных сайтах и цели работы в сети Интернет.

5.12. За отключение или понижение уровня защиты контент-фильтра сотрудник несет персональную ответственность.

6. Контроль за поддержанием безопасного доступа к сети Интернет

6.1. Текущий контроль за режимом работы контент-фильтра и состоянием антивирусной программы осуществляется сотрудником, ответственным за компьютер, самостоятельно, на регулярной основе.

6.2. При обнаружении проблем, сотрудник, ответственный за компьютер, должен самостоятельно устранить их в соответствии с Инструкцией по работе в сети Интернет для сотрудников образовательной организации *(Приложение 1)*. При невозможности самостоятельного устранения – сообщить о неполадках ответственному за информационную безопасность лицу.

6.3. Ответственный за компьютер сотрудник, самостоятельно добавивший личный белый список сайтов в контент-фильтр, регулярно, не реже одного раза в месяц, контролирует отсутствие указанных сайтов в реестре запрещенных сайтов.

6.4. Не реже двух раз в год (период летних и зимних каникул), либо по специальному распоряжению директора все компьютеры в ОО проверяются на соответствие требованиям безопасности, сформированным в настоящем Положении, комиссией в составе не менее 3-х человек, с последующим составлением акта.

(Приложение 1)

Инструкция
по организации доступа к сети Интернет и работе с контент - фильтром

Часть I. Основные направления работ по защите обучающихся от Нежелательной информации, распространяемой через сеть Интернет

1. Общие положения

1.1 Настоящая инструкция по организации доступа к сети Интернет и работе с контент - фильтром разработана в соответствии с законом РФ от 29.12.2010 г. № 436-ФЗ (в ред. от 14.10.2014 г.) «О защите детей от информации, причиняющей вред их здоровью и развитию» и ст. 3 Федерального закона от 25.07.2002 г. № 114-ФЗ (в ред. от 21.07.2014 г.) «О противодействии экстремистской деятельности» и на основе Положения по организации доступа к сети Интернет в МБОУ ПГО «СОШ № 18» от 09.01.2015 г. № 01/2-Д, в целях обеспечения учебной деятельности и доступа детей в образовательной организации с ограничением от информации, пропаганды и агитации, наносящих вред их здоровью, нравственному воспитанию и развитию (далее – Нежелательная информация).

1.2. Доступ к сети Интернет в образовательной организации предоставляется сотрудникам и обучающимся ОО для осуществления образовательной деятельности.

1.3. Доступ к сети Интернет осуществляется в минимальном объеме, необходимым для заявленных целей.

1.4. Требования настоящей инструкции обязательны к выполнению всеми сотрудниками образовательной организации, использующими персональные компьютеры и другие мультимедиа устройства на территории ОО.

2. Определение Нежелательной информации

2.1. К нежелательной информации относится информация, определенная законодательством Российской Федерации:

- информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, определенная Федеральным законом от 27.07.2006 г. № 149-ФЗ (в ред. от 27.07.2014 г.) «Об информации, информационных технологиях и защите информации»;
- информация, наносящая вред нравственному и духовному воспитанию детей, определенная Федеральным законом от 29.12.2010 г. № 436-ФЗ (в ред. от 14.10.2014 г.) «О защите детей от информации, причиняющей вред их здоровью и развитию».

3. Организация деятельности по защите обучающихся от Нежелательной информации во время нахождения в ОО

3.1. Защита учащихся от Нежелательной информации в сети Интернет осуществляется методом ограничения доступа к интернет-контенту.

3.2. Ограничение доступа осуществляется на двух уровнях:

- на стороне провайдера услуг доступа в Интернет – общая фильтрация для всех компьютеров и мультимедиа устройств, подключаемых через сеть ОО. Ограничивает доступ к Интернет-ресурсам, запрещённым соответствующими органами РФ (прокуратура, ФСКН, Роспотребнадзор и т.д.).
- на стороне конечного пользователя – программами, ограничивающими доступ к интернет - содержимому (далее Контент-фильтр), средствами комплексной антивирусной защиты (антивирусный мониторинг, проверка компьютера, контроль входящего интернет - трафика, антифишинговый и антихакерский контроль), дополнительно средствами фильтрации на маршрутизаторе с использованием безопасных DNS-серверов.

3.3. Контент-фильтр устанавливается на каждом компьютере, к которому возможен доступ обучающихся.

3.4. Основным (постоянным) уровнем защиты контент-фильтра принимается уровень белых списков – позволяет посещать только проверенные сайты.

3.5. Допускается добавление педагогом в контент-фильтр своего списка разрешённых сайтов, не входящих в перечень запрещённых сайтов.

3.6. Во время работы в сети Интернет сотрудники и учащиеся обязаны соблюдать Правила работы в сети Интернет, утвержденные директором ОО.

3.7. Сотрудники не несут ответственность за доступ обучающихся к Нежелательной информации с личных мобильных устройств обучающихся.

4. Обязанности и персональная ответственность за нарушение безопасности при работе в сети Интернет

4.1. Сотрудник, на рабочем месте которого, установлен компьютер, несет персональную ответственность за его работоспособность и надлежащее состояние защиты. В кабинетах, где установлено несколько компьютеров, ответственное лицо закрепляется отдельным документом. В случае, когда сотрудник использует личный компьютер, он самостоятельно обеспечивает безопасность работы в сети Интернет и несет ответственность за защиту обучающихся от Нежелательной информации.

4.2. Каждый ответственный лицу необходимо следить за текущим состоянием защиты компьютера.

4.3. При обнаружении некорректной работы компьютера или неработоспособных компонентов защиты необходимо незамедлительно сообщить об этом специалисту по охране труда для устранения.

4.4. Обучающимся ОО запрещен доступ к рабочим компьютерам сотрудников. Сотрудник, за которым закреплен компьютер, лично следит за недопущением обучающихся к данному компьютеру.

4.5. Во время работы обучающегося в сети Интернет педагогу необходимо находиться рядом и осуществлять контроль за работой учащегося в сети Интернет.

4.6. Ответственному за компьютер лицу, необходимо периодически (не реже одного раза в месяц), самостоятельно проверяет добавленные в личный белый список контент-фильтра сайты на соответствие с перечнем запрещённых сайтов.

4.7. В случае обнаружения доступа к запрещенному сайту или при наличии Нежелательной информации на сайте из белого списка, а также в случае выхода на сайт, содержащий Нежелательную информацию, ответственному за компьютер лицу необходимо вносить данный сайт в список запрещенных сайтов.

4.8. При трансляции изображения на доску (экран) контент-фильтр должен быть работать в основном режиме.

4.9. Ответственному за компьютер лицу для более широкого поиска информации в сети Интернет, при условии отсутствия в кабинете обучающихся и отсутствии трансляции на доску (экран), можно временно понизить уровень защиты контент-фильтра либо отключить его.

4.10. Временное отключение контент-фильтра должно обеспечивать автоматическое его включение при следующей загрузке операционной системы компьютера.

4.11. Ответственному за компьютер лицу после окончания работы в сети Интернет, а также после окончания работы в сети Интернет обучающихся, необходимо внести в Журнал регистрации работы в сети Интернет данные о посещенных сайтах и цели работы в сети Интернет.

4.12. Персональную ответственность за понижение уровня или отключение контент-фильтра несет лично ответственное за компьютер лицо.

5. Контроль за поддержанием безопасного доступа к сети Интернет

5.1. Текущий контроль за режимом работы контент-фильтра и состоянием антивирусной программы осуществляется сотрудником, несущим персональную ответственность за компьютер.

5.2. Сотрудник, несущий персональную ответственность за компьютер, самостоятельно добавивший личный белый список сайтов в контент-фильтр, регулярно, не реже одного раза в месяц контролирует, что данные сайты не входят в реестр запрещенных сайтов.

5.3. Возле каждого компьютера имеющего доступ к сети Интернет должен находиться Журнал регистрации работы в сети Интернет. Сотрудник после окончания работы в сети Интернет, а также после окончания работы обучающегося, вносит в журнал регистрации работы в сети Интернет данные о посещенных сайтах и цели работы в сети Интернет.

дата	ФИО сотрудника (ФИ учащегося)	Сайт, цель работы	подпись сотрудника

допускается распечатывание Истории браузера, в котором осуществлялась работа, которая заверяется подписью сотрудника, осуществляющего (контролирующего) работу в сети Интернет.

5.4. Не реже 2-х раз в год, либо по специальному распоряжению директора ОО все компьютеры проверяются комиссией в составе из не менее 3-х человек на соответствие требованиям безопасности с последующим составление акта.

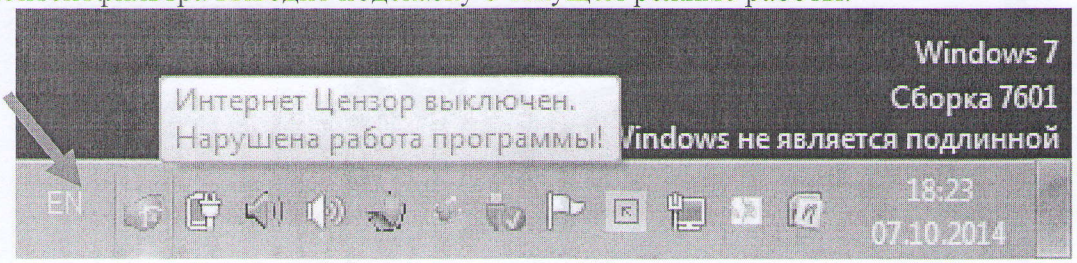
Часть II. Работа с Контент – фильтром

В образовательной организации используется Контент-фильтр «Интернетцензор», позволяющий эффективно защитить работу в сети Интернет от Нежелательной информации на основе белых списков. Доступ к сайтам в Интернет на основе белых списков базируется на принципе запрета всех сайтов, не входящих в доверенный проверенный список сайтов.

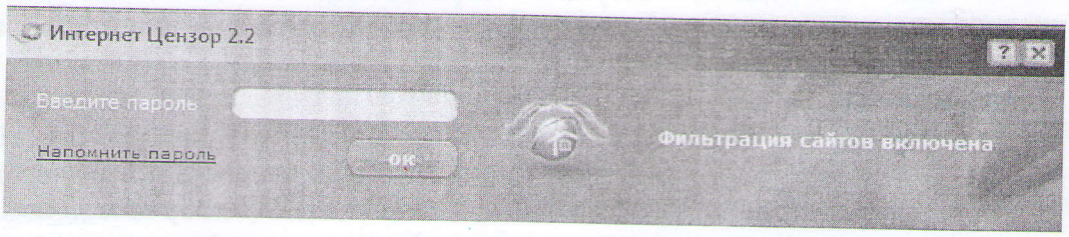
Основным (рабочим) режимом Контентфильтра является «Высокий уровень». Для удобства работы в Интернет уровень фильтрации может быть понижен либо отключен.

Запрещается удалять интернетцензор. Некорректное удаление программы влечёт за собой блокировку доступа к сайтам сети Интернет и невозможности настроить или отменить блокировку. Для настройки режима фильтрации есть все необходимые инструменты в самой программе фильтрации.

Работа с Интернетцензором осуществляется в програмном интерфейсе, вызываемом щелчком мыши по соответствующей иконке. Голубой цвет иконки свидетельствует о включенной фильтрации, красный – об отключенной. Наведение указателя мыши на значёк Контентфильтра выводит подсказку о текущем режиме работы.

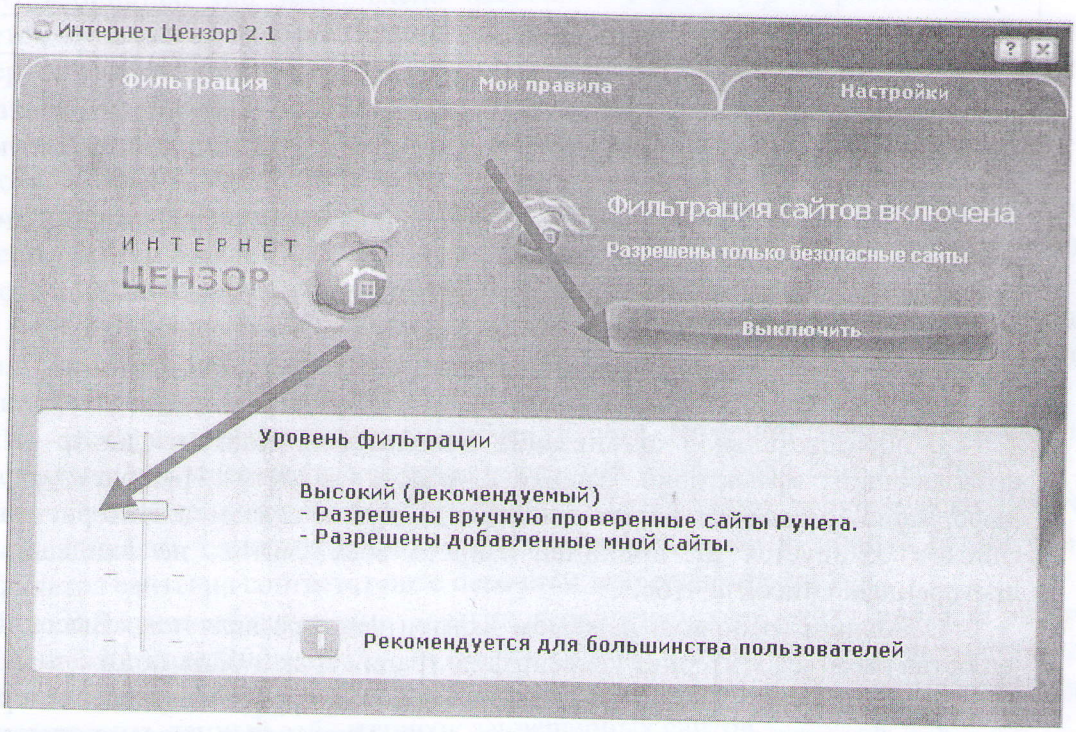


Для настройки режима работы Контент-фильра нужно щёлкнуть левой кнопкой мыши (ЛКМ) по значку Контент-фильтра. Откроется окно вода пароля для доступа к настройке программы, необходимо ввести действующий пароль (пароль контент-фильтра на вашем компьютере необходимо уточнить у Ответственного за контентную фильтрацию).



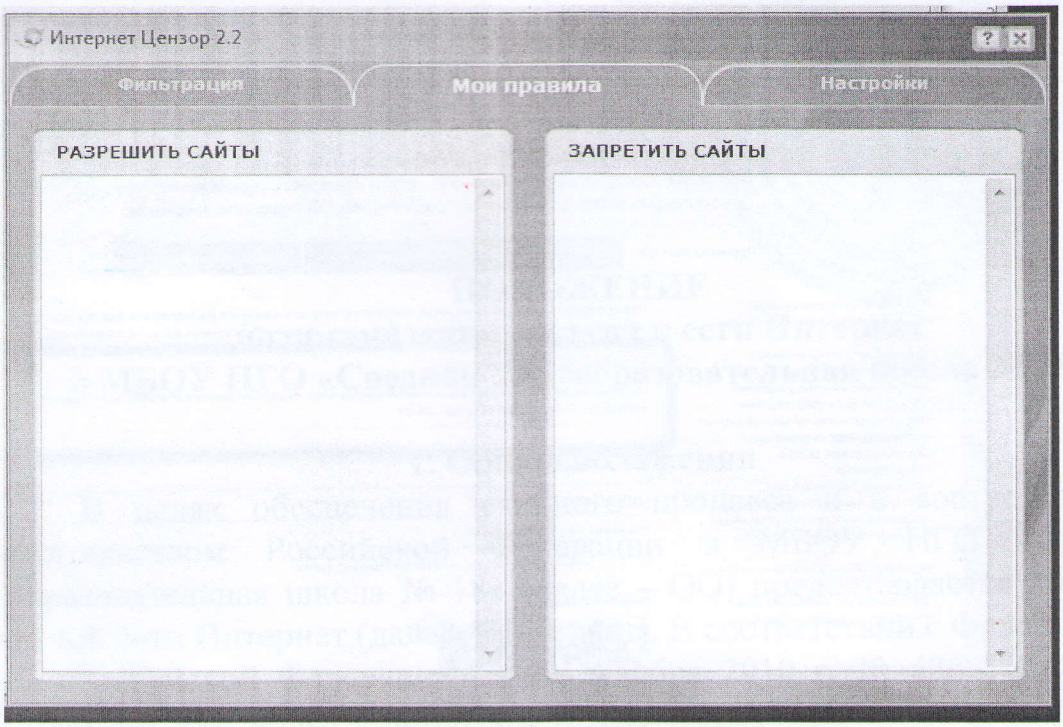
Если пароль верный, откроется окно настройки программы.

На первой вкладке можно совсем отключить фильтрацию, либо понизить уровень фильтрации (минимальная фильтрация соответствует самому нижнему положению ползунка)

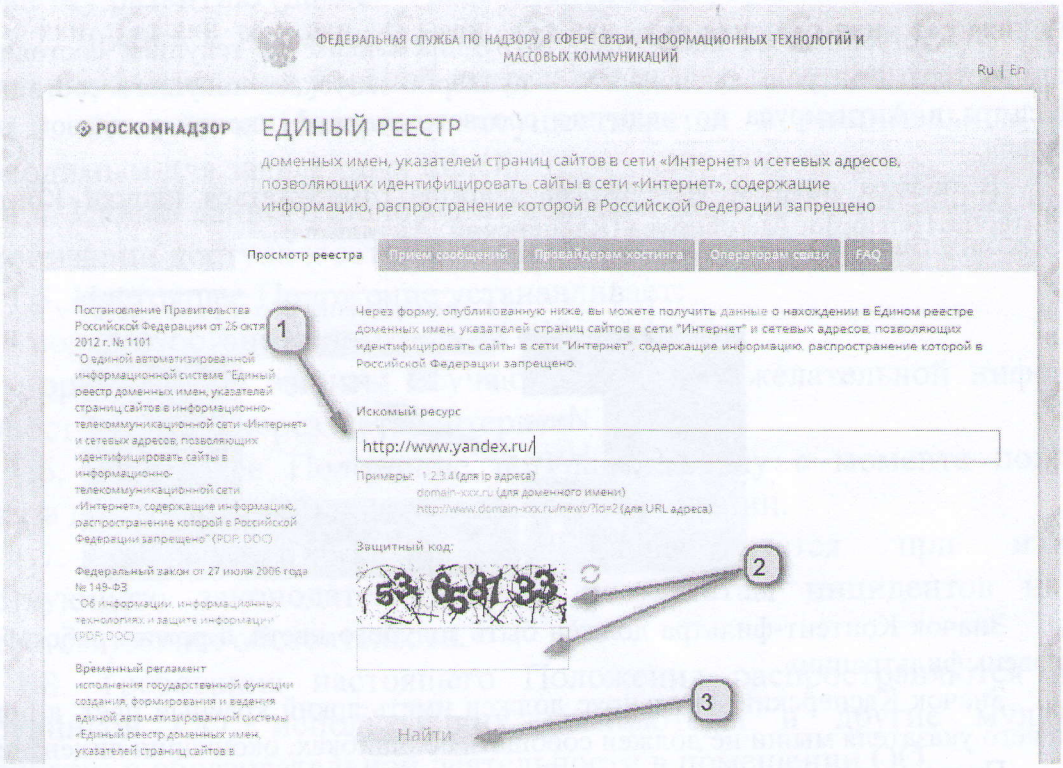


При отключении фильтрации, необходимо перезапустить браузер интернета (программа просмотра интернет сайтов).

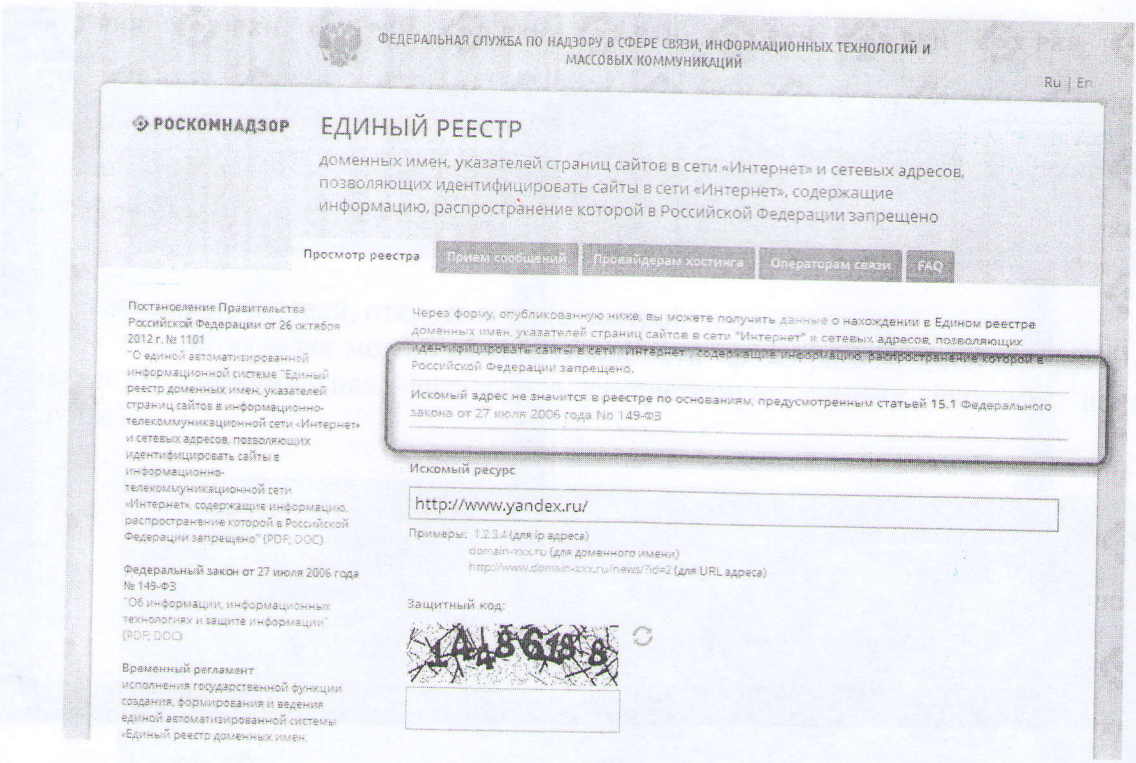
На вкладке «Мои правила» можно отдельно добавить сайты, к которым будет открыт или закрыт доступ соответственно. Просто добавляем адрес сайта в соответствующие списки.



При добавлении сайтов в раздел «Разрешённые сайты» (личный белый список) обязательно проверить добавляемый сайт на соответствие единому реестру запрещённых сайтов. Для этого нужно зайти на адрес реестра http://eais.rkn.gov.ru/ , и в форме указать адрес проверяемого сайта, после чего ввести код с картинки нажать кнопку «Найти».



Если искомый адрес не значится в реестре, то возможно его добавление в разрешённые сайты, в противном случае – запрещено.

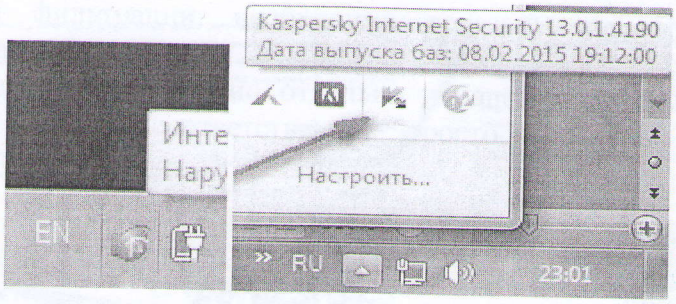


Запрещается менять пароли на Интернетцензор, и почту регистрации учётной записи.

Часть III. Проверка текущего состоянии защиты

Ответственный за компьютер сотрудник следит за текущим состоянием защиты компьютера. Контроль заключается в проверке запуска и текущего состояния Контент-фильтра и Антивируса по наличию соответствующих иконок в правом нижнем углу экрана.

В правом нижнем углу экрана должны отображаться иконки Контент-фильтра (ИнтернетЦензор) и Антивируса (Касперский Антивирус).



Значок Контент-фильтра должен быть голубого цвета, а режим работы – «Высокий уровень фильтрации».

Значок Касперский Антивирус должен иметь яркий красный цвет, а при наведении на него указателя мыши не должен сообщать об ошибках, окончании лицензии и т.п.

Проверка текущего состояния защиты должна проводиться при каждом включении компьютера.