

Утверждаю  
Ректор Российского исламского  
института

/Мухаметшин Р.М.

« 25 » мая 2020 г.

Частное учреждение высшего образования  
«Российский исламский институт»



## **Правила пользования компьютерным оборудованием и сетями Интернет на территории Российского исламского института (далее – РИИ)**

Данные правила были разработаны в соответствии с Федеральным законом от 29 декабря 2010 г. №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Федеральным законом от 29 декабря 2012 г. №273-ФЗ «Об образовании в Российской Федерации», Приказом Минкомсвязи России от 16 июня 2014 г. №161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию», Положением об использовании сети «Интернет» в ЧУВО «Российский исламский институт» (утвержден приказом ректора от 05 апреля 2017 года №159, в научно-образовательных целях в целях обеспечения реализации задач, направленных на ограничение доступа несовершеннолетних обучающихся к информации, причиняющей вред их здоровью и (или) развитию, а также не соответствующей задачам образования, в том числе распространяемой посредством информационно-телекоммуникационной сети «Интернет»

### **1. Организация доступа несовершеннолетних обучающихся к информационно-телекоммуникационной сети «Интернет»**

1.1. Самостоятельный доступ несовершеннолетних обучающихся в помещения Института, в которых установлены компьютеры, подключенные к сети «Интернет» допускается в присутствии преподавателей или ответственных работников.

1.2 Ответственность за допуск несовершеннолетних обучающихся к компьютерам, не используемым в учебном процессе, несут работники, которым компьютер был предоставлен Институтом для осуществления их должностных обязанностей.

1.3 Несовершеннолетним обучающимся доступ к беспроводной сети Wi-Fi РИИ не предоставляется. Работникам института запрещается передавать пароли доступа к сети WiFi несовершеннолетним обучающимся.

1.4 Доступ несовершеннолетних обучающихся к сети «Интернет» из компьютерных классов, для всех компьютеров в классе ограничивается системой веб контроль антивируса Касперский, с применением настроенных фильтров для ВУЗа. См. приложение №1. Доступ к настройкам антивируса защищен паролем.

1.5 Во время доступа несовершеннолетних обучающихся к информационно-телекоммуникационной сети «Интернет» вне учебных занятий, в том числе при выполнении самостоятельной работы в помещениях, предназначенных для самостоятельной работы, контроль использования ресурсов информационно-телекоммуникационной сети «Интернет» осуществляют следующие работники Института:

в компьютерных классах – работник, отвечающий за эксплуатацию информационных систем, сетей и компьютерной техники;

в читальных залах библиотеки Института доступ в интернет через авторизацию и персональный пароль. Контроль осуществляет – работник библиотеки;

в аудиториях для самостоятельной работы – работник, назначенный проректором по воспитательной работе.

Разработано:

Начальник отдела информатизации



Сайфутдинов М.Х.

Согласовано:

Проректор по учебной работе



Гильманов М.Р.

Проректор по общим вопросам



Галеев Н.Р.

## **ВЕБ-КОНТРОЛЬ**

Веб-Контроль управляет доступом пользователей к веб-ресурсам. Это позволяет уменьшить расход трафика и сократить нецелевое использование рабочего времени.

При попытке пользователя открыть веб-сайт, доступ к которому ограничен Веб-Контролем, Kaspersky Endpoint Security выполнит следующие действия:

- для HTTP-трафика, заблокирует доступ или покажет предупреждение (см. рис. ниже);
- для HTTPS-трафика, заблокирует доступ без описания проблемы (стандартное окно браузера об ошибке открытия страницы).

### **Способы управления доступом к веб-сайтам**

Веб-Контроль позволяет настраивать доступ к веб-сайтам следующими способами:

- **Категория веб-сайта.** Категоризацию веб-сайтов обеспечивает облачная служба Kaspersky Security Network, эвристический анализ, а также база известных веб-сайтов (входит в состав баз программы). Вы можете ограничить доступ пользователей, например, к категории "Социальные сети" или другим категориям.

- **Тип данных.** Вы можете ограничить доступ пользователей к данным на веб-сайте и, например, скрыть графические изображения. Kaspersky Endpoint Security определяет тип данных по формату файла, а не по расширению.

- **Отдельный адрес.** Вы можете ввести веб-адрес или использовать маски.

Вы можете использовать одновременно несколько способов регулирования доступа к веб-сайтам. Например, вы можете ограничить доступ к типу данных "Файлы офисных программ" только для категории веб-сайтов "Веб-почта".

### **Правила доступа к веб-сайтам**

Веб-Контроль управляет доступом пользователей к веб-сайтам с помощью *правил доступа*. Вы можете настроить следующие дополнительные



параметры правила доступа к веб-сайтам:

- Пользователи, на которых распространяется правило.

Например, вы можете ограничить доступ в интернет через браузер для всех пользователей организации, кроме IT-отдела.

- Расписание работы правила.

Например, вы можете ограничить доступ в интернет через браузер только в рабочее время.

### **Категории содержания веб-ресурсов**

Категории содержания веб-ресурсов (далее также "категории") в приведенном ниже списке подобраны таким образом, чтобы максимально полно описать блоки информации, размещенные на веб-ресурсах, с учетом их функциональных и тематических особенностей. Порядок категорий в списке не отражает относительной важности или распространенности категорий в сети Интернет. Названия категорий являются условными и используются лишь для целей программ и веб-сайтов "Лаборатории Касперского". Названия не обязательно соответствуют значению, которое им придает применимое законодательство. Один веб-ресурс может относиться к нескольким категориям одновременно.

#### **Для взрослых**

В общем определении категория включает в себя веб-ресурсы, относящиеся к сексуальной стороне человеческих отношений, философий, секс магазинов и т.д. Это может быть содержимое в любом формате и виде.

#### **Алкоголь, табак, наркотики и психотропы**

В общем определении категория включает в себя веб ресурсы, на которых есть упоминание алкоголя, наркотиков, табака в любых видах, в том числе рекламные, исторические, медицинские и обучающие ресурсы. А также веб ресурсы, где описаны или продаются приспособления для употребления указанных веществ.

#### **Насилие**

Данная категория включает веб-ресурсы, содержащие фото-, видео- и текстовые материалы, описывающие акты физического или психического насилия

над людьми, а также жестокого отношения к животным как цель существования этого контента.

### **Нецензурная лексика**

Категория включает веб-ресурсы, на которых обнаружены элементы нецензурной брани.

### **Оружие, взрывчатые вещества, пиротехника**

Данная категория включает веб-ресурсы, содержащие информацию об оружии, взрывчатых веществах и пиротехнической продукции.

### **Поиск работы**

Данная категория включает веб-ресурсы, предназначенные для установления контактов между работодателем и соискателем работы. К ним в частности относятся:

- Веб-сайты кадровых агентств (агентств по трудоустройству и/или агентств по подбору персонала).
- Веб-страницы работодателей, содержащие описание имеющихся вакансий и их преимуществ.
- Независимые порталы, содержащие предложения трудоустройства от работодателей и кадровых агентств.
- Социальные сети профессионального характера, которые в том числе позволяют размещать/находить данные о специалистах, которые не находятся в активном поиске работы.

### **Средства анонимного доступа**

Данная категория включает веб-ресурсы, выступающие в роли посредника для загрузки контента прочих веб-ресурсов с помощью специальных веб-приложений для:

- обхода ограничений администратора локальной сети на доступ к веб-адресам или IP-адресам;
- анонимного доступа к веб-ресурсам, в том числе к веб-ресурсам, которые преднамеренно не принимают HTTP-запросы с определённых IP-адресов или их групп (например, по стране происхождения).

### **Программное обеспечение, аудио, видео**

В общем определении категория включает в себя веб-ресурсы, предоставляющие возможность скачивания соответствующих файлов.

- **Торренты**

Торрент трекеры и веб ресурсы, помогающие организовать их работу.

- **Файловые обменники**

Веб-ресурсы, предоставляющие возможность обмена файлами.

- **Аудио, видео**

Веб-ресурсы, с которых можно загрузить или просмотреть/прослушать аудио или видео файлы.

**Азартные игры, лотереи, тотализаторы**

Категория охватывает веб-ресурсы, содержащие:

- Азартные игры, предусматривающие денежные взносы за участие.

- Тотализаторы, предусматривающие денежные ставки.

- Лотереи, предусматривающие приобретение лотерейных билетов/номеров.

**Общение в сети**

В общем определении категория включает в себя веб-ресурсы, позволяющие тем или иным пользователям (зарегистрированным или нет) отправлять персональные сообщения другим пользователям. Существует ряд веб-ресурсов рассчитанных на общение.

- **Веб-почта**

Веб-почта - исключительно страницы авторизации в почтовом сервисе и страницы почтового ящика, содержащего почтовые сообщения и сопутствующие данные (например, личные контакты). Для остальных веб-страниц интернет-провайдера, предлагающего почтовый сервис, данная категория не назначается.

- **Социальные сети**

Социальные сети – веб-сайты, предназначенные для построения, отражения и организации контактов между людьми, организациями, государством, требующие в качестве условия участия регистрацию учётной записи пользователя.

- **Чаты, форумы**

В данную категорию следует относить веб-чаты, а также веб-ресурсы, предназначенные для распространения и поддержки приложений для мгновенного обмена сообщениями, предоставляющих возможность коммуникации в реальном времени. А также форумы – специальные веб сервисы для публичного обсуждения различных тем с сохранением переписки.

- **Блоги**

Блоги – веб-ресурсы, предназначенные для публичного обсуждения различных тем с помощью специальных веб-приложений, включая блог-платформы (веб-сайты, предоставляющие платные или бесплатные услуги по созданию и обслуживанию блогов).

- **Сайты знакомств**

Веб ресурсы знакомств, которые помогают организовать знакомства между людьми, в том числе без сексуального подтекста.

Интернет-магазины, банки, платежные системы

В общем определении категория включает в себя веб-ресурсы, предназначенные для проведения любых операций с безналичными денежными средствами в режиме онлайн с помощью специальных веб-приложений. А также веб ресурсы, помогающие снять, сдать, купить или продать недвижимость.

- **Интернет-магазины**

Интернет-магазины и интернет-аукционы, предназначенные для реализации любых товаров, работ или услуг физическим и/или юридическим лицам, в том числе как веб-сайты магазинов, осуществляющих реализацию исключительно в интернете, так и интернет-представительства обычных магазинов, характерной особенностью которых является возможность оплаты в режиме онлайн.

- **Банки**

Веб-ресурсы банков.

- **Платежные системы**

К данной категории относятся следующие веб страницы:

- Специальные веб-страницы банков, предусматривающие услуги интернет-банкинга, включающие безналичные (электронные) переводы между

банковскими счетами, открытие банковских вкладов, конвертацию денежных средств, оплату услуг сторонних организаций и т.д.

- Веб-страницы электронных платёжных систем, предоставляющие доступ к персональной учётной записи пользователя.

- **Криптовалюты и майнинг**

Подкатегория включает веб-сайты, предоставляющие сервисы покупки и продажи криптовалют, сервисы информирования о криптовалютах и майнинге.

**Компьютерные игры**

Данная категория включает веб-ресурсы, посвящённые компьютерным играм разнообразных жанров. А также игровые сообщества и сервисы.

**Религии, религиозные объединения**

Данная категория включает веб-ресурсы, содержащие материалы об общественных течениях (движениях), объединениях (сообществах) и организациях, подразумевающих наличие религиозной идеологии и/или культа в любых проявлениях.

**Новостные ресурсы**

Новостные порталы на любые темы, в том числе социальные новости агрегаторы новостей, rss рассылки.

**Баннеры**

Категория включает веб-ресурсы, содержащие баннеры. Рекламная информация на баннерах может отвлекать пользователей от дел, а загрузка баннеров увеличивает объем трафика.

**Региональные ограничения законодательства**

- Запрещено законодательством Российской Федерации
- Запрещено законодательством Бельгии
- Запрещено полицией Японии

Веб-ресурсы, предоставляемые по соглашению с японской полицией, только для продуктов японского рынка.

**Действия с правилами доступа к веб-ресурсам**

Правило доступа к веб-ресурсам представляет собой набор фильтров и действие, которое Kaspersky Endpoint Security выполняет при посещении



пользователями описанных в правиле веб-ресурсов в указанное в расписании работы правила время. Фильтры позволяют точно задать круг веб-ресурсов, доступ к которым контролирует компонент Веб-Контроль.

Доступны следующие фильтры:

- **Фильтр по содержанию.** Веб-Контроль разделяет веб-ресурсы по категориям содержания и категориям типа данных. Вы можете контролировать доступ пользователей к размещенным на веб-ресурсах данным, относящимся к определенными этими категориями типам данных. При посещении пользователями веб-ресурсов, которые относятся к выбранной категории содержания и / или категории типа данных, Kaspersky Endpoint Security выполняет действие, указанное в правиле.

- **Фильтр по адресам веб-ресурсов.** Вы можете контролировать доступ пользователей ко всем адресам веб-ресурсов или к отдельным адресам веб-ресурсов и / или группам адресов веб-ресурсов.

Если задан и фильтр по содержанию, и фильтр по адресам веб-ресурсов, и заданные адреса веб-ресурсов и / или группы адресов веб-ресурсов принадлежат к выбранным категориям содержания или категориям типа данных, Kaspersky Endpoint Security контролирует доступ не ко всем веб-ресурсам выбранных категорий содержания и / или категорий типа данных, а только к заданным адресам веб-ресурсов и / или группам адресов веб-ресурсов.

- **Фильтр по именам пользователей и групп пользователей.** Вы можете задавать пользователей и / или группы пользователей, для которых контролируется доступ к веб-ресурсам в соответствии с правилом.

- **Расписание работы правила.** Вы можете задавать расписание работы правила. Расписание работы правила определяет время, когда Kaspersky Endpoint Security контролирует доступ к веб-ресурсам, указанным в правиле.

После установки программы Kaspersky Endpoint Security список правил компонента Веб-Контроль не пуст. Предусмотрены два правила:

- Правило "Сценарии и таблицы стилей", которое разрешает всем пользователям в любое время доступ к веб-ресурсам, адреса которых содержат

названия файлов с расширением css, js, vbs. Например: <http://www.example.com/style.css>, <http://www.example.com/style.css?mode=normal>.

- "Правило по умолчанию". Это правило в зависимости от выбранного действия разрешает или запрещает всем пользователям доступ ко всем веб-ресурсам, которые не попадают под действие других правил.

### **Мониторинг активности пользователей в интернете**

Kaspersky Endpoint Security позволяет записывать данные о посещении пользователями всех веб-сайтов, в том числе и разрешенных. Таким образом, вы можете получить полную историю просмотров в браузере. Kaspersky Endpoint Security отправляет события активности пользователя в Kaspersky Security Center, локальный журнал Kaspersky Endpoint Security, журнал событий Windows. Для получения событий в Kaspersky Security Center нужно настроить параметры событий в политике в Консоли администрирования или Web Console. Также вы можете настроить отправку событий Веб-Контроля по электронной почте и отображение уведомлений на экране компьютера пользователя.

Kaspersky Endpoint Security создает следующие события активности пользователя в интернете:

- блокировка веб-сайта (статус *Критические события* 🚫);
- предупреждение о нежелательном веб-сайте (статус *Предупреждения* ⚠️);
- посещение разрешенного веб-сайта (статус *Информационные сообщения* 😊).

Изменение шаблонов сообщений Веб-Контроля