



ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
(РОСАВИАЦИЯ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ» (МГТУ ГА)



**ЕГОРЬЕВСКИЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ КОЛЛЕДЖ
ИМЕНИ В.П. ЧКАЛОВА – ФИЛИАЛ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО
БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО
ОБРАЗОВАНИЯ «МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ» (МГТУ ГА)**

П Р И К А З

г. Егорьевск

№ 84

29.04.2021

«Об организации системы ограничения обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования»

В соответствии с Федеральным законом Российской Федерации от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации», Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральным законом от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и (или) развитию», приказом Министерства связи и массовых коммуникаций Российской Федерации от 16.06.2014 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», Методическими рекомендациями, направленными Минобрнауки России письмом от 28.04.2014 № ДЛ-115/03, и Методическими рекомендациями, направленными Минпросвещения Российской Федерации письмом от 07.06.2019 № 04-474, в целях защиты учащихся от информации, наносящей вред их здоровью и (или) развитию.

Утвердить:

1. Акт проверки системы контентной фильтрации (далее - СКФ) в образовательной организации (приложение №1);
2. Журнал работы СКФ (приложение №2);
3. Журнал регистрации случаев обнаружения обращений к сайтам,

содержащим информацию, причиняющую вред здоровью и (или) развитию детей, а также не соответствующей задачам образования (приложение №3);

4. Порядок проведения проверки эффективности использования системы контентной фильтрации интернет- ресурсов в Егорьевском АТК имени В.П.Чкалова – филиале МГТУ ГА(приложение №4);

5. Правила использования сети Интернет в Егорьевском АТК имени В.П.Чкалова – филиале МГТУ ГА (приложение №5);

6. План мероприятий по обеспечению информационной безопасности обучающихся (приложение № 7);

7. Основные настройки групповой политики, для настройки параметров компьютера и пользователя, а так же к учетным записям локальных пользователей. (приложение №8).

Отделу кадров внести изменения в должностные инструкции педагогических работников об ограничении доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования (приложение №6);

Директор



Шмельков А.В.

**Акт проверки контентной фильтрации
в Егорьевском АТК имени В.П.Чкалова – филиале МГТУ ГА**

№ _____

_____ (дата)

_____ (номер)

1. Общие сведения

Показатель	Значение
Количество компьютерных классов	
Общее количество компьютеров	
Количество компьютеров в локальной сети	
Количество компьютеров, подключенных к сети интернет	
Провайдер	
Скорость передачи данных	

2. Информация о контент-фильтре

Действия, необходимые для обеспечения контентной фильтрации интернет-ресурсов	Выполнение (да/нет)
Установлен контент-фильтр	
Название контент-фильтра	
Контент-фильтр работает на всех компьютерах, где есть доступ в сеть интернет	

3. Результаты проверки работы системы контентной фильтрации

Категории запрещенной информации в образовательной организации	Возможность доступа (да/нет)
Перечень видов информации, запрещенной к распространению посредством сети интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования согласно Методическим рекомендациям по ограничению 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	
Интернет-ресурсы, не включенные в Реестр безопасных образовательных сайтов	

Ответственный за информационную безопасность от информации, причиняющей вред их здоровью и (или) развитию.

_____ (подпись)

_____ (Ф. И. О.)

Журнал регистрации случаев обнаружения обращений к сайтам, содержащим информацию, причиняющую вред здоровью и (или) развитию детей, а также не соответствующей задачам образования

Дата обнаружения	
Должность и Ф.И.О. ответственного	
Номер компьютера	
Описание сайта в сети «Интернет», содержащего информацию, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования: Принятые меры	

« ___ » _____ 20__ г.

_____ Должность

_____ Подпись

_____ ФИО

Дата обнаружения	
Должность и Ф.И.О. ответственного	
Номер компьютера	
Описание сайта в сети «Интернет», содержащего информацию, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования: Принятые меры	

« ___ » _____ 20__ г.

_____ Должность

_____ Подпись

_____ ФИО

Порядок проведения проверки эффективности использования системы контентной фильтрации интернет-ресурсов в Егорьевском АТК имени В.П.Чкалова – филиале МГТУ ГА

1. Общие положения

1.1. Порядок проведения проверки эффективности использования системы контентной фильтрации интернет-ресурсов (далее – Порядок) определяет процедуру проверки работы системы контентной фильтрации в Егорьевском АТК имени В.П.Чкалова – филиале МГТУ ГА (далее – образовательная организация).

1.2. Порядок разработан в соответствии с Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Методическими рекомендациями по ограничению 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, утвержденными Минкомсвязи 16.05.2019, и использует терминологию, которая введена ранее перечисленными правовыми актами.

2. Порядок проверки системы контентной фильтрации

2.1. Проверку эффективности использования систем контентной фильтрации интернет-ресурсов в Егорьевском АТК имени В.П.Чкалова – филиале МГТУ ГА проводит ответственный за информационную безопасность от информации, причиняющей вред их здоровью и (или) развитию в течение учебного года не реже 1 раза в 3 месяца.

2.2. Ответственный за информационную безопасность от информации, причиняющей вред их здоровью и (или) развитию проверяет работоспособность системы контентной фильтрации на всех закрепленных за ним компьютерах организации путем ввода в поле поиска любого браузера ключевые слова из списка информации, запрещенной для просмотра обучающимися, с последующими попытками загрузки сайтов из найденных. В том числе ответственный за информационную безопасность проверяет, загружается ли информация, причиняющая вред здоровью и развитию детей, не имеющая отношения к образовательному процессу, в социальных сетях: Вконтакте, Одноклассники, Твиттер, Фейсбук, Инстаграм, Живой Журнал (livejournal.com) и др.

2.3. Чтобы провести проверку, ответственный за информационную безопасность от информации, причиняющей вред их здоровью и (или) развитию выбирает три–четыре ресурса с информацией, причиняющей вред

здоровью и (или) развитию детей, а также не соответствующей задачам образования, в том числе ищет информационную продукцию, запрещенную для детей, в форме сайтов, графических изображений, аудиовизуальных произведений и других форм информационной продукции.

2.4. В качестве проверочных ресурсов ответственный за информационную безопасность от информации, причиняющей вред их здоровью и (или) развитию использует сайты в том числе из списка экстремистских материалов – <https://minjust.gov.ru/ru/extremist-materials/>.

2.4.1. Ответственный за информационную безопасность от информации, причиняющей вред их здоровью и (или) развитию вносит название материала (части материала, адрес сайта) в поисковую строку браузера. Из предложенного списка адресов переходит на страницу сайта, содержащего негативный контент.

2.4.2. Если материал отображается и с ним можно ознакомиться без дополнительных условий, ответственный за информационную от информации, причиняющей вред их здоровью и (или) развитию безопасность фиксирует факт нарушения работы системы контентной фильтрации.

2.4.3. Если ресурс требует дополнительных действий (регистрации, условного скачивания, переадресации и т. д.), при выполнении которых материал отображается, ответственный за информационную безопасность от информации, причиняющей вред их здоровью и (или) развитию также фиксирует факт нарушения работы системы контентной фильтрации.

2.4.4. Если невозможно ознакомиться с негативным контентом при выполнении дополнительных условий (регистрации, скачивания материалов, переадресации и т. д.), нарушение не фиксируется.

2.5. Ответственный за информационную безопасность от информации, причиняющей вред их здоровью и (или) развитию составляет три–четыре запроса в поисковой строке браузера, состоящих из слов, которые могут однозначно привести на запрещенные для несовершеннолетних ресурсы, например по темам: экстремизм, проявление жестокости, порнография, терроризм, суицид, насилие и т. д. К примеру, вводятся фразы «изготовление зажигательной бомбы», «издевательства над несовершеннолетними», «способы суицида».

2.5.1. Из предложенного поисковой системой списка адресов ответственный за информационную безопасность от информации, причиняющей вред их здоровью и (или) развитию переходит на страницу двух–трех сайтов и знакомится с полученными материалами.

2.5.2. Ответственный за информационную безопасность от информации, причиняющей вред их здоровью и (или) развитию дает оценку материалам на предмет возможного нанесения ущерба физическому и психическому здоровью обучающихся.

2.5.3. Если обнаруженный материал входит в перечень запрещенной для детей информации (Приложение № 1 к Методическим рекомендациям по ограничению 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, утв. Минкомсвязи 16.05.2019), ответственный за информационную безопасность от информации, причиняющей вред их здоровью и (или) развитию фиксирует факт нарушения с указанием источника и критериев оценки.

2.6. По итогам мониторинга ответственный за информационную безопасность от информации, причиняющей вред их здоровью и (или) развитию оформляет акт проверки контентной фильтрации в образовательной организации по форме из приложения к Порядку.

2.7. Если ответственный за информационную безопасность от информации, причиняющей вред их здоровью и (или) развитию выявил сайты, которые не входят в Реестр безопасных образовательных сайтов, то перечисляет их в акте проверки контентной фильтрации в образовательной организации.

2.8. При выявлении компьютеров, подключенных к сети интернет и не имеющих системы контентной фильтрации, производится следующее действие:

– немедленное программное и/или физическое отключение доступа к сети интернет на выявленных компьютерах и направление запроса на установку и настройку системы контентной фильтрации в вычислительный центр.

Правила использования сети Интернет в Егорьевском АТК имени В.П.Чкалова – филиале МГТУ ГА

1. Общие положения

1.1. Настоящие Правила регулируют условия и порядок использования сети Интернет обучающимися, педагогическими работниками и другими сотрудниками Егорьевского АТК имени В.П.Чкалова– филиала МГТУ ГА (далее – колледж).

1.2. Правила имеют статус локального нормативного акта колледжа. Если нормами действующего законодательства РФ предусмотрены иные требования, чем настоящими Правилами, применяются нормы действующего законодательства РФ.

1.3. Использование сети Интернет в колледже подчинено следующим принципам:

- соответствие образовательным целям;
- способствование гармоничному формированию и развитию личности;
- уважение закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей Интернет;
- приобретение новых навыков и знаний;
- расширение применяемого спектра учебных и наглядных пособий;
- социализация личности, введение в информационное общество.

2. Политика использования сети Интернет в колледже

2.1. Использование сети Интернет в колледже возможно исключительно при условии ознакомления и согласия лица, пользующегося сетью Интернет в колледже, с настоящими Правилами.

2.2. Факт подтверждающий ознакомления и согласия удостоверяются подписью лица в журнале инструктажа на рабочем месте.

2.3. Во время занятий контроль за использованием обучающимися сети Интернет в соответствии с Правилами осуществляет преподаватель, ведущий занятие.

Преподаватель:

- наблюдает за использованием компьютера и сети Интернет обучающимися;
- запрещает дальнейшую работу обучающегося, в сети Интернет в случае нарушения настоящих Правил и иных нормативных документов, регламентирующих использование сети Интернет в колледже;

- принимает предусмотренные Правилами и иными нормативными документами меры для пресечения дальнейших попыток доступа к ресурсу / группе ресурсов, не совместимых с задачами образования.

2.4. Во время использования сети Интернет для свободной работы контроль осуществляет преподаватель, мастер производственного обучения, воспитатель и классный руководитель:

- определяет время и место для свободной работы в сети Интернет обучающихся, педагогических и других работников колледжа с учетом использования соответствующих технических мощностей колледжа в образовательном процессе, а также длительность сеанса работы одного человека;
- наблюдает за использованием компьютера и сети Интернет обучающимися;
- запрещает дальнейшую работу обучающегося в сети Интернет в случае нарушения настоящих Правил и иных нормативных документов, регламентирующих использование сети Интернет в колледже;
- не допускает обучающегося к работе в сети Интернет в предусмотренных Правилами случаях;
- принимает предусмотренные Правилами и иными нормативными документами меры для пресечения дальнейших попыток доступа к ресурсу / группе ресурсов, не совместимых с задачами образования.

2.5. При использовании сети Интернет в колледже осуществляется доступ только к ресурсам, содержание которых не противоречит законодательству РФ и не является несовместимым с целями и задачами образования и воспитания.

Проверка такого соответствия осуществляется с помощью специальных технических средств и программного обеспечения контентного ограничения доступа, установленного в колледже или предоставленного оператором услуг связи.

Пользователи сети Интернет в колледже понимают, что технические средства и программное обеспечение не могут осуществлять полную фильтрацию ресурсов сети Интернет в связи с частотой обновления ресурсов и осознают возможную опасность столкновения с ресурсом, содержание которого противоречит законодательству РФ и является несовместимым с целями и задачами образовательного процесса.

2.6. Решение о политике доступа к ресурсам / группам ресурсов сети Интернет принимает ответственное лицо за информационную безопасность самостоятельно либо с участием внешних экспертов, в качестве которых могут привлекаться:

- педагогические работники колледжа и других учреждений;
- лица, имеющие специальные знания либо опыт работы в рассматриваемой области;

- представители органов управления образованием;
- родители обучающихся, воспитанников.

При принятии решения ответственное лицо за информационную безопасность руководствуются:

- законодательством РФ;
- специальными познаниями, в т. ч. полученными в результате профессиональной деятельности;
- опытом организации образовательного процесса с использованием информационных технологий и возможностей сети Интернет;
- интересами обучающихся, воспитанников, целями образовательного процесса;
- рекомендациями профильных органов и организаций в сфере классификации ресурсов сети Интернет.

2.7. Отнесение определенных категорий и / или ресурсов в соответствующие группы, доступ к которым регулируется техническими средствами и программным обеспечением контентного технического ограничения доступа к информации, технически осуществляется ответственным лицом за информационную безопасность.

2.8. Категории ресурсов, в соответствии с которыми определяется политика использования сети Интернет в колледже, и доступ к которым регулируется техническими средствами и программным обеспечением контекстного технического ограничения доступа к информации, определяются в установленном порядке.

2.9. Принципами размещения информации на Интернет-ресурсах колледжа являются:

- соблюдение действующего законодательства РФ, интересов и прав граждан;
- защита персональных данных обучающихся, педагогических работников и других сотрудников;
- достоверность и корректность информации.

3. Процедура использования сети Интернет

3.1. Использование сети Интернет в колледже осуществляется в целях образовательного процесса. В рамках развития личности, ее социализации и получения знаний в области сети Интернет и компьютерной грамотности лицо может осуществлять доступ к ресурсам необразовательной направленности.

3.2. Обучающемуся запрещается:

- находиться на ресурсах, содержание и тематика которых является недопустимой для несовершеннолетних и / или нарушающей законодательство РФ (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т. п. розни, иные ресурсы схожей направленности);

- осуществлять любые сделки через Интернет;
- осуществлять загрузку файлов на компьютер колледжа без разрешения;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

3.3. При случайном обнаружении лицом, работающим в сети Интернет, ресурса, содержимое которого не совместимо с целями образовательного процесса, он обязан незамедлительно сообщить о нем ответственному лицу за информационную безопасность с указанием интернет-адреса (URL) и покинуть данный ресурс.

3.6. Ответственное лицо за информационную безопасность обязан:

- принять сообщение лица, работающего в сети Интернет;
- оценить ресурс и принять решение по политике доступа к нему;

Передаваемая информация должна содержать:

- интернет-адрес (URL) ресурса;
- тематику ресурса, предположения о нарушении ресурсом законодательства РФ либо несовместимости с задачами образовательного процесса;
- дату и время обнаружения;
- информацию об установленных в колледже технических средствах технического ограничения доступа к информации.

Формулировки для внесения изменений в должностные инструкции педагогических работников Егорьевского АТК имени В.П.Чкалова– филиала МГТУ ГА

Педагогический работник

1. Общие положения

Должен знать:

- дидактические возможности использования ресурсов сети Интернет;
- правила использования сети Интернет в колледже.
- методические рекомендации по ограничению 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.

2. Должностные обязанности:

- планирует использование ресурсов сети Интернет в учебном процессе с учетом специфики преподаваемого предмета;
- использует разнообразные приемы, методы и средства обучения, в том числе по индивидуальным учебным планам в рамках федеральных государственных образовательных стандартов, современные образовательные технологии и сайты в сети «Интернет»;
- систематически повышает свою профессиональную квалификацию по направлению «Безопасное использование сайтов в сети «Интернет» в образовательном процессе в целях обучения и воспитания обучающихся в образовательной организации»;
- осуществляет контрольно-оценочную деятельность в образовательном процессе с использованием современных способов оценивания в условиях информационно - коммуникационных технологий;

3. Права

Вправе использовать в своей работе сайты сети «Интернет», не наносящие вред здоровью и (или) развитию детей, а также соответствующие задачам образования.

4. Ответственность

Несет ответственность за организацию доступа к сети «Интернет» в своих кабинетах и ограничение доступа обучающихся к видам информации, распространяемой посредством сети «Интернет» причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в ходе учебного процесса.

План мероприятий по обеспечению информационной безопасности обучающихся

п/п	Мероприятие	Сроки
1.	Изучение нормативно-правовой базы, методических рекомендаций и издание (актуализация) организационно-распорядительных документов по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет	Июнь - август
2.	Настройка (установка) технических средств, применяемых при организации доступа к сети Интернет (компьютерное оборудование, сетевое оборудование, системное и прикладное программное обеспечение) в соответствии с требованиями методических рекомендаций по ограничению 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,	Июнь - август
4.	Установка, конфигурация, настройка режимов работы технических средств контентной фильтрации	Июнь - август
5.	Ознакомление работников образовательной организации с методическими рекомендациями по ограничению в образовательных учреждениях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, и локальных нормативных актов образовательной организации по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет	Август
6.	Информирование работников образовательной организации, обучающихся и их родителей (законных представителей) об ответственности за нарушение требований законодательства Российской Федерации и организационно-распорядительных документов образовательной организации по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет	Август - сентябрь
7.	Информирование родителей (законных представителей) обучающихся о существующих угрозах в сети Интернет, о методах и способах защиты детей от информации, причиняющей вред здоровью и (или) развитию детей	Сентябрь - октябрь

8.	Проведение периодического контроля состояния системы обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет	Не реже 1 раза в 3 месяца
9.	Организация преподавания обучающимся основ информационной безопасности в рамках реализации образовательной программы образовательных организаций в соответствии методическими рекомендациями по основам информационной безопасности для обучающихся общеобразовательных организаций с учётом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности	В течение учебного года
10.	Проведение Единого урока по безопасности в сети «Интернет»	Октябрь
11.	Проведение серии мероприятий проекта «Сетевичок» для обучающихся	Октябрь - ноябрь
12.	Участие в проектах информационного сообщества по информационной безопасности	В течении года
13.	Ведение локальных нормативных актов образовательной организации в области информационной безопасности обучающихся	В течение учебного года
14.	Обновление материалов по информационной безопасности на информационных стендах.	В течение учебного года
15.	Размещение на официальном сайте образовательной организации информации по вопросам обеспечения информационной безопасности детей	В течении учебного года

Основные настройки групповой политики, для настройки параметров компьютера и пользователя, а так же к учетным записям локальных пользователей

1. Включение полноэкранный режим Включена
2. Включить рекомендуемые сайты Включена
3. Включить фильтрацию ActiveX Включена
4. Выключить возможность закрепления сайтов в Internet Explorer на рабочем столе Включена
5. Выполнять эти программы при входе в систему Включена
6. Задать действие по умолчанию для новой вкладки Включена
7. Запрет доступа к странице about:flags в Microsoft Edge Включена
8. Запрет изменения фона главного меню Включена Нет
9. Запретить игнорирование сообщений SmartScreen Защитника Windows о сайтах Включена
10. Запретить игнорирование сообщений SmartScreen Защитника Windows о файлах Включена
11. Запретить игнорирование сообщений функции "SmartScreen Защитника Windows" о сайтах Включена
12. Запретить изменение избранного в Microsoft Edge Включена
13. Запретить изменение изображения экрана блокировки и экрана входа в систему Включена
14. Запретить настройку создания новых вкладок Включена
15. Запретить переопределение ошибок сертификата Включена
16. Запретить удаленное управление рабочим столом Включена
17. Запретить установку съемных устройств Включена
18. Зоны безопасности: запретить пользователям добавлять и удалять вебсайты Включена
19. Компакт-диски и DVD-диски: Запретить выполнение Включена
20. Компакт-диски и DVD-диски: Запретить запись Включена
21. Компакт-диски и DVD-диски: Запретить чтение Включена
22. Настроить блокирование всплывающих окон Включена
23. Настроить начальные страницы Включена
24. Настроить режим терминала Включена
25. Настроить список сайтов в режиме предприятия Включена
26. Настройка кнопки "Домой" Включена
27. Настройка открытия в новом окне Microsoft Edge Включена
28. Настройка поисковой системы по умолчанию Включена
29. Не разрешать пользователям включать и отключать надстройки Включена
30. Включена
31. Ограничить результаты обнаружения сайтов по домену Включена
32. Отключить гаджеты рабочего стола Включена
33. По умолчанию сохранять документы в OneDrive Включена
34. Подготовить избранное Включена

35. Предотвращать открытие веб-страницы "Первый запуск" в Microsoft Edge Включена
36. Применить аватар по умолчанию ко всем пользователям Включена
37. Применить конкретное изображение экрана блокировки и экрана входа в систему, которое будет использоваться по умолчанию Включена
38. Принудительно задать фон начального экрана Включена Нет
39. Разрешить Microsoft Edge запускать и загружать начальную страницу и страницу новой вкладки при загрузке Windows и каждый раз при закрытии Microsoft Edge Включена
40. Разрешить предварительный запуск Microsoft Edge при загрузке Windows, когда система простаивает, и каждый раз при закрытии Microsoft Edge Включена
41. Разрешить работу в полноэкранный режиме Включена
42. Съемные диски: Запретить выполнение Включена
43. Съемные диски: Запретить запись Включена
44. Съемные диски: Запретить чтение Включена
45. Удалить список всех программ в меню «Пуск» Включена
46. Настроить дополнительные поисковые системы Отключена
47. Настроить параметр «Запустить Adobe Flash» Отключена
48. Разрешить Adobe Flash Отключена
49. Разрешить доступ к средствам разработчика Отключена
50. Разрешить загрузку неопубликованного расширения Отключена
51. Разрешить настройку поисковой системы Отключена
52. Разрешить печать Отключена
53. Разрешить предложения из раскрывающегося списка в адресной строке Отключена
54. Разрешить просмотр InPrivate Отключена
55. Разрешить удаление данных браузера при выходе Отключена