Приложение 4
к приказу по
МКОУ «ТельмановскаяСОШ»
от 03.09.2019г.№ 207-ОД

Инструкция ответственного за контроль использования обучающимися сети Интернет

1. Настоящая инструкция устанавливает порядок действий при обнаружении сотрудниками образовательных учреждений:

1) возможности доступа обучающихся к потенциально опасному контенту;

2) отказа доступа к контенту, не представляющему опасности для обучающихся, вызванного техническими причинами.

2. Контроль за использованием обучающимися сети Интернет осуществляют:

1) во время занятия – проводящий его преподаватель и(или) работник ОУ, специально выделенный для помощи в проведении занятий;

2) во время использования сети Интернет для свободной работы обучающихся – сотрудник ОУ, назначенный руководителем ОУ в установленном порядке.

3. Преподаватель:

— определяет время и место работы обучающихся в сети Интернет с учетом использования в образовательном процессе соответствующих технических возможностей, а также длительность сеанса работы одного обучающегося;

— наблюдает за использованием обучающимися компьютеров и сети Интернет;

— способствует осуществлению контроля за объемом трафика ОУ в сети Интернет;

— запрещает дальнейшую работу обучающегося в сети Интернет на уроке (занятии) в случае нарушения им порядка использования сети Интернет и предъявляемых к обучающимся требований при работе в сети Интернет;

— доводит до классного руководителя информацию о нарушении обучающимся правил работы в сети Интернет;

— принимает необходимые меры по пресечению дальнейших попыток доступа к ресурсу/группе ресурсов, не совместимых с задачами образования.

4. При обнаружении ресурса, который, по мнению преподавателя, содержит информацию, запрещенную для распространения в соответствии с законодательством Российской Федерации, или иного потенциально опасного для обучающихся контента, он сообщает об этом лицу, ответственному за работу Интернета и ограничение доступа.

5. В случае отказа доступа к ресурсу, разрешенному в ОУ, преподаватель также сообщает об этом лицу, ответственному за работу Интернета и ограничение доступа.

Инструкция пользования

персональным компьютером и ресурсами сети

1. Общие положения

1.1. Целью настоящей инструкции является регулирование работы системных администраторов и пользователей, распределения сетевых ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации. Более эффективного использования сетевых ресурсов и уменьшить риск умышленного или неумышленного неправильного их использования;

1.2. К работе в системе допускаются лица, назначенные начальником соответствующего отдела и прошедшие инструктаж и регистрацию в отделе ИТСО;

1.3. Работа в системе каждому работнику разрешена только на определенных компьютерах, в определенное время и только с разрешенными программами и сетевыми ресурсами. Если нужно работать вне указанного времени, на других компьютерах и с другими программами, необходимо согласовать это с системным администратором;

1.4. По уровню ответственности и правам доступа к сети пользователи сети разделяются на следующие категории: системные администраторы и пользователи;

1.5 Пользователь подключенного к сети компьютера - лицо, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю прав доступа к ней;

1.6. Каждый сотрудник пользуется индивидуальным именем пользователя для своей идентификации в сети, выдаваемым системным администратором;

1.7. Каждый сотрудник сам создает пароль для входа в компьютерную сеть;

1.8. Каждый сотрудник должен пользоваться только своим именем пользователя и паролем для входа в компьютер, локальную сеть и сеть Интернет, передача их кому-либо запрещена;

1.9. В случае нарушения правил пользования сетью, связанных с используемым им компьютером, пользователь сообщает системному администратору, который проводит расследование причин и выявление виновников нарушений и принимает меры к пресечению подобных нарушений;

1.10. В случае появления у пользователя компьютера сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах несанкционированного удаленного доступа к информации, размещенной на контролируемом им компьютере ли каком-либо другом, пользователь должен немедленно сообщить об этом системному администратору сети;

1.11. Системный администратор - лицо, обслуживающее сервер и следящее за правильным функционированием сети. Системный администратор дает разрешение на подключение компьютера к сети, выдает IP-адрес компьютеру, создает учетную запись электронной почты

для пользователя. Самовольное подключение является серьезнейшим нарушением правил пользования сетью;

1.12. Системный администратор информирует пользователей обо всех плановых профилактических работах, которые могут привести к частичной или полной неработоспособности сети на ограниченное время, а также об изменениях предоставляемых сервисов и ограничениях, накладываемых на доступ к ресурсам сети;

1.13. Системный администратор имеет право отключить компьютер пользователя от сети в случае, если с данного компьютера производились попытки несанкционированного доступа к информации на других компьютерах, и в случаях других серьезных нарушений настоящей инструкции;

1.14. Пользователь должен ознакомиться с настоящей инструкцией. Обязанность ознакомления пользователя с инструкцией лежит на системном администраторе и начальнике отдела ИТСО.

2. Работа за компьютером

2.1. Запрещено самостоятельно разбирать компьютер и все его комплектующие. При возникновении неисправностей необходимо обратиться в отдел ИТСО;

2.2. Все кабели, соединяющие системный блок с другими устройствами, следует вставлять и вынимать только при выключенном компьютере. Исключение составляют USB-устройства: они могут быть подключены к включенному компьютеру;

2.3. Запрещено самостоятельно устанавливать, удалять, деактивировать и изменять программное обеспечение и сетевые настройки на компьютере. Этим занимается отдел ИТСО;

2.4. Запрещено аварийно завершать работу компьютера кнопкой "Reset" или отключением от электросети. Завершайте работу компьютера правильно, через кнопку (Пуск);

2.5. Запрещено подвергать компьютер и периферийные устройства физическим, термическим и химическим воздействиям. (Нельзя сидеть на компьютере, проливать на него чай, кофе, просыпать семечки, ставить у батареи и других нагревательных приборов);

2.5. По завершению рабочего дня компьютер необходимо выключить, и обесточить;

2.6. Перед началом работы пользователь должен:

* Включить выключатель сетевого фильтра. При включении кнопка должна начать светиться;

* Включить источник бесперебойного питания (ИБП) и выждать 5 секунд;

* Включить монитор (если выключен);

* Включить компьютер кнопкой "Power". Дождаться загрузки операционной системы (ОС);

* Войти в систему, используя свои личные имя пользователя и пароль.

2.7. По завершению работы пользователь должен:

* Закрыть все открытые программы и документы, сохранив нужные изменения;

* С помощью меню "Пуск->Завершение работы" выключить компьютер и дождаться завершения работы. (Системный блок перестанет мигать и шуметь);

* Выключить монитор;

* Выключить источник бесперебойного питания (ИБП), нажав кнопку на передней панели;

* Выключить сетевой фильтр.

2.8. При отключении электроэнергии источник бесперебойного питания (ИБП) позволяет компьютеру оставаться в рабочем состоянии от 5 до 20 минут. При отключении электроэнергии в помещении пользователь должен в немедленном порядке провести правильное выключение компьютера.

3. Работа в локальной сети

3.1. Пользователи сети обязаны:

3.1.1. Соблюдать правила работы в сети, оговоренные настоящей инструкцией;

3.1.2. При доступе к внешним ресурсам сети, соблюдать правила, установленные системными администраторами для используемых ресурсов;

3.1.3. Немедленно сообщать системному администратору сети или начальнику отдела ИТСО об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящей инструкции кем-либо. Администраторы, при необходимости, с помощью других специалистов, должны провести расследование указанных фактов и принять соответствующие меры;

3.1.4. Не разглашать известную им конфиденциальную информацию (имена пользователей, пароли), необходимую для безопасной работы в сети;

3.1.5. Обеспечивать беспрепятственный доступ специалистам отдела ИТСО к сетевому оборудованию и компьютерам пользователей, для организации профилактических и ремонтных работ;

3.1.6. Выполнять предписания специалистов отдела ИТСО, направленные на обеспечение безопасности сети;

3.1.7. В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться к системному администратору или начальнику отдела ИТСО.

3.2. Пользователи сети имеют право:

3.2.1. Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках, если иное не предусмотрено по согласованию с отделом ИТСО. Системные администраторы вправе ограничивать доступ к некоторым сетевым

ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на повышение эффективности использования сетевых ресурсов;

3.2.2. Обращаться к администратору сети по вопросам, связанным с распределением ресурсов компьютера. Какие-либо действия пользователя, ведущие к изменению объема используемых им ресурсов, или влияющие на загруженность или безопасность системы (например, установка на компьютере коллективного доступа), должны санкционироваться системным администратором сети;

3.2.3. Обращаться за помощью к системному администратору при решении задач использования ресурсов сети;

3.2.4. Вносить предложения по улучшению работы с ресурсом.

3.3. Пользователям сети запрещено:

3.3.1. Разрешать посторонним лицам пользоваться вверенным им компьютером (кроме случаев подключения/отключения ресурсов, выполняемого специалистами ИТСО);

3.3.2. Использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей без согласования со специалистами ИТСО;

3.3.3. Самостоятельно устанавливать или удалять установленные системным администратором сетевые программы на компьютерах, подключенных к сети, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов;

3.3.4. Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю;

3.3.5. Вскрывать компьютеры, сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование без согласования с системным администратором, изменять настройки BIOS, а также производить загрузку рабочих станций с дискет;

3.3.6. Самовольно подключать компьютер к сети, а также изменять IP-адрес компьютера, выданный системным администратором. Передача данных в сеть с использованием других IP адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других компьютерах;

3.3.7. Работать с каналоемкими ресурсами (video, audio, chat и др.) без согласования с системным администратором сети. При сильной перегрузке канала вследствие использования каналоемких ресурсов текущий сеанс пользователя, вызвавшего перегрузку, будет прекращен;

3.3.8. Получать и передавать в сеть информацию, противоречащую действующему законодательству РФ и нормам морали общества, представляющую коммерческую или государственную тайну;

3.3.9. Обхождение учетной системы безопасности, системы статистики, ее повреждение или дезинформация;

3.3.10. Использовать иные формы доступа к сети Интернет, за исключением разрешенных системным администратором: пытаться обходить установленный отделом ИТСО межсетевой экран при соединении с сетью Интернет;

3.3.11. Осуществлять попытки несанкционированного доступа к ресурсам сети, проводить или участвовать в сетевых атаках и сетевом взломе;

3.3.12. Использовать сеть для массового распространения рекламы (спам), коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз и т.п.

4. Работа с электронной почтой

4.1. Электронная почта предоставляется сотрудникам организации только для выполнения своих прямых служебных обязанностей. Использование ее в личных целях запрещено. Создание почтового ящика проводится системным администратором по служебной записке;

4.2. Все электронные письма, создаваемые и хранимые на компьютерах организации, являются собственностью организации и не считаются персональными;

4.3. Организация оставляет за собой право получить доступ к электронной почте сотрудников, если на то будут веские причины. Содержимое электронного письма не может быть раскрыто, кроме как с целью обеспечения безопасности или по требованию правоохранительных органов;

4.4. Конфигурировать программы электронной почты так, чтобы стандартные действия пользователя, использующие установки по умолчанию, были бы наиболее безопасными;

4.5. Выходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение политики безопасности фирмы;

4.6. Пользователи не должны позволять кому-либо посылать письма от чужого имени. Это касается их начальников, секретарей, ассистентов или других сослуживцев;

4.7. Организация оставляет за собой право осуществлять наблюдение за почтовыми отправлениями сотрудников. Электронные письма могут быть прочитаны организацией, даже если они были удалены и отправителем, и получателем. Такие сообщения могут использоваться для обоснования наказания;

4.8. В качестве клиентов электронной почты могут использоваться только утвержденные почтовые программы;

4.9. Осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).

5. Работа в сети Интернет

5.1. Доступ к сети Интернет предоставляется по служебной записке;

5.2. Пользователи используют программы для поиска информации в сети Интернет только в случае, если это необходимо для выполнения своих должностных обязанностей;

5.3. По использованию Интернет ведется статистика и поступает в архив фирмы. В конце каждого месяца все пользователи сети Интернет заполняет и подписывает личную статистку по использованию ресурсов сети;

5.4. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротоколированы и использоваться для принятия решения о применении к нему санкций;

5.5. Сотрудникам организации, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим или нарушает действующее законодательство РФ;

5.6. Все программы, используемые для доступа к сети Интернет, должны быть утверждены сетевым администратором и на них должны быть настроены необходимые уровни безопасности;

5.7. Сотрудники, нанятые по контракту, должны соблюдать эту политику после предоставления им доступа к сети Интернет;

5.8. Запрещено получать и передавать через сеть информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую тайну, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения;

5.9. Запрещено получать доступ к информационным ресурсам сети или сети Интернет, не являющихся публичными, без разрешения их собственника.

Рекомендации по обеспечению безопасности при работе в Сети Интернет

- Не запускайте у себя на компьютере программ из ненадежных источников и не открывайте приложения к письмам, даже если письмо пришло от Вашего хорошего знакомого: в них могут быть спрятаны вирусы или троянские кони. Сначала сохраните это приложение в файл и проверьте его антивирусной программой. Помните, что злоумышленники могут прибегнуть к разнообразным приемам, чтобы обманом получить у Вас информацию об идентификационных параметрах.
- Не надо верить всем сообщениям о новых страшных вирусах, появившихся в Интернет, особенно если в сообщении сказано, что надо распространить эту информацию всем Вашим знакомым. Это сообщение может оказаться носителем вируса или просто компьютерной шуткой. Дополнительную информацию про компьютерные шутки и письма счастья можно посмотреть на HoaxBusters.ciac.org.
- Если Вы получили письмо от незнакомого человека или организации, то знайте, что скорее всего, это спам - назойливые рекламные письма - и письмо попало в Ваш ящик не по ошибке, а специально. Чтобы не получать письма от этого адресата впредь, нужно написать жалобу администратору сети, откуда прислано это письмо. Если же это не помогает, напишите письмо в техническую службу по адресу: admin@ptl.ru.
- Обязательно установите на ВСЕ компьютеры антивирусную программу для защиты от троянских коней и вирусов в режиме резидентного монитора (тогда она будет проверять все запускаемые программы и открываемые документы автоматически). Мы рекомендуем Вам использовать AVP(www.avp.ru.). Обновляйте антивирусные базы данных не реже, чем каждые 3-5 дней. Большинство антивирусов позволяют делать это бесплатно и через Интернет. Если антивирусная база не обновлялась более 3 месяцев, эффективность антивируса сильно снижается. Для защиты от неизвестных вирусов и троянских коней также можно установить программу-ревизор (мы рекомендуем AVP Inspector). Необъяснимые изменения файлов или появление новых файлов, обнаруженных ею, являются признаками появления нового вируса или троянского коня. Регулярно (не реже 1 раз в неделю) смотрите статистику использования Вами Интернет. Если Вы заметили подозрительный трафик, допустим в дни, когда вы отдыхали, свяжитесь с нами по адресу: web@ptl.ru
- Ограничьте доступ к Вашему компьютеру с помощью программ управления доступом (их можно посмотреть на сайте www.listsoft.ru) и введите установки безопасности (запрос пароля BIOSом при включении компьютера). Так же рекомендуем закрыть возможность соединения по следующим портам:

- Пакеты протокола TCP с портом получателя 80. Это защитит от использования уязвимых WWW-серверов на Вашем компьютере. Они могут содержать ошибки, позволяющие читать все файлы на диске.
- Делайте резервные копии системных файлов и важных данных и храните их в безопасном месте (не на жестком диске Вашего компьютера). В случае сбоя жесткого диска или вирусной атаки это позволит Вам быстро продолжить работу.
- Помните, что программы, которыми Вы пользуетесь при работе в Интернет, могут содержать ошибки безопасности ("дыры"). Эти ошибки могут позволить злоумышленнику заблокировать Ваш компьютер или получить несанкционированный доступ к нему через Интернет. Производители операционных систем и прикладных программ регулярно публикуют информацию об обнаруженных "дырах" (например, www.microsoft.com) и исправленные версии программ. Проверьте, что Вы установили ВСЕ исправления для используемых Вами программ, и если нет - сделайте это как можно скорее. Следите за публикациями о новых обнаруженных ошибках в программах и оперативно устанавливайте исправления для них. Рекомендуем для этого подписаться на списки рассылки на сайтах www.cert.ru и www.sans.org.
- Для повышения безопасности следует установить на компьютере персональный пакетный фильтр - программу, которая поможет защитить Ваш компьютер от несанкционированного доступа злоумышленников к нему через Интернет путем блокирования некоторых принимаемых и передаваемых пакетов. Мы рекомендуем использовать бесплатную программу "Сфера" (www.sphere.agnitum.com) или Tiny Personal Firewall (www.tinysoftware.com). Кроме того, можно воспользоваться хорошо зарекомендовавшим себя AtGuard. Дополнительную информацию про пакетные фильтры можно прочитать на www.grc.com.
- Не думайте, что вирусы и троянские кони могут находиться только в программах, загруженных из Интернета - как показывает печальный опыт покупателей пиратских CD, на них все чаще появляются программы, также зараженные вирусами или троянскими конями. Если уж Вы купили CD, проверьте его хорошей антивирусной программой с последней антивирусной базой данных.
- Если у вас установлена программа онлайнового общения ICQ, ни в коем случае не создавайте с ее помощью ICQ Home page - при ее создании на вашей машине запускается собственный WWW-сервер, содержащий ошибку, из-за которой хакеры смогут получить доступ ко всем файлам на вашем диске! Если она у вас создана, тут же отключите ее.

Инструкция по безопасности при работе в сети Интернет.

Обращаем Ваше внимание на действия, обеспечивающие безопасность при работе во внутренней широкополосной сети нашей компании и при подключении к всемирной сети Интернет. При подключении к Локальной сети и Интернет большинство пользователей сразу начинают пользоваться предоставленными услугами, зачастую не подозревая об опасности, которая может подстерегать их при работе. Если компьютер незащищён, он может стать объектом атак «хакеров» или подвергнуться воздействию вирусов. Все это, в конечном итоге, ведёт к печальным последствиям: потере важной информации, завладению Вашими паролями, номерами кредитных карт, использованию Вашего трафика, нестабильной работе компьютера. Для предотвращения этого необходимо:

1. Подготовить компьютер для подключения к Интернет.
2. Соблюдать основные требования использования пароля.
3. Соблюдать правила пользования электронной почтой.
4. Своевременно получать обновления операционной системы от Microsoft Corp. И обновления от производителей программного обеспечения, защищающего Ваш компьютер (антивирусная программа, сетевой экран)

Подготовка Вашего компьютера для подключения к сети:

1. Отключите сигнальный (сетевой) кабель от сетевой карты.
2. Установите операционную систему Windows 2000 Pro SP4 или Windows XP SP2. Предпочтительнее, чтобы это была «чистая» ОС, т.е. установленная заново на отформатированный диск.
3. Установите антивирусную программу с обновленной базой данных. Эта программа должна работать в режиме постоянного мониторинга.
4. Просканируйте все файлы на наличие вируса.
5. Установите и настройте любую программу из класса firewall (брандмауэр, сетевой экран).
6. Для всех пользователей операционной системы заведите пароли, длиной не менее 8 символов. Это необходимо сделать обязательно! При установке Windows 2000 и особенно Windows XP обратите внимание на пункт ввода пароля для пользователя «Администратор».
7. Настройте сетевые подключения: отключите «Службу доступа к файлам и принтерам» Вашего компьютера и «Клиент для сетей Микрософт» в свойствах протокола TCP/IP подключения по локальной сети укажите выделенный Вам при заключении договора IP адрес, маску подсети и шлюз
8. Запустите мастер новых подключений и создайте новое подключение к Интернету. Откройте окно свойств созданного подключения и на закладке «Сеть» уберите галочки перед компонентами «Служба доступа к файлам и принтерам» и «Клиент для сетей Микрософт».

9. Только после выполнения п.п. 2-8 подключите сигнальный (сетевой) кабель к разъему сетевой карты.

Правила обращения с паролем:

1. Используйте пароль для доступа в Интернет, состоящий из ЛАТИНСКИХ заглавных и прописных букв и цифр (длина пароля не менее 8 символов). Не используйте в качестве пароля слова, самый защищенный пароль — случайный набор символов.
2. Обязательно измените пароль на доступ в Интернет во время первого сеанса работы в Интернете. Это можно сделать на нашем сайте в разделе Личный кабинет.
3. Храните пароли в надежном месте, никогда не сохраняйте их на компьютере (не ставьте галочку «сохранить пароль»), никому не сообщайте и периодически меняйте в своем Личном кабинете на нашем сайте.
4. В случае обнаружения подозрительной активности Вашего компьютера (происходит несанкционированный обмен данными) немедленно отключите соединение с локальной сетью и обратитесь к специалистам службы технической поддержки АБОНЕНТОВ (тел.3-14-67).
5. Если Ваш пароль украли! Главное как можно раньше узнать об этом. В подавляющем большинстве случаев цель взломщика — получить возможность воспользоваться доступом в сеть Интернет за Ваш счет, поэтому Вам нужно регулярно проверять свой баланс и статистику использования услуг. Как только увидите что-то подозрительное, немедленно меняйте пароль и свяжитесь со службой технической поддержки АБОНЕНТОВ (тел.3-14-67).

Правила пользования электронной почтой:

1. Назначьте пароль для доступа к Вашему почтовому ящику, отличный от пароля на доступ в Интернет.
2. Никогда не открывайте писем от сомнительных отправителей. В таких письмах могут содержаться вредоносные программы (вирусы). Настройте вашу антивирусную программу на проверку всей приходящей почты на наличие вирусов (смотрите документацию, предоставленную изготовителем антивирусной программы).
3. Никогда не отвечайте на письма, содержащие просьбу прислать Ваши учетные данные (логин и пароль), даже, если в адресе отправителя Вы увидите адрес той или иной службы компании «НэтЛайн». **Мы никогда не посылаем таких писем своим АБОНЕНТАМ!** Имейте в виду, что это довольно распространенный способ, применяемый злоумышленниками для завладения чужими паролями.

Будьте бдительны!

Регламент работы учителей и школьников в сети Интернет

Сеть Интернет представляет собой глобальное объединение компьютерных сетей и информационных ресурсов, принадлежащих множеству различных людей и организаций. Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности.

Пользователь сети Интернет – лицо использующее ресурсы всемирной компьютерной сети.

При работе с ресурсами сети Интернет недопустимо:

- распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

- публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию.

При работе с ресурсами Интернет запрещается:

- загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;

- использовать программные и аппаратные средства, позволяющие получить доступ к ресурсам сети Интернет, содержание которых не имеет отношения к образовательному процессу, а так же к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.