

**ДЕПАРТАМЕНТ ОБЩЕГО ОБРАЗОВАНИЯ
ТОМСКОЙ ОБЛАСТИ**

**Областное государственное бюджетное общеобразовательное
учреждение кадетская школа-интернат
«Томский кадетский корпус»**

Приказ

22 августа 2018 г.

№ 284

**Об утверждении локальных нормативных актов по
безопасной работе в сети Интернет**

В целях соблюдения прав обучающихся на защиту от информации, пропаганды и агитации, наносящих вред здоровью, нравственному и духовному развитию обучающихся, в соответствии с федеральным законом от 28.07.1998 года № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»,

ПРИКАЗЫВАЮ:

1. Утвердить Регламент организации доступа к сети Интернет (Приложение №1).
2. Утвердить Регламент организации антивирусной защиты (Приложение №2).
3. Утвердить Классификатор информации, не соответствующий задачам образовательно-воспитательного процесса, классификатор информации, распространение которой среди обучающихся ограничено, классификатор информации, распространение которой запрещено в соответствии с законодательством РФ (Приложение №3).
4. Утвердить Инструкцию пользователя при работе в сети Интернет (Приложение №4).
5. Утвердить Порядок доступа в помещения ОГБОУ кадетская школа-интернат «Томский кадетский корпус, в которых ведется обработка персональных данных (Приложение №5).
6. Утвердить Инструкцию о порядке действий при осуществлении контроля за использованием обучающимися сети Интернет (Приложение №6).
7. Утвердить План мероприятий по обеспечению информационной безопасности обучающихся на 2018-2019 учебный год (Приложение №7).
8. Контроль за исполнением данного приказа оставляю за собой.

Директор



С.П. Ерохин

РЕГЛАМЕНТ ОРГАНИЗАЦИИ ДОСТУПА К СЕТИ ИНТЕРНЕТ

Основные понятия:

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, содержащим информацию, несовместимую с задачами образования и воспитания обучающихся, а также 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.

ОБЩИЕ ПОЛОЖЕНИЯ

Использование сети Интернет в образовательном учреждении направлено на решение задач учебно-воспитательного процесса. Доступ к сети Интернет должен осуществляться только с использованием лицензионного программного обеспечения или программного обеспечения, разрешенного для свободного использования. Настоящий Регламент регулирует условия и порядок использования сети Интернет в образовательном учреждении (ОУ).

Организация использования сети Интернет в образовательном учреждении

Вопросы использования возможностей сети Интернет в учебно-воспитательном процессе рассматриваются на педагогическом совете. Правила использования сети Интернет вводятся в действие приказом директора ОУ, они разрабатываются с учетом:

- законодательства Российской Федерации, региональных нормативно-правовых актов;
- целей образовательно-воспитательного процесса;
- рекомендациями профильных органов и организаций в сфере классификации ресурсов Сети;
- интересами обучающихся.

Руководитель образовательного учреждения отвечает за обеспечение пользователям (сотрудникам и обучающимся) эффективного и безопасного доступа к сети Интернет. Для обеспечения доступа к Сети участников образовательно-воспитательного процесса руководитель ОУ назначает своим приказом ответственного за информатизацию ОУ из числа заместителей директора образовательного учреждения за организацию работы с Интернетом.

Педагогический совет ОУ:

- принимает решение о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет;
- во время занятий в рамках учебно-воспитательного процесса контроль использования обучающимися сети Интернет осуществляет преподаватель (воспитатель), ведущий занятие. При этом преподаватель:
- контролирует использование обучающимися компьютера в сети Интернет;
- принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательно-воспитательному процессу.

Обучающимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации, и которые имеют прямое отношение к образовательно-воспитательному процессу. Проверка выполнения данного требования осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации, установленного на компьютерах образовательного учреждения и(или) предоставленного оператором услуг связи.

Пользователи и ответственные за работу в сети Интернет в ОУ должны учитывать, что технические средства и программное обеспечение не в состоянии обеспечить полную фильтрацию ресурсов сети Интернет из-за частого обновления ресурсов. В связи с этим существует вероятность обнаружения обучающимися ресурсов, не имеющих отношения к образовательно-воспитательному процессу, содержание которых противоречит законодательству Российской Федерации. При обнаружении факта выхода на такие ресурсы пользователю или ответственному за точку доступа лицу необходимо сообщить об этом ответственному за использование сети Интернет в ОУ, указав при этом адрес ресурса.

Отнесение определенных ресурсов и (или) категорий ресурсов в соответствующие группы, доступ к которым регулируется техническими средствами и программным обеспечением контентной фильтрации, в соответствии с принятыми в ОУ правилами, обеспечивается работником ОУ назначенным приказом руководителя.

Принципы размещения информации на Интернет-ресурсах ОУ призваны обеспечить:

- соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;
- защиту персональных данных обучающихся, преподавателей и сотрудников ОУ;
- достоверность и корректность информации.

Персональные данные обучающихся (включая фамилию и имя, класс/группу/год обучения, возраст, фотографию, данные о месте жительства, телефонах и пр., иные

сведения личного характера) могут размещаться на Интернет-ресурсах только с письменного согласия лица, чьи персональные данные размещаются (законного представителя несовершеннолетнего).

В информационных сообщениях о мероприятиях, размещенных на сайте ОУ без уведомления и получения согласия упомянутых лиц или их законных представителей, могут быть указаны лишь фамилия и имя обучающегося, либо фамилия, имя и отчество преподавателя, сотрудника или родителя.

При получении согласия на размещение персональных данных, представитель ОУ обязан разъяснить возможные риски и последствия их опубликования. ОУ не несет ответственности за такие последствия, если предварительно было получено письменное согласие лица (его законного представителя) на опубликование персональных данных.

Права, обязанности и ответственность пользователей

Преподаватели, воспитатели, сотрудники и обучающиеся могут бесплатно пользоваться доступом к глобальным Интернет-ресурсам по разрешению лица, назначенного ответственным за организацию в ОУ работы в сети Интернет и ограничению доступа.

Пользователям запрещается:

1. Осуществлять действия, запрещенные законодательством РФ.
2. Посещать сайты, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской Федерации (порнография, эротика, пропаганда насилия, терроризма, политического и религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности).
3. Загружать и распространять материалы, содержащие 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.
4. Загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом.
5. Передавать информацию, представляющую коммерческую или государственную тайну, распространять информацию, порочащую честь и достоинство граждан.
6. Устанавливать на компьютерах дополнительное программное обеспечение, как полученное в Интернете, так и любое другое без специального разрешения ответственного за информатизацию в ОУ.
7. Изменять конфигурацию компьютеров, в том числе менять системные настройки компьютера и любых программ, установленных на нем.
8. Осуществлять действия, направленные на «ВЗЛОМ» любых компьютеров, находящихся как в «точке доступа к Интернету» ОУ, так и за его пределами.
9. Использовать возможности «точки доступа к Интернету» ОУ для пересылки и записи непристойной, клеветнической, оскорбительной, угрожающей и порнографической продукции, материалов и информации.
10. Осуществлять любые сделки через Интернет.

Пользователи несут ответственность:

1. За содержание передаваемой, принимаемой и печатаемой информации.
2. За нанесение любого ущерба компьютерному оборудованию ОУ (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность.

3. За несообщение об обнаружении ресурса, содержание которого не имеет отношения к образовательно-воспитательному процессу. Преподаватель обязан зафиксировать доменный адрес ресурса, время его обнаружения и сообщить об этом лицу, ответственному за работу Сети и ограничение доступа к информационным ресурсам.

Пользователи имеют право:

1. Работать в сети Интернет в течение периода времени, определенного Правилами ОУ.
2. Сохранять полученную информацию на съемном носителе.
3. Размещать, с разрешения ответственных лиц информацию на Интернет-ресурсах ОУ.

РЕГЛАМЕНТ организации антивирусной защиты

Общие положения

Целью создания системы антивирусной защиты является обеспечение защищенности информационно-коммуникационной системы (далее ИКС) от воздействия различного рода вредоносных программ и несанкционированных массовых почтовых рассылок, предотвращения их внедрения в информационные системы, выявления и безопасного удаления из систем в случае попадания, а также фильтрации доступа пользователей Учреждения к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

Основополагающими требованиями к системе антивирусной защиты образовательного учреждения являются:

- средство защиты не должно оказывать противодействие конкретному вирусу или группе вирусов, противодействие должно оказываться в предположениях, что вирус может быть занесен на компьютер и о вирусе (о его структуре (в частности, сигнатуре) и возможных действиях) ничего не известно;
- решение задачи антивирусной защиты должно осуществляться в реальном времени.

Мероприятия, направленные на решение задач по антивирусной защите:

- установка только лицензированного программного обеспечения либо бесплатное антивирусное программное обеспечение, идущее в комплекте с подлинной операционной системой (типа Microsoft Security Essentials (сеть до 10 рабочих станций) или Microsoft Forefront Endpoint Protection (сеть более 10 рабочих станций)), поддерживающее работу с пользовательскими профилями;
- регулярное обновление и ежедневные профилактические проверки;
- непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах ИКС;
- ежедневный анализ, ранжирование и предотвращение угроз распространения и воздействия вредоносных программ путем выявления уязвимостей используемого в ИКС операционного программного обеспечения и сетевых устройств, и устранения обнаруженных дефектов в соответствии с данными поставщика программного обеспечения и других специализированных экспертных антивирусных служб;
- проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур;
- проведение системным администратором и ответственными за точки доступа лицами регулярных проверок целостности критически важных программ и данных. Наличие лишних файлов и следов несанкционированного внесения изменений должно быть зарегистрировано в журнале и изучено;
- внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования;

- необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения;
- следует иметь планы обеспечения бесперебойной работы образовательного учреждения для случаев вирусного заражения, в том числе планы резервного копирования всех необходимых данных и программ, и их восстановления. Эти меры особенно важны для сетевых файловых серверов, поддерживающих большое количество рабочих станций.

1. Технологические инструкции

1.1. В образовательном учреждении приказом директора назначается лицо, ответственное за антивирусную защиту, в должностных инструкциях которого прописывается порядок действий в период вирусных эпидемий, порядок действий при возникновении внештатных ситуаций, связанных с работоспособностью средств антивирусной защиты, порядок действий для устранения последствий заражений. Кроме того, ответственность за обеспечение антивирусной защиты несет руководитель образовательного учреждения.

1.2. В образовательном учреждении может использоваться только лицензионное антивирусное программное обеспечение либо свободно-распространяемое программное обеспечение.

1.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, почтовые сообщения), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация, находящаяся на съемных носителях (CD-ROM, DVD, flash-накопителях и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

1.4. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

2. Требования к проведению мероприятий по антивирусной защите

В начале работы при загрузке компьютера в автоматическом режиме должно выполняться обновление антивирусных баз и серверов.

2.1. Периодические проверки электронных архивов должны проводиться не реже одного раза в неделю, данные, расположенные на рабочих станциях пользователей - ежедневно.

2.2. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

- непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка на серверах и персональных компьютерах учреждения.
- при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).
- при отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

2.3. В случае обнаружения зараженных вирусами файлов или электронных писем пользователи обязаны:

- приостановить работу.
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты.
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.
- провести лечение или уничтожение зараженных файлов.

3. Ответственность

3.1. Ответственность за организацию антивирусной защиты возлагается на руководителя образовательного учреждения и ответственное лицо, им назначенное.

3.2. Ответственность за проведение мероприятий антивирусного контроля на АРМ образовательного учреждения возлагается на пользователей и ответственного за обеспечение антивирусной защиты, соблюдение требований настоящей Инструкции при работе на персональных компьютерах возлагается на ответственных за кабинет, где используется данный компьютер.

4. Регламент работы с электронной почтой

4.1. Электронный(ные) почтовый(вые) ящик(и) учреждения может(гут) использоваться только в служебных целях.

Запрещается: рассылка личных почтовых сообщений, спама, вложений с вирусами, сообщений неэтичного или противозаконного характера, сведений для служебного пользования и другой конфиденциальной информации (без официально запроса) и т.п.

По электронной почте образовательного учреждения производится обмен информацией законодательного, нормативно-правового, учебного, учебно-методического характера между учреждениями образования, органами управления образованием разных уровней, поставщиками оборудования и материалов, подрядчиками, поставщиками услуг и другими организациями, предприятиями и учреждениями, связанными с образовательным учреждением договорными или иными обязательствами.

4.2. За передачу и прием информации по электронной почте образовательного учреждения отвечает лицо, в должностные инструкции которого входит ведение делопроизводства.

4.3. Пользователь электронной почты образовательного учреждения должен строго соблюдать локальные правила и инструкции по работе с электронной корреспонденцией, а также данный Регламент.

Классификатор информации, не соответствующий задачам образования

№ п/п	Тематическая категория	Содержание
1	Алкоголь.	Реклама алкоголя, пропаганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию.
2	Баннеры и рекламные программы.	Баннерные сети, всплывающая реклама, рекламные программы.
3	Вождение и автомобили (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Не имеющая отношения к образовательному процессу информация об автомобилях и других транспортных средствах, вождении, автозапчастях, автомобильных журналах, техническом обслуживании, аксессуарах к автомобилям.
4	Досуг и развлечения (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Не имеющая к образовательному процессу информация: - фотоальбомы и фотоконкурсы; - рейтинги открыток, гороскопов, сонников; - гадания, магия, астрология; - ТВ - программы; - прогнозы погоды; - тесты, конкурсы онлайн; - туризм, путешествия; - тосты, поздравления; - кроссворды, сканворды, ответы к ним; - фантастика; - кулинария, рецепты, диеты; - мода, одежда, обувь, модные аксессуары, показы мод; - тексты песен, кино, киноактеры, расписания концертов, спектаклей, кинофильмов, заказ билетов в театры, кино и т.п.; - о дачах, участках, огородах, садах, цветоводстве, животных, питомцах, уходе за ними; - о рукоделии, студенческой жизни, музыке и музыкальных направлениях, группах, увлечениях, хобби, коллекционировании; - о службах знакомств, размещении объявлений онлайн; - анекдоты, «приколы», слухи; - о сайтах и журналах для женщин и для мужчин; - желтая пресса, онлайн - ТВ, онлайн - радио; - о знаменитостях; - о косметике, парфюмерии, прическах, ювелирных украшениях.
5	Здоровье и медицина (ресурсы	Не имеющая отношения к образовательному

	данной категории, не имеющие отношения к образовательному процессу).	процессу информация о шейпинге, фигуре, похудении, медицине, медицинских учреждениях, лекарствах, оборудовании, а также иные материалы на тему «Здоровье и медицина», которые, являясь академическими, по сути могут быть также отнесены к другим категориям (порнография, трупы и т.п.).
6	Компьютерные игры (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Не имеющая отношения к образовательному процессу информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет») по тематике компьютерных игр, не соответствующая задачам образования, такая как порталы браузерных игр, массовые многопользовательские ролевые онлайн игры (MMORPG), массовые многопользовательские игры, основанные на имитации боевых или противоправных действий, советы для игроков и ключи для установки и прохождения игр, игровые форумы и чаты.
7	Корпоративные сайты, интернет-представительства негосударственных учреждений (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Содержащие информацию, не имеющую отношения к образовательному процессу, сайты коммерческих фирм, компаний, предприятий, организаций.
8	Ресурсы, базирующиеся либо ориентированные на обеспечение анонимности распространителей и потребителей информации.	Анонимные форумы, чаты, доски объявлений и гостевые книги, такие как имиджборды, анонимайзеры, программы, обеспечивающие анонимизацию сетевого трафика в сети «Интернет» (tor, I2P).
9	Банки рефератов, дипломных работ, эссе, за исключением соответствующих задачам образования.	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), представляющая собой банки готовых рефератов, дипломных работ, эссе, за исключением печатных и электронных образовательных и информационных ресурсов, создаваемых в организациях, осуществляющих образовательную деятельность.
10	Личная и Немодерируемые информация.	Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информацию (адреса, телефоны и т.п.), личные странички, дневники, блоги.
11	Онлайн - казино и тотализаторы.	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая информацию об электронных казино, тотализаторах, играх на деньги.
12	Отправка SMS с использованием Интернет-ресурсов.	Сайты, предлагающие услуги по отправке SMS - сообщений.
13	Мошеннические сайты.	Сайты, навязывающие платные услуги на базе SMS - платежей, сайты, обманном

		путем собирающие личную информацию (фишинг).
14	Модерируемые доски объявлений (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Сайты, содержащие информацию, не имеющую отношения к образовательному процессу, модерируемые доски сообщений/объявлений, а также модерируемые чаты.
15	Магия, колдовство, чародейство, ясновидение, приворот по фото, теургия,	Информационная продукция, оказывающая психологическое воздействие на детей, при которой ребенок обращается к тайным силам
	волшебство, некромантия, тоталитарные секты.	с целью влияния на события, а также реального или кажущегося воздействия на состояние.
16	Неприличный и грубый юмор.	Неэтичные анекдоты и шутки, в частности обыгрывающие особенности физиологии человека.
17	Нижнее белье, купальники.	Сайты, на которых рекламируется нижнее белье, купальники, а также присутствуют образы полуобнаженных людей.
18	Обеспечение анонимности пользователя, обход контентных фильтров.	Сайты, предоставляющие инструкции по обходу прокси и доступа к запрещенным страницам; Peer-to-Peer программы, сервисы бесплатных прокси-серверов, сервисы, дающие пользователю анонимность.
19	Платные сайты.	Сайты, на которых вывешено объявление о платности посещения веб-страниц.
20	Поиск работы, резюме, вакансии (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Содержащие информацию, не имеющую отношения к образовательному процессу, интернет-представительства кадровых агентств, банки вакансий и резюме.
21	Поисковые системы (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Содержащие информацию, не имеющую отношения к образовательному процессу, интернет-каталоги, системы поиска и навигации в сети «Интернет».
22	Религия и атеизм (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Сайты, содержащие информацию, не имеющую отношения к образовательному процессу, информацию религиозной и антирелигиозной направленности.
23	Системы поиска изображений.	Системы для поиска изображений, не имеющих отношения к образовательному процессу, в сети «Интернет» по ключевому слову или словосочетанию.
24	СМИ (ресурсы данной категории, не имеющие отношения к образовательному процессу).	СМИ, содержащие новостные ресурсы и сайты СМИ (радио, телевидения, печати), не имеющие отношения к образовательному процессу.
25	Реклама табака, пропаганда потребления табака.	Сайты, пропагандирующие потребление табака; реклама табака и изделий из него.
26	Чаты (ресурсы данной категории, не	Не имеющие отношения к образовательному

	имеющие отношения к образовательному процессу).	процессу сайты для анонимного общения в режиме онлайн.
27	Убийства, насилие.	Сайты, содержащие описание или изображение убийств, мертвых тел, насилия и т.п.
28	Торговля и реклама (ресурсы данной категории, не имеющие отношения к образовательному процессу).	Не имеющие отношения к образовательному процессу сайты следующих категорий: аукционы, онлайн-распродажи, интернет-магазины, каталоги товаров и цен, электронная коммерция, модели мобильных телефонов, юридические услуги, полиграфия, типографии и их услуги, таможенные услуги, охранные услуги, иммиграционные услуги, услуги по переводу текста на иностранные языки, канцелярские товары, налоги, аудит, консалтинг, деловая литература, дом, ремонт, строительство, аренда/покупка/продажа недвижимости, продажа услуг мобильной связи (например, картинки и мелодии для сотовых телефонов), заработок в сети «Интернет», электронная коммерция.

*рекомендуется исключить из обработки систем контент - фильтрации образовательные ресурсы, относящиеся к домену edu.ru

Классификатор информации, распространение которой среди детей определенных возрастных категорий ограничено

№ п/п	Тематическая категория	Содержание
1	Информация, представляемая в виде изображения жестокости.	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая описание, фотографии, рисунки, видеоматериалы сцен жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия.
2	Информация, вызывающая у обучающихся страх, ужас или панику.	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая описание, фотографии, рисунки, видеоматериалы, унижающие человеческое достоинство в форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий.
3	Информация сексуального характера.	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), представляемая в виде изображений, видеоматериалов, описания половых отношений между мужчиной и женщиной.
4	Информация, содержащая нецензурную лексику.	Информационная продукция (в том числе сайты, форумы, доски объявлений, страницы социальных сетей, чаты в сети «Интернет»), содержащая бранные слова и выражения, не относящиеся к нецензурной лексике.

Классификатор информации, распространение которой запрещено в соответствии с законодательством РФ

№ п/п	Тематическая категория	Содержание
1	Пропаганда войны, разжигание ненависти и вражды, пропаганда порнографии и антиобщественного поведения.	- Информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды. - Информация, пропагандирующая порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение.
2	Злоупотребление свободой, СМИ - экстремизм.	Информация, содержащая публичные призывы к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы.
3	Злоупотребление свободой СМИ - наркотические средства.	Сведения о способах, методах разработки, изготовления, местах приобретения

		наркотических средств, психотропных веществ и их прекурсоров, пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров.
4	Злоупотребление свободой СМИ - информация с ограниченным доступом.	Сведения о специальных средствах, технических приемах и тактике проведения контртеррористических операций.
5	Злоупотребление СМИ - скрытое воздействие.	Информация, содержащая скрытые вставки и иные технические способы воздействия на подсознание людей и (или) оказывающая вредное влияние на их здоровье.
6	Экстремистские материалы или экстремистская деятельность (экстремизм).	А) Экстремистские материалы, то есть предназначенные для обнародования документов или информация, призывающие к осуществлению экстремистской деятельности, либо обосновывающие или оправдывающие необходимость осуществления такой деятельности, в том числе труды руководителей национал-социалистической рабочей партии Германии, фашистской партии Италии; публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство, либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой-либо этнической, социальной, расовой, национальной или религиозной группы. Б) Экстремистская деятельность (экстремизм) включает деятельность по распространению материалов (произведений), содержащих хотя бы один из следующих признаков: - насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, захват или присвоение властных полномочий, создание незаконных вооруженных формирований; - осуществление террористической деятельности либо публичное оправдание терроризма; - возбуждение расовой, национальной или религиозной розни, а также социальной розни, связанной с насилием или призывами к насилию; - унижение национального достоинства; осуществление массовых беспорядков, хулиганских действий и актов вандализма по мотивам идеологической, политической, расовой, национальной или религиозной

ненависти либо вражды, а равно по мотивам ненависти либо вражды в отношении какой-либо социальной группы; граждан по признаку их отношения к религии, социальной, расовой, национальной, религиозной или языковой принадлежности;

- воспрепятствование законной деятельности органов государственной власти, избирательных комиссий, а также законной деятельности должностных лиц указанных органов, комиссий, сопровождаемое насилием или угрозой его применения;

- публичная клевета в отношении лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, при исполнении им своих должностных обязанностей или в связи с их исполнением, сопровождаемая обвинением указанного лица в совершении деяний, указанных в настоящей статье, при условии, что факт клеветы установлен в судебном порядке;

- применение насилия в отношении представителя государственной власти либо угроза применения насилия в отношении представителя государственной власти или его близких в связи с исполнением им своих должностных обязанностей;

- посягательство на жизнь государственного или общественного деятеля, совершенное в целях прекращения его государственной или иной политической деятельности либо из мести за такую деятельность;

- нарушение прав и свобод человека и гражданина, причинение вреда здоровью и имуществу граждан в связи с их убеждениями, расовой или национальной принадлежностью, вероисповеданием, социальной принадлежностью или социальным происхождением. пропаганда исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, социальной, расовой, национальной, религиозной или языковой принадлежности;

- воспрепятствование законной деятельности органов государственной власти, избирательных комиссий, а также законной деятельности должностных лиц указанных органов, комиссий, сопровожаемое насилием или угрозой его

		применения; - публичная клевета в отношении лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, при исполнении им своих должностных обязанностей или в связи с их исполнением, сопровождаемая обвинением указанного лица в совершении деяний, указанных в настоящей статье, при условии, что факт клеветы установлен в судебном порядке; - применение насилия в отношении представителя государственной власти либо угроза применения насилия в отношении представителя государственной власти или его близких в связи с исполнением им своих должностных обязанностей; - посягательство на жизнь государственного или общественного деятеля, совершенное в целях прекращения его государственной или иной политической деятельности либо из мести за такую деятельность; - нарушение прав и свобод человека и гражданина, причинение вреда здоровью и имуществу граждан в связи с их убеждениями, расовой или национальной принадлежностью, вероисповеданием, социальной принадлежностью или социальным происхождением.
7	Вредоносные программы.	Программы для ЭВМ, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети.
8	Преступления.	- Клевета (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию); - оскорбление (унижение чести и достоинства другого лица, выраженное в неприличной форме); - публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма; - склонение к потреблению наркотических средств и психотропных веществ; - незаконное распространение или рекламирование порнографических материалов; - публичные призывы к осуществлению экстремистской деятельности;

		- информация, направленная на пропаганду национальной, классовой, социальной нетерпимости, а также социального, расового, национального и религиозного неравенства; - публичные призывы к развязыванию агрессивной войны.
9	Ненадлежащая реклама.	Информация, содержащая рекламу алкогольной продукции и табачных изделий.
10	Информация с ограниченным доступом.	Информация, составляющая государственную, коммерческую, служебную или иную охраняемую законом тайну.

Инструкция пользователя по компьютерной безопасности в сети Интернет

Обучающимся:

1. Обязанности обучающегося - пользователя сети Интернет.
 - 1.1 Обучающийся обязан выполнять требования лица, уполномоченного контролировать использование сети Интернет.
 - 1.2 Соблюдать тишину, чистоту и порядок в компьютерном классе.
 - 1.3 Во время образовательно-воспитательного процесса в компьютерном классе и в любой другой точке доступа образовательного учреждения, посещать Интернет-ресурсы только образовательной направленности.
 - 1.4 Сообщать ответственному лицу о случайном попадании на ресурс, явно не соответствующий образовательной направленности и/или нарушающий законодательство РФ.
2. Обучающемуся - запрещается:
 - посещать сайты, содержащие информацию не образовательной направленности (порнографическую, антигосударственную, со сценами насилия и т.п.), участвовать в нетематических форумах, чатах, конференциях, социальных сетях;
 - устанавливать дополнительное программное обеспечение, полученное в Интернете или любое другое, без согласования с ответственным за информатизацию лицом;
 - изменять конфигурацию компьютера, в том числе менять системные настройки и настройки программ, установленных на нем, а также включать, выключать и перезагружать компьютер без согласования с ответственным за точку доступа в Интернет лицом;
 - осуществлять действия, направленные на «взлом» любых компьютеров.
3. Права обучающегося - пользователя сети Интернет.
 - 3.1. Обучающийся имеет право во время занятия работать в сети Интернет в течение времени, отведенного ответственным за точку доступа лицом.
 - 3.2. Сохранять полученную информацию на внешнем носителе.
4. Ответственность обучающегося - пользователя сети Интернет
 - 4.1. Обучающийся несет ответственность за содержание передаваемой, принимаемой и распечатываемой информации.
 - 4.2. Обучающиеся, не соблюдающие настоящую инструкцию, лишаются права работы в сети Интернет, к ним могут быть применены меры воспитательного и дисциплинарного воздействия.
 - 4.3. При нанесении любого ущерба «точке доступа к Интернету» (порча имущества, вывод оборудования из рабочего состояния) законные представители обучающегося несут материальную ответственность.

Сотрудникам:

1. Обязанности сотрудника - пользователя сети Интернет.
 - 1.1. Использовать ресурсы сети Интернет образовательного учреждения в образовательных целях.
 - 1.2. Уважать законы, авторские права, честь и достоинство других пользователей сети Интернет.

1.3. Использовать ресурсы сети Интернет для приобретения новых знаний и навыков в области образования, расширения спектра учебных и наглядных пособий, содействия гармоничному формированию и развитию личности обучающегося, ее социализации, введению в информационное общество.

1.4. Осуществлять контроль за использованием обучающимися ресурсов сети Интернет образовательной организации во время занятий: наблюдать за использованием компьютера и сети Интернет, запрещать работу обучающегося в случае нарушения им настоящей инструкции и других документов, регламентирующих использование сети Интернет, принимать меры по пресечению попыток доступа к ресурсам, несовместимым с задачами образования.

Интернет-ресурсы не образовательной направленности

1. Пользователям 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, распространять рекламную, коммерческую или схожую по направленности информацию, участвовать в чатах, конференциях, форумах не образовательной направленности, распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

2. При случайном обнаружении лицом, работающим в сети Интернет, ресурса, содержимое которого несовместимо с целями образовательного процесса, он обязан незамедлительно сообщить о таком ресурсе Уполномоченному лицу с указанием Интернет-адреса (URL) и покинуть данный ресурс.

Порядок
доступа в помещения ОГБОУ кадетская школа-интернат «Томский кадетский
корпус, в которых ведется обработка персональных данных

1. Общие положения

1.1. Порядок доступа в помещения ОГБОУ кадетская школа-интернат «Томский кадетский корпус», в которых ведется обработка персональных данных (далее - Порядок, образовательное учреждение) разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

1.2. Целью настоящего Порядка является исключение несанкционированного доступа к персональным данным субъектов персональных данных образовательного учреждения.

2. Основные понятия

В настоящем Порядке используются следующие понятия и сокращения:

субъект персональных данных - физическое лицо, обратившееся в учреждение, гражданин, претендующий на замещение должности в образовательном учреждении; лицо, замещающее (замещавшее) должность учреждения; лицо, замещающее должность директора учреждения;

персональные данные - любая информация, относящаяся прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

конфиденциальность персональных данных - порядок обработки персональных данных, который препятствует доступу к информации третьим лицам без согласия субъекта персональных данных, а также ее передаче;

доступ к персональным данным - возможность получения доступа к персональным данным и их использование;

3. Доступ в помещения, в которых осуществляется обработка персональных данных

3.1. Вскрытие и закрытие помещений, в которых ведется обработка персональных данных, осуществляется работниками учреждения, допущенными к обработке персональных данных, местом работы которых определены данные помещения. Доступ посторонних лиц в данные помещения запрещен. Доступ работников образовательного учреждения разрешен только в присутствии работников ответственных за обработку персональных данных, хранящихся в этом помещении, при условии соблюдения мер безопасности персональных данных.

3.2. Размещение информационных систем, в которых обрабатываются персональные данные, осуществляется в охраняемых помещениях. В этих помещениях организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц (п.3.1.).

3.3. Нахождение в помещениях учреждения лиц, не являющихся лицами, допущенными к обработке персональных данных, возможно только при сопровождении уполномоченного работника учреждения на время, ограниченное необходимостью решения вопросов, связанных с предоставлением персональных данных, предоставлением муниципальных услуг, осуществлением муниципальных функций.

3.4. Запрещается оставлять материальные носители с персональными данными без контроля, вне запираемых шкафов, в незапертом помещении, в котором осуществляется обработка персональных данных.

3.5. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, свободно допускаются работники Администрации, уполномоченные на обработку персональных данных.

Инструкция
о порядке действий при осуществлении контроля за использованием обучающимися
сети Интернет

1. Настоящая Инструкция устанавливает порядок действий при обнаружении работниками образовательного учреждения возможности доступа обучающихся к потенциально опасному контенту.
2. Контроль за использованием обучающимися сети Интернет осуществляют:
 - во время проведения занятий - педагогический персонал, проводящий занятие и (или) специально уполномоченное руководством образовательного учреждения на осуществление такого контроля лицо;
 - во время использования сети Интернет для свободной работы обучающихся - ответственное за работу точки доступа лицо.
3. Лицо, осуществляющее контроль за использованием обучающимися сети Интернет:
 - определяет время и место работы кадет в сети Интернет с учетом использования соответствующих технических возможностей в образовательно-воспитательном процессе, а также длительность сеанса работы одного обучающегося;
 - способствует осуществлению контроля за объемом трафика образовательного учреждения в сети Интернет;
 - наблюдает за использованием компьютеров и сети Интернет обучающимися;
 - запрещает дальнейшую работу обучающегося в сети Интернет в случае нарушения им порядка использования сети Интернет и предъявляемых требований при работе в сети Интернет;
 - не допускает кадет к работе в Интернете в предусмотренных Правилами использования сети Интернет случаях;
 - принимает необходимые меры для пресечения дальнейших попыток доступа к ресурсу/группе ресурсов, несовместимых с задачами образования.
4. При обнаружении информации, в отношении которой у лица, осуществляющего контроль за использованием обучающимися сети Интернет, возникают основания предполагать, что такая информация относится к числу запрещенной для распространения в соответствии с законодательством Российской Федерации или иному потенциально опасному для учащихся контенту, ответственное лицо письменно направляет соответствующую информацию ответственному за информатизацию или руководителю образовательного учреждения, которые принимают необходимое решение.
5. При обнаружении вызванного техническими причинами отказа доступа к контенту, не представляющему опасности для учащихся, доступ к которому не противоречит принятым нормативным актам на уровнях федеральном, субъекта Российской Федерации, муниципальном, а также на уровне образовательного учреждения, лицо, осуществляющее контроль за использованием обучающимися сети Интернет устно, а при необходимости письменно, направляет соответствующую информацию ответственному за информатизацию или руководителю образовательного учреждения, которые принимают необходимое решение.

**План мероприятий по обеспечению информационной безопасности
обучающихся на 2018-2019 уч. год**

№ п/п	Наименование мероприятия	Срок исполнения	Исполнители, ответственные за Реализацию мероприятия	Ожидаемые результаты (количественные и качественные показатели)
I. Создание организационно-правовых механизмов защиты обучающихся от распространения информации, причиняющей вред их здоровью и развитию				
1.1	Размещение на официальном сайте образовательного учреждения рекомендаций для родителей и обучающихся о	Октябрь 2018	Заместитель директора по безопасности	100% Ознакомление родителей с информацией
1.2	Проведение внеурочных занятий кадетами по теме «Приемы безопасной работы в интернете»	Ноябрь 2018	Классные руководители	100% охват обучающихся ОУ
1.3.	Обеспечение контент-филтрации в образовательном учреждении	В течение образовательного процесса	Заместители директора, Системный администратор	Качественная работа контент-филтра
1.4.	Обеспечение исправной работы антивирусной программы на АРМ	В течение календарного года	Системный администратор	Качественная антивирусная защита
II. Внедрение систем исключения доступа к информации, несовместимой с задачами гражданского становления детей				
2.1.	Мониторинг функционирования и использования в ОУ программного продукта, обеспечивающего контент-филтрацию интернет-трафика.	Ежеквартально	Рабочая комиссия	Обеспечение контент-филтрации трафика. Акты проверок.
2.2.	Мониторинг функционирования и использования в ОУ программного продукта, обеспечивающего антивирусную защиту ПК АРМ	Ежеквартально	Рабочая комиссия	Обеспечение антивирусной защиты ПК АРМ. Акты проверок.

III. Профилактика у обучающихся интернет-зависимости, игровой зависимости и правонарушений с использованием информационно-телекоммуникационных технологий, формирование навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде через обучение их способам защиты от вредной информации.

3.1.	Проведение медиа-уроков по теме «Информационная безопасность»	По рабочим программам	Классные руководители, Учитель информатики	Обеспечение 100% охвата учащихся школы повышение грамотности обучающихся по проблемам информационной безопасности.
3.2.	Ведение раздела «Безопасность» на сайте ОУ	В течение уч. года	Зам по безопасности	Актуальность раздела.
3.3.	Организация и проведение обучающих семинаров для классных руководителей по профилактике среди обучающихся использования противоправного контента	Один раз в год	Заместитель директора по УР, учитель информатики	Повышение грамотности по проблемам информационной безопасности всех участников образовательного процесса
3.4.	Организация свободного доступа обучающихся и учителей к высококачественным сетевым образовательным ресурсам	В течение уч. года	Заместитель директора по УР, администратор сайта	100% Обеспечение доступа обучающихся и учителей к электронным образовательным ресурсам через сеть интернет
3.5.	Внедрение и использование программно-технических средств, обеспечивающих исключение доступа обучающихся к ресурсам сети интернет, содержащим информацию, несовместимую с задачами образования и воспитания	В течение уч. года	Ответственный за информатизацию ОУ, системный администратор	Установка программно-технических средств, обеспечивающих исключение доступа обучающихся к ресурсам сети интернет и установка их на компьютеры