МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ТОГУРСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА
ИМЕНИ ГЕРОЯ РОССИИ СЕРГЕЯ ВЛАДИМИРОВИЧА МАСЛОВА»

«УТВЕРЖДЕНО»
Директор МБОУ «Тогурская СОШ
им. С.В. Маслова»
_____ О.А. Пшеничникова
Приказ № 300 от 30.08.2024 г

РАБОЧАЯ ПРОГРАММА
учебного курса внеурочной деятельности
«Информационная безопасность»

Класс 8

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0099A27EC6F28D873C5013FA7A5FA5EEF3
Владелец: Пшеничникова Олеся Андреевна
Действителен: с 19.09.2024 до 13.12.2025

Программу составил:
Трифонова Ольга Юрьевна

с. Тогур 2024

Аннотация рабочей программы

Рабочая программа учебного предмета «Информационная безопасность» *в ней учтены приоритеты научно-технологического развития Российской Федерации* (Пр-294, п. 2а-16) и обновление программы воспитания и социализации обучающихся в школах Российской Федерации; авторской программы по «Информационная безопасность» для 7-9 классов (авторы Цветкова М. С., Якушина Е. В.).

Данная программа обеспечивается линией учебно-методических комплектов по Информационной безопасности для 5-11 классов под редакцией Цветковой М. С., Якушиной Е. В.), выпускаемой издательством «БИНОМ. Лаборатория знаний».

Цель изучения предмета/курса «Информационная безопасность»:

обеспечить социальные аспекты информационной безопасности в воспитании культуры информационной безопасности у школьников в условиях цифрового мира, включение на регулярной основе цифровой гигиены в контекст воспитания и обучения детей, формирование у выпускника школы правовой грамотности по вопросам информационной безопасности, которые влияют на социализацию детей в информационном обществе, формирование личностных и метапредметных результатов воспитания и обучения детей

Данная цель решает следующие образовательные **задачи**:

— формировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей, как ценность человеческой жизни, свободы, равноправия и достоинства людей, здоровья, опыта гуманных, уважительных отношений с окружающими;

— создавать педагогические условия для формирования правовой и информационной культуры обучающихся, развития у них критического отношения к информации, ответственности за поведение в сети Интернет и последствия деструктивных действий, формирования мотивации к познавательной, а не игровой деятельности, воспитания отказа от пустого времяпрепровождения в социальных сетях, осознания ценности живого человеческого общения;

— формировать отрицательное отношение ко всем проявлениям жестокости, насилия, нарушения прав личности, экстремизма во всех его формах в сети Интернет;

— мотивировать обучающихся к осознанному поведению на основе понимания и принятия ими морально-правовых регуляторов жизни общества и государства в условиях цифрового мира;

— научить молодых людей осознавать важность проектирования своей жизни и будущего своей страны — России в условиях развития цифрового мира, ценность ИКТ для достижения высоких требований к обучению профессиям будущего в мире, принимать средства в Интернете как среду созидания, а не разрушения человека и общества.

Практические (ПРЕДМЕТНЫЕ) задачи по Информационной безопасности в школе – — формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики; умение принимать обоснованные решения в конкретной опасной ситуации с учетом реально складывающейся обстановки и индивидуальных возможностей.

Учебный предмет «Информационная безопасность» входит во внеурочную область изучения в 8 классах и на его изучение отводится 34 часов (34 учебных недели). Материал курса располагается следующим образом и содержит следующие разделы:

Линия «Информационное общество и информационная культура»

Модуль 1. Современное информационное пространство и искусственный интеллект.

1.1. Киберпространство. Кибермиры. Киберфизическая система.

1.2. Киберобщество. Киберденьги. Кибермошенничество.

Модуль 2. Современная информационная культура.

2.1. Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство.

2.2. Социальная инженерия. Классификация угроз социальной инженерии.

2.3. Новые профессии в киберобществе. Цифровизация профессий.

Линия «Информационное пространство и правила информационной безопасности»

Модуль 3. Угрозы информационной безопасности.

3.1. Киберугрозы. Кибервойны. Киберпреступность.

Уязвимости кибербезопасность.

Запрещенные и нежелательные сайты.

3.2. Защита от вредоносных программ и информационных атак.

3.3. Практика электронного обучения в сфере информационной безопасности.

Предусмотрены следующие виды контроля: входной и промежуточный.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Нормативную правовую основу настоящей примерной образовательной программы по учебному курсу «Информационная безопасность» составляют следующие документы:

— Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

— ФГОС основного общего образования;

— ПООП основного общего образования;

— распоряжение Правительства РФ от 2 декабря 2015 г. № 2471-р «Об утверждении Концепции информационной безопасности детей»;

— Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

— Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы»;

— Перечень поручений по реализации Послания Президента Федеральному Собранию от 27 февраля 2019 г. Пр-294.

Примерная образовательная программа по учебному курсу «Информационная безопасность» (далее — программа) разработана на основе требований федерального государственного образовательного стандарта основного общего образования к результатам их освоения в части предметных результатов в рамках формирования ИКТ-компетентностей обучающихся по работе с информацией в глобальном информационном пространстве, а также личностных и метапредметных результатов в рамках социализации обучающихся в информационном мире и формирования культуры информационной безопасности обучающихся.

Программа включает пояснительную записку, в которой раскрываются цели изучения, общая характеристика и определяется место учебного курса «Информационная безопасность» в учебном плане, раскрываются основные подходы к отбору содержания и характеризуются его основные содержательные линии.

Программа устанавливает планируемые результаты освоения основной образовательной программы по курсу информационной безопасности для основного общего образования для 5—6 и 7—9 классов соответственно.

Программа определяет примерное календарное планирование учебного курса для указанных возрастных групп общего образования с указанием примерных часов на каждую тему по модулям программы в рамках их интеграции в дополнение к программам отдельных учебных предметов, а также в рамках программы воспитания (социализации) обучающихся или как отдельного учебного курса из часов, формируемых образовательной организацией.

Программа учебного курса «Информационная безопасность» разработана для организаций, реализующих программы общего образования. *В ней учтены приоритеты научно-технологического развития Российской Федерации* (Пр-294, п. 2а-16) и обновление программы воспитания и социализации обучающихся в школах Российской Федерации.

Цели изучения учебного курса «Информационная безопасность»

Безопасность в сети Интернет в свете быстрого развития информационных технологий, их глобализации, использования облачных технологий и повсеместного массового распространения среди детей мобильных персональных цифровых устройств доступа к сети Интернет, появления большого количества сетевых сервисов и интернет-коммуникаций, в том числе закрытых сетевых сообществ неизвестного толка, а также общедоступных и зачастую навязчивых интернет-ресурсов (СМИ, реклама, спам), содержащих негативный и агрессивный контент, расширения угроз новых сетевых средств вмешательства в личное информационное пространство на персональных устройствах, работающих в Интернете, а также в связи с массовым использованием детьми электронных социальных/банковских карт, имеющих персональные настройки доступа к ним, резко повышает потребность в воспитании у обучающихся культуры информационной безопасности в целях предотвращения негативных последствий массового использования Интернета детьми и их защиты от агрессивной и противоправной информации.

Программа учебного курса информационной безопасности имеет высокую актуальность и отражает важные вопросы безопасной работы с новыми формами коммуникаций и услуг цифрового мира: потребность в защите персональной информации, угрозы, распространяемые глобальными средствами коммуникаций Интернета и мобильной связи, использующими рассылки сообщений,

электронную почту, информационно-коммуникативные ресурсы взаимодействия в сети Интернет через массово доступные услуги электронной коммерции, социальные сервисы, сетевые объединения и сообщества, ресурсы для досуга (компьютерные игры, видео и цифровое телевидение, цифровые средства массовой информации и новостные сервисы), а также повсеместное встраивание дистанционных ресурсов и технологий в учебную деятельность, использующую поиск познавательной и учебной информации, общение в социальных сетях, получение и передачу файлов, размещение личной информации в коллективных сервисах. Помимо профилактики информационных угроз и противоправных действий через ресурсы в сети Интернет и мобильные сети, крайне актуально использовать коммуникации для привлечения обучающихся к информационно-учебной и познавательно-творческой активности по использованию позитивных интернет-ресурсов: учебных, культурных, научно-популярных, интеллектуальных, читательских, медийных, правовых, познавательных и специализированных социальных сообществ и сервисов для детских объединений и творческих мероприятий для детей и молодежи.

При реализации требований безопасности в сети Интернет для любого пользователя, будь то школьник или учитель, образовательное учреждение должно обеспечивать защиту конфиденциальных сведений, представляющих собой в том числе персональные данные школьника, и предотвращать доступ к противоправной негативной информации. Но включение детей в интернет-взаимодействие наиболее активно осуществляется вне школы без надлежащего надзора со стороны взрослых.

В связи с этим в настоящее время необходимо особое внимание уделять воспитанию у детей *культуры информационной безопасности* при работе в сети Интернет вне школы с участием родителей. Для этого следует проводить непрерывную образовательно-просветительскую работу с детьми, формировать у обучающихся ответственное и критическое отношение к источникам информации, правовую культуру в сфере защиты от негативной информации и противоправных действий средствами коммуникаций, в том числе внимательно относиться к использованию детьми личных устройств мобильной связи, домашнего компьютера с Интернетом, телевизора, подключенного к Интернету, использовать дома программные средства защиты от доступа детей к негативной информации или информации по возрастным признакам (возраст+). Научить школьника правильно ориентироваться в большом количестве ресурсов в сети Интернет — важная задача для вовлечения детей в современную цифровую образовательную среду, отвлечения их от бесполезного контента и игромании, бесцельной траты времени в социальных сетях и сервисах мобильной связи.

Главная цель курса — обеспечить социальные аспекты информационной безопасности в воспитании культуры информационной безопасности у школьников в условиях цифрового мира, включение на регулярной основе цифровой гигиены в контекст воспитания и обучения детей, формирование у выпускника школы правовой грамотности по вопросам информационной безопасности, которые влияют на социализацию детей в информационном обществе, формирование личностных и метапредметных результатов воспитания и обучения детей:

— формировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей, как ценность человеческой жизни, свободы, равноправия и достоинства людей, здоровья, опыта гуманных, уважительных отношений с окружающими;

— создавать педагогические условия для формирования правовой и информационной культуры обучающихся, развития у них критического отношения к информации, ответственности за поведение в сети Интернет и последствия деструктивных действий, формирования мотивации к познавательной, а не игровой деятельности, воспитания отказа от пустого времяпрепровождения в социальных сетях, осознания ценности живого человеческого общения;

— формировать отрицательное отношение ко всем проявлениям жестокости, насилия, нарушения прав личности, экстремизма во всех его формах в сети Интернет;

— мотивировать обучающихся к осознанному поведению на основе понимания и принятия ими морально-правовых регуляторов жизни общества и государства в условиях цифрового мира;

— научить молодых людей осознавать важность проектирования своей жизни и будущего своей страны — России в условиях развития цифрового мира, ценность ИКТ для достижения высоких требований к обучению профессиям будущего в мире, принимать средства в Интернете как среду созидания, а не разрушения человека и общества.

Место учебного курса «Информационная безопасность» в учебном плане

Особенностью программы курса является ее поэтапное развитие для разных возрастных групп обучающихся основного общего образования с учетом из возрастных особенностей. Программа курса

ориентирована на включение в контекст обучения и воспитания новых видов информационных угроз и средств противодействия им. Программа курса представлена двумя разделами по возрастным группам: для 5—6 классов и 7—9 классов.

Реализация программы учебного курса возможна в разных формах:

— как дополнительные модули обучения в интеграции с предметами «Информатика» и (или) «ОБЖ» для двух возрастных групп: 5—6 и 7—9 классов (от 30 учебных часов для каждой возрастной группы);

— в рамках отдельного учебного курса «Информационная безопасность» для внеурочной деятельности по выбору из объема часов, формируемых самостоятельно образовательной организацией;

— в рамках часов, предусмотренных по программе воспитания (социализации) в образовательной организации для разных уровней общего образования.

Программа учебного курса поддерживается электронными ресурсами на основе документальных фильмов, анимационных ресурсов и электронных практикумов в открытом доступе от ИТ-компаний Российской Федерации в рамках их участия в проектах по информационной безопасности для детей. В основе курса лежат технические, этические и правовые нормы соблюдения информационной безопасности, установленные контролирующими и правоохранительными органами, а также практические рекомендации ведущих ИТ-компаний и операторов мобильной связи Российской Федерации.

Общая характеристика учебного курса «Информационная безопасность»

Начинать обучение по курсу информационной безопасности крайне актуально по острым проблемным ситуациям в условиях присутствия в жизни детей персональных устройств работы в сети Интернет и мобильных сетях связи, а также для содействия при использовании детьми Интернета для обучения, творческого и развивающего досуга, познавательной деятельности. Программа направлена на решение вопросов массового формирования культуры информационной безопасности школьников, которые живут в современном информационном обществе, стремительно расширяющем общедоступные коммуникации в Интернете.

Проникновение мобильных устройств с доступом к Интернету в быт и досуг детей обострило проблему интернет-зависимости, игромании, зависимости от социальных сетей, необоснованного доверия посторонним людям в сети и, как следствие, незащищенности детей от атак мошенников, преступников, агрессивно настроенных людей, включая вовлечение детей в теневые, закрытые субкультуры, несущие угрозу здоровью и даже жизни ребенка.

Раздел программы курса для 5—6 классов отражает практические вопросы и жизненные проблемы:

— негативный и позитивный Интернет, цифровизация профессий;

— культура организации компьютерного досуга и профилактика игромании;

— мошенники в сети Интернет;

— агрессия в Интернете;

— сетевой этикет;

— навязчивые предложения;

— правила регистрации в электронных ресурсах и защита личных данных.

Раздел программы курса для 7—9 классов отражает особенности современного цифрового мира как киберпространства, насыщенного сетевыми сервисами и интернет-коммуникациями, доступными детям, новыми сервисами и устройствами с искусственным интеллектом (умные вещи, Интернет вещей), в том числе несущими в себе угрозы:

— закрытые сетевые сообщества неизвестного толка, опасные группы, негативные контакты;

— навязчивые интернет-ресурсы (спам, реклама, азартные игровые сервисы);

— сайты, содержащие негативный и агрессивный контент, в том числе противоправные материалы, влекущие ответственность по законам Российской Федерации;

— сетевые средства вмешательства в личное информационное пространство на персональных устройствах, работающих в Интернете;

— использование электронных сервисов, социальных/банковских карт, имеющих персональные настройки доступа к ним.

Отражение потребностей цифрового мира в современной цифровой грамотности и новых профессиональных качествах современного человека востребовано в жизни и учебе школьников и несет в себе актуальные запросы для выпускника основного общего образования в его дальнейшей

жизни и профессиональном выборе с обязательным использованием требований информационной безопасности:

— профориентация в мире профессий будущего, знакомство с профессиями в сфере информационной безопасности;

— популяризация электронных средств и ресурсов обучения;

— развитие кругозора о полезных интернет-ресурсах;

— получение представлений о цифровых технологиях для улучшения качества жизни;

— навыки обдуманного поведения при поиске информации в сети Интернет, критический анализ полученной информации, умение работать с информацией избирательно и ответственно.

СОДЕРЖАНИЕ УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Линия «Информационное общество и информационная культура»

Модуль 1. Современное информационное пространство и искусственный интеллект. 1.1. Киберпространство. Кибермиры. Киберфизическая система.

1.2. Киберобщество. Киберденьги. Кибермошенничество.

Модуль 2. Современная информационная культура.

2.1. Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство.

2.2. Социальная инженерия. Классификация угроз социальной инженерии.

2.3. Новые профессии в киберобществе. Цифровизация профессий.

Линия «Информационное пространство и правила информационной безопасности»

Модуль 3. Угрозы информационной безопасности.

3.1. Киберугрозы. Кибервойны. Киберпреступность.

Уязвимости кибербезопасность.

Запрещенные и нежелательные сайты.

3.2. Защита от вредоносных программ и информационных атак.

3.3. Практика электронного обучения в сфере информационной безопасности.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРОГРАММЕ

Программа учебного курса «Информационная безопасность» отражает в содержании цели поддержки и сопровождения безопасной работы с информацией в учебно-познавательной, творческой и досуговой деятельности (планируемые личностные, метапредметные и предметные результаты освоения курса).

В соответствии с федеральным государственным образовательным стандартом основного общего образования необходимо сформировать у обучающихся с учетом возрастных особенностей на каждом уровне общего образования такие *личностные результаты*, которые позволят им грамотно ориентироваться в информационном мире с учетом имеющихся в нем угроз:

— принимать ценности человеческой жизни, семьи, гражданского общества, многонационального российского народа, человечества;

— быть социально активными, уважающими закон и правопорядок, соизмеряющими свои поступки с нравственными ценностями, осознающими свои обязанности перед семьей, обществом, Отечеством;

— уважать других людей, уметь вести конструктивный диалог, достигать взаимопонимания, сотрудничать для достижения общих результатов;

— осознанно выполнять правила здорового образа жизни, безопасного для человека и окружающей его среды.

В рамках достижения этих личностных результатов при реализации программы курса информационной безопасности наиболее актуально в условиях быстро меняющегося и несущего в себе угрозы информационного мира обеспечить:

— развитие морального сознания и компетентности в решении моральных проблем на основе личностного выбора, формирование нравственных чувств и нравственного поведения, осознанного и ответственного отношения к собственным поступкам;

— формирование ценности здорового и безопасного образа жизни; усвоение правил индивидуального и коллективного безопасного поведения в чрезвычайных ситуациях, угрожающих жизни и здоровью людей.

В результате освоения программы курса информационной безопасности акцентируется внимание на *метапредметных результатах* освоения основной образовательной программы:

— освоение социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах, включая взрослые и социальные сообщества; участие в школьном самоуправлении и общественной жизни в пределах возрастных компетенций с учетом региональных, этнокультурных, социальных и экономических особенностей;

— формирование коммуникативной компетентности в общении и сотрудничестве со сверстниками, детьми старшего и младшего возраста, взрослыми в процессе образовательной, общественно полезной, учебно-исследовательской, творческой и других видов деятельности;

— умение использовать средства информационно-коммуникационных технологий (ИКТ) в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности.

Планируется достижение *предметных результатов*, актуальных для курса информационной безопасности в интеграции с предметами «Информатика» для 7—9 классов.

Линия «Информационное пространство и правила информационной безопасности»:

— формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики;

— умение принимать обоснованные решения в конкретной опасной ситуации с учетом реально складывающейся обстановки и индивидуальных возможностей.

В результате освоения программы курса с учетом возрастных групп выпускник освоит жизненно важные практические компетенции.

Выпускник научится понимать:

— источники информационных угроз, вредоносные программы и нежелательные рассылки, поступающие на мобильный телефон, планшет, компьютер;

— роль близких людей, семьи, правоохранительных органов для устранения проблем и угроз в сети Интернет и мобильной телефонной связи, телефоны экстренных служб;

— виды информационных угроз, правила поведения для защиты от угроз, виды правовой ответственности за проступки и преступления в сфере информационной безопасности;

— проблемные ситуации и опасности в сетевом взаимодействии и правила поведения в проблемных ситуациях, ситуациях профилактики и предотвращения опасности;

— этикет сетевого взаимодействия, правовые нормы в сфере информационной безопасности;

— правила защиты персональных данных;

— назначение различных позитивных ресурсов в сети Интернет для образования и в профессиях будущего.

Выпускник научится применять на практике:

— правила цифровой гигиены для использования средств защиты персональных данных (формировать и использовать пароль, использовать код защиты персонального устройства, регистрироваться на сайтах без распространения личных данных);

— компетенции медиаинформационной грамотности при работе с информацией в сети Интернет, критическое и избирательное отношение к источникам информации;

— компетенции компьютерной грамотности по защите персональных устройств от вредоносных программ, использованию антивирусных программных средств, лицензионного программного обеспечения;

— информационно-коммуникативные компетенции по соблюдению этических и правовых норм взаимодействия в социальной сети или в мессенджере, умение правильно вести себя в проблемной ситуации (оскорбления, угрозы, предложения, агрессия, вымогательство, ложная информация и др.), отключаться от нежелательных контактов, действовать согласно правовым нормам в сфере информационной безопасности (защиты информации).

Выпускник освоит нормы культуры информационной безопасности в системе универсальных учебных действий для самостоятельного использования в учебно-познавательной и досуговой деятельности позитивного Интернета и средств электронного обучения с соблюдением правил информационной безопасности.

Для выявления достижения планируемых результатов обучения рекомендуется использовать диагностические тесты и опросы, проектные работы и конкурсы по информационной безопасности в образовательных организациях.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ КУРСА

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

№ п/п	Наименование разделов и тем программы	Количество часов Всего	Основное содержание	Основные виды деятельности обучающихся	Формы проведения занятий	Электронные (цифровые) образовательные ресурсы
1	**Модуль 1.** Современное информационное пространство и искусственный интеллект	10	Киберпространство. Кибермиры. Киберфизическая система. Кибероблество. Киберденьги. Кибермошенничество. Практикум Практическая работа на основе онлайнкурса Академии Яндекс «Безопасность в Интернете» по теме «Безопасные онлайн-платежи».	Практическая работа с ресурсами и программами на компьютере		Авторские презентации, ресурсы сети интернет
2	**Модуль 2.** Современная информационная культура	10	Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство. Социальная инженерия. Классификация угроз социальной инженерии. Практическая работа от компаний мобильной связи Билайн, МТС и Мегафон (по выбору учащихся)	Практическая работа с ресурсами и программами на компьютере		Авторские презентации, ресурсы сети интернет
3	**Модуль 3.** Угрозы информационной безопасности	10	Кибервойны. Киберпреступность. Примеры киберпреступлений. Уязвимости кибербезопасности. Угрозы информационной безопасности. Запрещенные и нежелательные сайты. Новые профессии в кибероблестве. Практическая работа на основе онлайн- курса Академии Яндекса «Безопасность в Интернете» (продолжение), по темам: защита от вредоносных программ; безопасность аккаунтов.	Практическая работа с ресурсами и программами на компьютере		Авторские презентации, ресурсы сети интернет
4	Резервное время	4				

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

ОБЯЗАТЕЛЬНЫЕ УЧЕБНЫЕ МАТЕРИАЛЫ ДЛЯ УЧЕНИКА

1. Роскомнадзор, официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, URL: http://rkn.gov.ru/
2. Цветкова М. С., Якушина Е. В. Информационная безопасность. Правила безопасного Интернета. 2–4 классы : учебное пособие.— М.: БИНОМ. Лаборатория знаний, 2020. — 112 с.
3. Цветкова М. С., Якушина Е. В. Информационная безопасность. Безопасное поведение в сети Интернет. 5–6 классы : учебное пособие. — М.: БИНОМ. Лаборатория знаний, 2020. — 96 с.
4. Цветкова М. С., Хлобыстова И. Ю. Информационная безопасность. Кибербезопасность. 7–9 классы : учебное пособие. — М.: БИНОМ. Лаборатория знаний, 2020. — 64 с.
5. Цветкова М. С., Голубчиков С. В., Новиков В. К., Семибратов А. М., Якушина Е. В. Информационная безопасность: Правовые основы информационной безопасности. 10–11 классы : учебное пособие. — М.: БИНОМ. Лаборатория знаний, 2020. — 112 с.

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ УЧИТЕЛЯ

1. Цветкова, М.С. Информационная безопасность. 2–11 классы : методическое пособие для учителя / М. С. Цветкова. — М.: БИНОМ. Лаборатория знаний, 2020.

ЦИФРОВЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ И РЕСУРСЫ СЕТИ ИНТЕРНЕТ

1. Сайт электронного приложения к пособиям по информационной безопасности, URL: http://lbz.ru/metodist/ authors/ib/
2. «Безопасный Билайн», компания Билайн, URL: http:// moskva.beeline.ru/customers/help/safe-beeline/
3. «Безопасность», компания МТС, URL: http://www.safety. mts.ru/ru/
4. «Безопасное общение», компания Мегафон, URL: http:// moscow.megafon.ru/bezopasnoe_obschenie/
5. «Памятка по безопасному общению», компания Мегафон, URL: http://moscow.megafon.ru/download/~msk/~moscow/ stopfraud/brochure.pdf
6. Открытый онлайн-курс «Безопасность в Интернете», «Ака демия Яндекс», компания Яндекс, URL: https:// academy.yandex.ru/events/online-courses/internet_security/

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ДЕПАРТАМЕНТ ОБЩЕГО ОБРАЗОВАНИЯ ТОМСКОЙ ОБЛАСТИ
УПРАВЛЕНИЕ ОБРАЗОВАНИЯ АДМИНИСТРАЦИИ
КОЛПАШЕВСКОГО РАЙОНА
МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ТОГУРСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА
ИМЕНИ ГЕРОЯ РОССИИ СЕРГЕЯ ВЛАДИМИРОВИЧА МАСЛОВА»

«СОГЛАСОВАНО»

Заместитель директора

«_____»___2023 г.

_____ Зинова О.Г.
Подпись ФИО заместителя директора

ПОУРОЧНОЕ ПЛАНИРОВАНИЕ

внеурочной деятельности
(учебного предмета; элективного курса; внеурочной деятельности)

Информационная безопасность
(наименование учебного предмета, элективного курса, курса внеурочной деятельности)

основное общее образование
(уровень образования: начальное общее, основное общее, среднее общее образование)

_____
(класс)

на 2023-2024 учебный год

Учитель _____
предмет

_____
ФИО

Поурочное планирование

Учитель: Трифонова О.Ю.
Класс: 8
Предмет: Информационная безопасность
УМК:
Запланировано: 34

№ п.п.	Модуль/тема	Всего часов	Контрольные работы	Практическая работа	Дата план	Дата факт
	Модуль 1. Современное информационное пространство и искусственный интеллект	*11*	*5*	*5*		
	Киберпространство. Кибермиры.	2		1		
	Киберфизическая система.	2		1		
	Киберобщество. Киберденьги.	2		1		
	Кибермошенничество	2		1		
	Практическая работа на основе онлайнкурса Академии Яндекс «Безопасность в Интернете» по теме «Безопасные онлайнплатежи».	2		2		
	Обобщение по теме «Современное информационное пространство и искусственный	1	1			

	интеллект»					
	Модуль 2. Современная информационная культура	*11*	*1*	*6*		
	Киберкультура.	*2*		*1*		
	От книги к гипертексту. Киберкнига.	*2*		*1*		
	Киберискусство.	*2*		*1*		
	Социальная инженерия. Классификация угроз социальной инженерии	*1*		*0,5*		
	Новые профессии в киберобществе. Цифровизация профессий	*1*		*0,5*		
	Практическая работа от компаний мобильной связи Билайн, МТС и Мегафон (по выбору учащихся)	*2*		*2*		
	Обобщение по теме «Современная информационная культура»	*1*	*1*			
	Модуль 3. Угрозы информационной безопасности	*12*	*2*	*7*		
	Киберугрозы. Кибервойны.	2		1		

	Киберпреступность.					
	Уязвимости кибербезопасности. Угрозы информационной безопасности.	2		1		
	Запрещенные и нежелательные сайты	2		1		
	Защита от вредоносных программ и информационных атак	3	1	2		
	Практическая работа на основе онлайнкурса Академии Яндекса «Безопасность в Интернете» (продолжение), по темам: защита от вредоносных программ; безопасность аккаунтов	2		2		
	Обобщение по теме «Угрозы информационной безопасности»	1	1			
	Всего:	30	13	17		