Муниципальное бюджетное общеобразовательное учреждение
«Школа № 65 имени Героя Советского Союза В.Д Андреянова»
городского округа Самара
(МБОУ Школа № 65 г.о. Самара)
443008, г. Самара, ул. Ново-Вокзальная, д. 19, ИНН 6319034904, КПП 631901001
Эл.почта: sam-school65@63edu.ru, тел.:374-52-44

«РАССМОТРЕНО»
на заседании методического
объединения классных руководителей
протокол № 2
от 25.08 2026г.
_____/Гривцова Ю.Е./

«УТВЕРЖДАЮ»
Директор МБОУ Школа № 65
_____/Дементьева О.В./
Приказ №166-од от 27.08 2026 г.

«ПРОВЕРЕНО»
Заместитель директора
_____/Гуракова Е.С./
26.08 2026 г.

РАБОЧАЯ ПРОГРАММА
ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

Информационная безопасность

Для 5 - 9 классов

Рабочая программа по внеурочной деятельности «Информационная безопасность» составлена для учащихся 5-9 классов, а также родителям обучающихся всех возрастов.

Программа разработана на основе учебного пособия Наместникова М.С. «Информационная безопасность, или на расстоянии одного вируса» 7-9 классы, Просвещение 2019 год и направлена на достижение следующих планируемых результатов Федерального государственного образовательного стандарта основного общего образования:

- личностных.
- метапредметных (регулятивных, познавательных, коммуникативных);
- предметных;

Курс является важной составляющей частью работы с учащимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.), задумывающимися о своей личной безопасности, безопасности своей семьи и своих друзей, а также проявляющими интерес к изучению истории и технологических основ информационной безопасности. Кроме того, реализация курса создаст условия для сокращения цифрового разрыва между поколениями и позволит родителям выступать в качестве экспертов, передающих опыт. Направление программы курса внеурочной деятельности – общеинтеллектульное.

Программа курса ориентирована на выполнение требований Федерального государственного образовательного стандарта основного общего образования к организации и содержанию внеурочной деятельности школьников. Ее реализация даёт возможность раскрытия индивидуальных способностей школьников, развития интереса к различным видам индивидуальной и групповой деятельности, закрепления умения самостоятельно организовать свою учебную, в том числе проектную деятельность.

В основу рабочей программы взяты следующие нормативно-правовые документы:

1. Федеральный закон РФ от 31.07.2020г. "О внесении изменений в Федеральный закон "Об образовании в Российской Федерации" по вопросам воспитания обучающихся"
2. Приказ Министерства просвещения Российской Федерации от 11.12.2020г. № 712 "О внесении изменений в некоторые федеральные государственные образовательные стандарты общего образования по вопросам воспитания обучающихся"
3. Приказ Министерства просвещения Российской Федерации от 31.05.2021 № 287 «Об утверждении федерального государственного образовательного стандарта основного общего образования»
4. Концепция духовно-нравственного развития и воспитания личности гражданина России;
5. Информационно-методическое письмо Минпросвещения Российской Федерации «Методические рекомендации по организации внеурочной деятельности» от 05.07.2022 № ТВ-1290/03
6. Рабочая программа воспитания обучающихся ГБОУ СОШ им. М.П.Крыгина с. Кабановка;
7. Примерная рабочая программа учебного курса «Цифровая гигиена»/ Министерство образования и науки Самарской области, 2019.
8. М.С. Наместникова. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы/ М.: Просвещение,2019

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 тремя разделами по возрастным группам: для 5—6 классов, 7—9 классов и родители.

Реализация программы учебного курса возможна в разных формах:

— как дополнительные модули обучения в интеграции с предметами «Информатика» и (или) «ОБЗР».

— 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.

Цель программы:

формирование активной позиции школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им;

обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз.

Задачи программы:

дать представление о современном информационном обществе,информационной безопасности личности и государства;

сформировать навыки ответственного и безопасного поведения современнойинформационно-телекоммуникационной среде;

сформировать навыки по профилактике и коррекции зависимого поведенияшкольников, связанного с компьютерными технологиями и Интернетом;

сформировать общекультурные навыки работы с информацией (умений грамотно пользоваться источниками информации, правильно организовать информационный процесс);

дать представление о видах и способах распространения вредоносных кодов, способов защиты личных устройств;

познакомить со способами защиты от противоправных посягательств в сети Интернет, защиты личных данных.

СОДЕРЖАНИЕ

УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Содержание учебного курса «Информационная безопасность» для разных возрастных модулей программы складывается из двух линий:

1) Информационное общество и информационная культура.
2) Информационное пространство и правила информационной безопасности.

5 – 6 классы

Линия «Информационное общество и информационная культура»

Модуль1.Информационноеобщество.

Информационное общество. История создания сети Интернет. Что такое Всемирная паутина? Интернет как глобальная компьютерная сеть.

Как стать пользователем Интернета. Опасности для пользователей Интернета. Сайты, электронные сервисы.

Угрозы в сети Интернет.
Защита личных данных в сети Интернет.
Сетевой этикет.
Коллекции сайтов для детей .Электронные музеи.
Линия «Информационное пространство и правила информационной безопасности»
Модуль 2.ПравилапользователейсетиИнтернет.
Работа с СМС, электронной почтой, видеосервисами, в чатах и социальных сетях. Что такое информационная безопасность.
Защита от вредоносных программ и нежелательных рассылок, от негативных сообщений, защита своих устройств от внешнего вторжения.
Общение в социальной сети, работа с поисковыми системами и анализ информации, ответственность за распространение ложной и негативной информации, защита от нежелательных сообщений и контактов, вызов экстренной помощи.
Использование полезных ресурсов в сети Интернет, работа в сети Интернет для людей с особыми потребностями.

7—9классы

Линия «Информационное общество информационная культура»

Модуль 1. Современное информационное пространство и искусственный интеллект.

1.1. Киберпространство. Кибермиры. Киберфизическая система.
1.2.Кибероблество.Киберденьги.Кибермошенничество.
Модуль 2. Современная информационная культура.
Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство.

Социальная инженерия. Классификация угроз социальной инженерии.

Новые профессии в кибероблестве. Цифровизация профессий.

Линия «Информационное пространство и правила информационной безопасности»
Модуль 3.Угрозы информационной безопасности.
Киберугрозы. Кибервойны. Киберпреступность.
Уязвимости кибербезопасность.
Запрещенные и нежелательные сайты.
Защита от вредоносных программ и информационных атак.
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 быстроменяющегося 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»и(или) «ОБЗР» для 5—6 и 7—9классов.

Линия «Информационное общество и информационная культура»:

— понимание личной и общественной значимости современной культуры безопасности жизнедеятельности;

— знание основных опасных и чрезвычайных ситуаций социального характера, включая экстремизм и терроризм, и их последствий для личности, общества игосударства; формирование антиэкстремистской и антитеррористической личностной позиции;

— знание и умение применять меры безопасности и правила поведения в условиях опасных и чрезвычайных ситуаций.

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 медиа информационной грамотности при работе с информацией в сети Интернет, критическое и избирательное отношение к источникам информации;

— компетенциикомпьютернойграмотностипозащитеперсональныхустройствот 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»

5—6 классы

Программа учебного курса для 5—6 классов основного общего образования рассчитана на объем не менее 30 часов. Программа курса может быть реализована по выбору образовательной организации как самостоятельный учебный курс во внеурочной деятельности детей за один год обучения или отдельными модулями в программах освоения учебных предметов «Информатика» и (или) «ОБЖ» (в 5—6 классах), а также в рамках школьных мероприятий с участием родителей интегрирована модулями в календарное планирование программы воспитания.

Варианты учебного планирования:

Вариант 1. Планирование обучения за один год обучения. Один урок в неделю. 68 уроков.

Вариант 2.Планирование обучения по модулям в 5 — 6 классах.

Модуль 1, всего 34 урока.

Модуль 2, всего34урока.

Модуль/тема	**Всего часов**	**Теоретические занятия**	**Практическая работа с ресурсами и программами на компьютере**
Линия «Информационное общество и Информационная культура»	***34***	***13***	***21***
Модуль1. Информационное общество	*34*	*13*	*21*
1.1.Информационное общество	6	3	3
1.2.Интернет как глобальная компьютерная сеть. Сайты, электронные сервисы. Коллекции сайтов для учебной и познавательной деятельности	9	2	7
1.3.Угрозы в сети Интернет. Защита личных данных в Сети Интернет	12	6	6
1.4.Сетевой этикет. Коллекции сайтов для детей. Электронные музеи	7	2	5
Линия «Информационное пространство и правила информационной безопасности»	***34***	***14***	***20***

Модуль2.Правила пользователей сети Интернет	*34*	*14*	*20*
2.1.Работа с СМС, Электронной почтой, видеосервисами, в чатах и социальных сетях	6	3	3
2.2.Защита от вредоносных программ и нежелательных рассылок, от негативных сообщений, защита своих устройств от внешнего вторжения	7	3	4
2.3.Общениевсоциальной сети, работа с поисковыми системами и анализ информации, ответственность за распространение ложной и негативной информации, защита от нежелательных сообщений и контактов, вызов экстренной помощи	13	6	7
2.4.Использование полезных ресурсов в сети Интернет, работа в сети Интернет для людей с особыми потребностями	8	2	6
Всего:	68	27	41

7—9классы

Программа учебного курса для 7—9 классов основного общего образования рассчитана на объем не менее 30 часов. Программа курса может быть реализована по выбору образовательной организации как самостоятельный учебный курс во внеурочной деятельности детей за один год обучения или отдельными модулями в программах освоения учебных предметов «Информатика» и (или) «ОБЗР» (в 7—9 классах), а также в рамках школьных мероприятий с участием родителей интегрирована модулями в календарное планирование программы воспитания.

Варианты учебного планирования:

Вариант 1.Планированиеобучениязаодингодобучения.Одинуроквнеделю.102 урока.

Вариант 2.Планированиеобученияпомодулямв7—9классах.

Модуль 1, всего 34 урока.

Модуль 2, всего34урока.

Модуль 3, всего34урока.

Модуль/тема	**Всего часов**	**Теоретические занятия**	**Практическая работа с ресурсами и программами на компьютере**
Линия «Информационное общество и информационная культура»	***68***	***17***	***51***
Модуль1.Современное информационное пространство и искусственный интеллект	*34*	*7*	*27*
1.1.Киберпространство. Кибермиры. Киберфизическая система	15	3	12
1.2.Кибероbщество. Киберденьги. Кибермошенничество	19	4	15
Модуль2. Современная Информационная культура	*34*	*10*	*24*
2.1.Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство.	10	4	6
2.2.Социальная инженерия. Классификация угроз	12	4	8
социальной инженерии 2.3.Новые профессии в кибероbществе. Цифровизация профессий	12	2	10

Линия «Информационное пространство и правила информационной безопасности»	***34***	***12***	***22***
Модуль3. Угрозы информационной безопасности	*34*	*12*	*22*
3.1.Киберугрозы. Кибервойны. Киберпреступность. Уязвимости кибербезопасности. Угрозы информационной безопасности. Запрещенные и Нежелательные сайты	10	4	6
3.2.Защитаот Вредоносных программ и информационных атак	10	4	6
3.3. Практика электронного обученияв сфере информационной безопасности	14	4	10
Всего:	102	29	73

Работа с родителями

При работе с родителями важнейшей задачей является преодоление «цифрового разрыва» и обучение родителей правильной оценке своих возможностей в помощи детям в Интернете – возможностей, которые достаточно велики.

Разработчики курса предполагают, что родители с бóльшей готовностью включатся в программу развития цифровой гигиены, предлагающую им общение, совместный поиск и развивающие игры и т.п.

Вместе с тем, формами проведения мероприятий для родителей также могут являться: лектории, выступления на родительских собраниях, микрообучение на основе технологий онлайн обучения, геймификация, создание чек-листов, совместное обучение, совместные родительско-детские проекты и пр.

Разработчики курса «Цифровая гигиена» предлагают использовать вышеуказанное приложение в качестве конструктора при подготовке к мероприятиям.

Тематическое планирование учебного курса (для родителей).

Тема 1. История возникновения Интернета. Понятия Интернет угроз. Изменения границ допустимого в контексте цифрового образа жизни

Тема 2. Изменения нормативных моделей развития и здоровья детей и подростков.

Тема 3. Цифровая гигиена: зачем это нужно? Понятие периметра безопасности. Обеспечение эмоционально-психологического периметра безопасности в соответствии с возрастными особенностями ребенка. Баланс ценностей развития и ценностей безопасности.

Тема 4. Угрозы информационной безопасности: атаки, связанные с компьютерной инженерией. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Тема 5. Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Груминг, кибербуллинг. Чему мы должны научить ребёнка для профилактики насилия в Сети?

Тема 6. Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Фишинг.

Обращение с деньгами в сети Интернет. Детская пластиковая карта: быть или не быть?
Тема 7. Контентные риски. Настройка и безопасное использование смартфона или планшета. Семейный доступ.
Тема 8. Пособия и обучающие программы по формированию навыков цифровой гигиены.