МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Департамент образования и науки ХМАО-Югры

Департамент образования администрации г. Лангепаса

ЛГ МАОУ "СОШ № 1"

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
Руководитель ШМО	Заместитель директора по УР	Директор школы
_____	_____	_____
И.Л. Марченко Протокол № 2 от «31» 08 2023 г.	И.А. Шайнурова «31» 08 2023 г.	Н.В.Шахматова приказ № 526-о от «31» 08 2023 г.

РАБОЧАЯ ПРОГРАММА

(ID 1863635)

Курса внеурочной деятельности «Информационная безопасность (базовый уровень)»

для обучающихся 9 классов

г. Лангепас

2023 г.

Нормативную правовую основу образовательной программы по 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.

Образовательная программа по 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 курса «Информационная безопасность» в 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 9 классов.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа 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.

Общая характеристика 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 внеурочной деятельности для 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.

Цели изучения 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 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.

Целевая аудитория. Учащиеся 9 классов

Место курса «Информационная безопасность» в плане внеурочной деятельности

На изучение курса «Информационная безопасность» в 9 классе отводится 34 часа (1 час в неделю).

Программа курса ориентирована на включение в контекст обучения и воспитания новых видов информационных угроз и средств противодействия им.

— в рамках отдельного 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 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.

СОДЕРЖАНИЕ КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Содержание 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.

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 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» и (или) «ОБЖ».

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 и государства; 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 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»

Модуль/тема	Всего часов	Теоретические занятия	Практическая работа с ресурсами и программами на компьютере
Линия «Информационное общество и информационная культура»	***21***	***10***	***11***
Модуль 1. Современное информационное пространство и искусственный интеллект	*11*	*6*	*5*
1.1. Киберпространство. Кибермиры. Киберфизическая система	5	2	3
1.2. Киберобщество. Киберденьги. Кибермошенничество	6	4	2
Модуль 2. Современная информационная культура	*10*	*4*	*6*
2.1. Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство.	4	2	2
2.2. Социальная инженерия. Классификация угроз социальной инженерии	4	2	2
2.3. Новые профессии в киберобществе. Цифровизация профессий	2		2
Линия «Информационное пространство и правила информационной безопасности»	***13***	***6***	***6***

Модуль 3. Угрозы информационной безопасности	*13*	*6*	*6*
3.1. Киберугрозы. Кибервойны. Киберпреступность. Уязвимости кибербезопасности. Угрозы информационной безопасности. Запрещенные и нежелательные сайты	6	4	2
3.2. Защита от вредоносных программ и информационных атак	3	1	2
3.3. Практика электронного обучения в сфере информационной безопасности	3	1	2
Итоговое тестирование	1		
Всего:	34	12	17

КАЛЕНДАРНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ (9 А, В КЛАССЫ)

№ п/п	Тема урока	Количество часов	Дата изучения	Электронные цифровые образовательные ресурсы
Модуль 1. Современное информационное пространство и искусственный интеллект **(11 ч)**				
1	Киберпространство.	1	02.10.2023	https://resh.edu.ru/subject/38/
2	Кибермиры.	2	09.10.2023 16.10.2023	https://resh.edu.ru/subject/38/
3	Киберфизическая система	2	23.10.2023 30.10.2023	https://resh.edu.ru/subject/38/
4	Киберобщество.	1	06.11.2023	https://resh.edu.ru/subject/38/
5	Киберденьги.	2	13.11.2023 20.11.2023	https://resh.edu.ru/subject/38/
6	Кибермошенничество	3	27.11.2023 04.12.2023	https://resh.edu.ru/subject/38/
Модуль 2. Современная информационная культура **(10 ч)**				
7	Киберкультура.	1	11.12.2023	https://resh.edu.ru/subject/38/
8	От книги к гипертексту.	1	18.12.2023	https://resh.edu.ru/subject/38/
9	Киберкнига.	1	25.12.2023	https://resh.edu.ru/subject/38/
10	Киберискусство.	1	01.01.2024	https://resh.edu.ru/subject/38/

11	Социальная инженерия	2	08.01.2024 15.01.2024	https://resh.edu.ru/subject/38/
12	Классификация угроз социальной инженерии	2	22.01.2024 29.01.2024	https://resh.edu.ru/subject/38/
13	Новые профессии в киберобществе.	1	05.02.2024	https://resh.edu.ru/subject/38/
14	Цифровизация профессий	1	12.02.2024	https://resh.edu.ru/subject/38/
Модуль 3. Угрозы информационной безопасности **(13 ч)**				
15	Киберугрозы.	1	19.02.2024	https://resh.edu.ru/subject/38/
16	Кибервойны.	1		https://resh.edu.ru/subject/38/
17	Киберпреступность.	1	26.02.2024	https://resh.edu.ru/subject/38/
18	Уязвимости кибербезопасности.	1		https://resh.edu.ru/subject/38/
19	Угрозы информационной безопасности.	1	04.03.2024	https://resh.edu.ru/subject/38/
20	Запрещенные и нежелательные сайты	1	11.03.2024	https://resh.edu.ru/subject/38/
21	Защита от вредоносных программ и информационных атак	3	15.04.2024 22.04.2024 29.04.2024	https://resh.edu.ru/subject/38/
22	Практика электронного обучения в сфере информационной безопасности	3	06.05.2024 13.05.2024 20.05.2024	https://resh.edu.ru/subject/38/

23	Итоговое тестирование	1		https://resh.edu.ru/subject/38/

КАЛЕНДАРНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ (9 Б КЛАСС)

№ п/п	Тема урока	Количество часов	Дата изучения	Электронные цифровые образовательные ресурсы
Модуль 1. Современное информационное пространство и искусственный интеллект **(10 ч)**				
1	Киберпространство.	1	06.10.2023	https://resh.edu.ru/subject/38/
2	Кибермиры.	2	13.10.2023 20.10.2023	https://resh.edu.ru/subject/38/
3	Киберфизическая система	2	27.10.2023 10.11.2023	https://resh.edu.ru/subject/38/
4	Киберобщество.	1	17.11.2023	https://resh.edu.ru/subject/38/
5	Киберденьги.	2	24.11.2023 01.12.2023	https://resh.edu.ru/subject/38/
6	Кибермошенничество	2	08.12.2023 15.12.2023	https://resh.edu.ru/subject/38/
Модуль 2. Современная информационная культура **(10 ч)**				
7	Киберкультура.	1	22.12.2023	https://resh.edu.ru/subject/38/

8	От книги к гипертексту.	1	12.01.2024	https://resh.edu.ru/subject/38/
9	Киберкнига.	1	19.01.2024	https://resh.edu.ru/subject/38/
10	Киберискусство.	1	26.01.2024	https://resh.edu.ru/subject/38/
11	Социальная инженерия	2	02.02.2024 09.02.2024	https://resh.edu.ru/subject/38/
12	Классификация угроз социальной инженерии	2	16.02.2024 23.02.2024	https://resh.edu.ru/subject/38/
13	Новые профессии в киберобществе.	1	01.03.2024	https://resh.edu.ru/subject/38/
14	Цифровизация профессий	1	08.03.2024	https://resh.edu.ru/subject/38/
Модуль 3. Угрозы информационной безопасности **(10 ч)**				
15	Киберугрозы. Кибервойны.	1	15.03.2024	https://resh.edu.ru/subject/38/
16	Киберпреступность. Уязвимости кибербезопасности.	1	22.03.2024	https://resh.edu.ru/subject/38/
17	Угрозы информационной безопасности.	1	29.03.2024	https://resh.edu.ru/subject/38/
18	Запрещенные и нежелательные сайты	1	05.04.2024	https://resh.edu.ru/subject/38/
19	Защита от вредоносных программ и информационных атак	3	12.04.2024 19.04.2024 26.04.2024	https://resh.edu.ru/subject/38/

20	Практика электронного обучения в сфере информационной безопасности	3	03.05.2024 10.05.2024 17.05.2024	https://resh.edu.ru/subject/38/

Для реализации курса на основе программы необходимо наличие следующих *технических средств*:

- компьютерное рабочее место учителя, подключенное к сети Интернет (Wi-Fi или по кабелю),
- проекционное оборудование или интерактивная доска с возможностью демонстрации презентаций;
- компьютеры или ноутбуки, расположенные в компьютерном классе, где каждый ученик работает с устройством либо индивидуально, либо в парах;
- компьютеры или ноутбуки как учащихся, так и учителя должны быть на операционных системах Windows/MacOS;
- типовое программное обеспечение, применяемое общеобразовательными организациями;
- интегрированная среда разработки (IDE) для языка программирования Python;
- Jupyter Notebooks — среда разработки, для запуска файлов из материалов УМК с компьютера или из облачного хранилища.

Технические требования к ПО

<table>
<tr><td colspan="2">ПК или ноутбук на базе ОС Windows, MacOS</td></tr>
<tr><td>Системные требования Windows</td><td>Системные требования MacOS</td></tr>
<tr><td>● Операционная система Windows 7 или выше
● Процессор Intel® Core Duo или аналогичный с частотой 1,5 ГГц или выше
● 2/4 ГБ оперативной памяти для систем под управлением 32/64-битной Windows</td><td>● Операционная система MacOS X 10.10 или выше
● Процессор Intel® Core Duo или аналогичный с частотой 1,5 ГГц или выше
● 1,5 ГБ оперативной памяти - Процессор Intel® Core Duo или аналогичный с частотой 1,5 ГГц или выше
● 1,5 ГБ оперативной памяти</td></tr>
<tr><td colspan="2">● Разрешение экрана 1024x768 или больше
● Наличие интернет-соединения
● Необходимо использовать актуальные версии одного из следующих браузеров: Edge, Chrome, Safari, Firefox, Opera</td></tr>
</table>

Формы аттестации

Выполнение итогового тестирования.

СПИСОК ЛИТЕРАТУРЫ И ЭЛЕКТРОННЫХ РЕСУРСОВ

1. Н.Н.Самылкина, «Готовимся к ЕГЭ по информатике», учебное пособие, элективный курс, изд-во Бином, Москва, 2008г.
2. Сайт информационной поддержки по ЕГЭ http://www.ege.ru/.
3. Сайт Федерального института педагогических измерений ФИПИ http://www.fipi.ru
4. Сайт РЦОКОиИТ http://ege.spb.ru/
5. Образовательный портал http://www.ege.edu.ru
6. Интернет-олимпиада по информатике СПбГУИТМО http://olymp.ifmo.ru
7. Свободный форум экспертов на сайте www.ege.spbinform.ru

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 6BE0D777A722CF157F987AF46689750D
Владелец: ШАХМАТОВА НАТАЛЬЯ ВЛАДИМИРОВНА
Действителен: С 25.04.2023 ДО 18.07.2024