МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ГОРОДА НОВОСИБИРСКА
«ЛИЦЕЙ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

Рабочая программа
по внеурочной деятельности
спецкурс «Информационная безопасность»

направление: информатика
Срок освоения: 1 год
Возраст обучающихся: 14 лет (8 класс)

г. Новосибирск, 2015

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая программа по внеурочной деятельности «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 учебного курса «Информационная безопасность» разработана для организаций, реализующих программы общего образования. *В ней учтены приоритеты научно-технологического развития Российской Федерации* (Пр-294, п. 2а16) и обновление программы воспитания и социализации обучающихся в школах Российской Федерации.

Рабочая программа разработана на основе нормативных документов:

1. ФЗ от 29.12.2012 273-ФЗ «Об образовании в Российской Федерации»;
2. Постановление Главного государственного санитарного врача РФ от 29 декабря 2010 г. №189 г. Москва «Об утверждении СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения в ОУ»
3. ФГОС ООО (Приказ Министерства просвещения РФ от 31 мая 2021 г. № 287 “Об утверждении федерального государственного образовательного стандарта основного общего образования”
4. ФОП ООО по информатике (углубленный уровень)

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.

Программа курса внеурочной деятельности 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»

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.

Задачи курса:

— 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.

ОБЩАЯ ХАРАКТЕРИСТИКА ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА: ТЕХНОЛОГИЙ, МЕТОДОВ, ФОРМ, СРЕДСТВ ОБУЧЕНИЯ И РЕЖИМ ЗАНЯТИЙ

Технологии, используемые в учебном процессе:

1. Информационно-коммуникационные технологии
2. Технология развития критического мышления
3. Проектная технология
4. Технология развивающего обучения
5. Здоровьесберегающие технологии
6. Технология проблемного обучения
7. Игровые технологии

ФОРМА ПРОВЕДЕНИЯ ЗАНЯТИЙ

Курс внеурочной деятельности рассчитан на 2 часа в неделю (68 часа в год). Обучение предусматривает групповую форму занятий в классе с учителем. Занятия предусматривают индивидуальную и групповую работу школьников, а также предоставляют им возможность проявить и развить свою самостоятельность. В курсе наиболее распространены следующие формы работы: обсуждения, дискуссии, решения задач и кейсов. Преобладающий тип занятий – практикум.

МЕСТО УЧЕБНОГО ПРЕДМЕТА «ИНФОРМАТИКА» В УЧЕБНОМ ПЛАНЕ

Программа курса ориентирована на включение в контекст обучения и воспитания новых видов информационных угроз и средств противодействия им. Реализация программы учебного курса представлена в рамках отдельного учебного курса по выбору «Информационная безопасность».

Рабочая программа курса составлена с использованием пособий «Информационная безопасность. Безопасное поведение в сети Интернет» Цветкова М. С., Якушина Е. В. – Издательство: Просвещение, 2022 г., «Информационная безопасность. Кибербезопасность» Цветкова М. С., Якушина Е. В. – Издательство:
Просвещение, 2023 г.

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.

ПЛАНИРУЕМЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

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;

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

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.

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;

— 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 учебнопознавательной 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.

•

СОДЕРЖАНИЕ УЧЕБНОГО ПРЕДМЕТА

Содержание учебного курса «Информационная безопасность» 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.

ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№ п/п	Тема занятия	Количество часов	Форма проведения занятий	Электронные цифровые образовательные ресурсы
1	*Линия «Информационное общество и информационная культура»* **Модуль 1.** Современное информационное пространство и искусственный интеллект	**20**	Беседа, просмотр видеоурока, обсуждение Практическая работа с ресурсами и программами на компьютере	https://lbz.ru/metodist/author s/ib/7-9.php
	1.1. Киберпространство. Кибермиры. Киберфизическая система	10		
	1.2. Кибероbщество. Киберденьги. Кибермошенничество	10		
2	**Модуль 2.** Современная информационная культура	**20**	Беседа, просмотр видеоурока, обсуждение Практическая работа с ресурсами и программами на компьютере	https://lbz.ru/metodist/author s/ib/7-9.php
	2.1. Киберкультура. От книги к гипертексту. Киберкнига. Киберискусство.	8		
	2.2. Социальная инженерия. Классификация угроз социальной инженерии	8		
	2.3. Новые профессии в кибероbществе. Цифровизация профессий	4		
3	*Линия «Информационное пространство и правила информационной безопасности»* **Модуль 3.** Угрозы информационной безопасности	**28**	Беседа, просмотр видеоурока, обсуждение	https://lbz.ru/metodist/author s/ib/7-9.php

	3.1. Киберугрозы. Кибервойны. Киберпреступность.	8	Практическая работа с	
	Уязвимости кибербезопасности. Угрозы информационной безопасности. Запрещенные и нежелательные сайты		ресурсами и программами на компьютере	
	3.2. Защита от вредоносных программ и информационных атак	10		https://apkpro.ru/informacionnaya-bezopasnost/
	3.3. Практика электронного обучения в сфере информационной безопасности	10		
	Итого по программе	**68**		

СПОСОБЫ ОЦЕНКИ ДОСТИЖЕНИЙ УЧАЩИМИСЯ ПЛАНИ РУЕМЫХ РЕЗУЛЬТАТОВ

ТЕКУЩЕЕ ОЦЕНИВАНИЕ

Содержание обучения по информатике на уровне основного общего образования предельно насыщено, поэтому время, которое может быть выделено для оценивания предметных результатов, очень ограничено. В связи с этим выбираются компактные и кратковременные форматы оценивания предметных результатов обучения. Предпочтения отдаются кратковременному устному или письменному опросу, преимущественно в тестовой форме из-за возможности его оперативного использования. Большая часть тем курса информатики рассчитана на формирование цифровых навыков на практике, поэтому практическая работа является и формой обучения, и одним из видов оценивания. В конце изучения темы проводится контрольная работа или контрольная практическая работа.

ТЕМАТИЧЕСКОЕ, ПРОМЕЖУТОЧНОЕ (РУБЕЖНОЕ) ОЦЕНИВАНИЕ

Тематическое оценивание направлено на выявление и оценку достижения образовательных результатов, связанных с изучением отдельных тем образовательной программы.

Промежуточное оценивание проводится по итогам изучения крупных блоков образовательной программы, включающих несколько тем, или формирование комплексного блока учебных действий (работа с различным программным обеспечением для обработки текста, графики, мультимедиа и пр.).

Промежуточное или тематическое оценивание проводится в конце изучения всего тематического раздела или большой темы из него, поэтому по используемым заданиям и критериям оценивания оно схоже с итоговым на этапе внешнего оценивания.

На завершающем этапе изучения темы проверяются освоение способов деятельности, которые свободно переносятся на решение актуальных задач, связанных с использованием цифрового окружения. Подразумевается, что обучающийся разбирается в функциональных связях между объектами изучения, освоил их и активно использует свои знания и навыки, например, в других темах или за пределами учебных ситуаций.

В случае использования достаточно объемного теста, рассчитанного на весь урок, при переводе набранных баллов в отметку по предмету используют подсчет процентного соотношения правильных и неправильных ответов, при этом:

- 85–100 % правильных ответов = «отлично»;
- 65–84 % правильных ответов = «хорошо»;
- 50–64 % правильных ответов = «удовлетворительно»;
- <50% правильных ответов = «неудовлетворительно».

ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОГО И УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ РАБОЧЕЙ ПРОГРАММЫ

Программное обеспечение (в том числе системное ПО)

1. Анализатор базовой безопасности Microsoft: Microsoft Baseline Security Analyzer (бесплатная);
2. Операционная система Winows 10;
3. am.Requirements (распространяется свободно);
4. AnyLogic 8.75 Personal Learning Edition (бесплатная);
5. Arduino IDE 1.8.15 (распространяется свободно);
6. Astra linux common edition (распространяется свободно);
7. Cisco Packet Tracer (бесплатная);
8. CoppeliaSim V4.2.0 rev5 EDU (распространяется свободно);
9. Enigmail for Thunderbird 2.1.9 (распространяется свободно);
10. fping 5.0 (распространяется свободно);
11. Google Chrome (распространяется свободно);
12. Gpg4win 3.1.16 (распространяется свободно);
13. Kaspersky Security Cloud;
14. Kaspersky Total Security;
15. KasperskyOS Community Edition (бесплатная);
16. Microsoft Security Assessment tool (бесплатная);
17. Mosquitto 2.0.11 (распространяется свободно);
18. nmap 7.91 (распространяется свободно);
19. PyCharm community edition (бесплатная);
20. Tails 4.20 (распространяется свободно);
21. The Amnesic Incognito Live System (распространяется свободно);
22. Thunderbird 78.0 (распространяется свободно);
23. Ubuntu for Raspberry Pi (распространяется свободно);
24. Ubuntu Server 18.04.5 (распространяется свободно);
25. VirtualBox 6.1 (распространяется свободно);
26. Visual Studio Code (распространяется свободно);
27. Wireshark is 3.4.6. (распространяется свободно);

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА
ОБЯЗАТЕЛЬНЫЕ УЧЕБНЫЕ МАТЕРИАЛЫ ДЛЯ УЧЕНИКА

Цветкова М. С., Якушина Е. В. Информационная безопасность. Правила безопасного Интернета. 7-9 классы : учебное пособие.— М.: БИНОМ. Лаборатория знаний, 2020 — 112 с.
https://lbz.ru/metodist/authors/ib/7-9.php

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ УЧИТЕЛЯ

7-9 классы

1. Роскомнадзор, официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых http://rkn.gov.ru/
2. Цветкова М. С., Якушина Е. В. Информационная безопасность. Правила безопасного Интернета. 7-9 классы : учебное пособие.— М.: БИНОМ. Лаборатория знаний, 2020 — 112 с.
3. Цветкова М. С., Якушина Е. В. Информационная безопасность. Безопасное поведение в сети Интернет. 7-9 классы : учебное пособие. — М.: БИНОМ. Лаборатория знаний, 2020 — 96 с.
4. Сайт электронного приложения к пособиям по информационной безопасности, URL: http://lbz.ru/metodist/authors/ib/
5. Открытый онлайн-курс «Безопасность в Интернете», https://lbz.ru/metodist/authors/ib/7-9.php

ЦИФРОВЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ И РЕСУРСЫ СЕТИ ИНТЕРНЕТ

7-9 классы

https://lbz.ru/metodist/authors/ib/7-9.php https://digital-likbez.datalesson.ru/ https://youthsafety.megafon.ru/
https://apkpro.ru/informacionnaya-bezopasnost/
http://lbz.ru/metodist/authors/ib/