ВОЛХОВСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН ЛЕНИНГРАДСКОЙ ОБЛАСТИ
МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ «ЦЕНТР ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ - ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

ПРИНЯТА
на заседании
педагогического совета
протокол №1 от 30.08.2024

УТВЕРЖДЕНА
приказом МБУДО «Центр информационных технологий»
от 30.08.2024 №66 ОД

Подписан: МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ " ЦЕНТР ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ - ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ"

Дополнительная общеразвивающая программа

социально-гуманитарной направленности

«Я/МЫ безопасность»

модуль «Нам не страшны интернет-угрозы»

Возраст обучающихся: 15-18 лет

Срок реализации: 1 год

Составитель программы:
методист Артемьева И.А.

Волхов

2024

Оглавление

Дополнительная общеразвивающая программа социально-гуманитарной направленности «Я/МЫ безопасность»

модуль «Нам не страшны интернет-угрозы»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа разработана в соответствии с требованиями:

- Федерального закона от 29.12.2010 N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»,
- Концепции информационной безопасности детей, утвержденной распоряжением Правительства РФ от 02.12.2015.
- Концепции развития дополнительного образования детей (утверждена Распоряжением Правительства Российской Федерации от 31.03.2022 № 678-р),

- Приказа Министерства Просвещения Российской Федерации от 27 июля 2022 года № 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»

- Приказа Министерства просвещения Российской Федерации от 05 августа 2020 № 882/391 «Об организации и осуществлении образовательной деятельности при сетевой форме реализации образовательных программ»
- Санитарно-эпидемиологических требований к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи» от 28.09.2020 г. № 28 (СП 2.4. 3648-20).

Актуальность.

На сегодняшний день практический каждый человек, так или иначе, пользуется сетью Интернет. Интернет – это возможность уникальной коммуникации, построенной на принципе равного доступа. Такой тип коммуникации позволяет объединять людей вокруг общих интересов или целей, выстраивая внутри общества горизонтальные связи. Мы живем в эпоху информационных и компьютерных технологий. У каждого в семье есть компьютер, ноутбук, планшет или смартфон. Мы уже не представляем свою жизнь без интернета. С каждым годом сообщество российских интернет-пользователей молодеет. Дети и подростки – активные пользователи интернета. Дети поколения Рунета растут в мире, сильно отличающемся от того, в котором росли их родители. Между тем, помимо огромного количества возможностей, интернет несет и множество рисков. Зачастую дети и подростки в полной мере не осознают все возможные проблемы, с которыми они могут столкнуться в сети.

Вопрос о безопасности встает на первое место. Безопасность использования интернета и информационных и коммуникационных технологий одна из актуальнейших и важнейших тем современности.

Особенности программы.

Программа «Нам не страшны интернет-угрозы» является одним из модулей программы социально-гуманитарной направленности «Я/МЫ безопасность» учреждений дополнительного образования Волховского муниципального района.

В требованиях ФГОС к предметным результатам освоения курса информатики для уровней начального, основного общего и среднего общего образования отсутствует предметная область «Основы безопасности в Интернете», но в рамках метапредметных результатов и предметных умений дисциплины «Информатика» вопросы информационной безопасности обозначены.

Новизна дополнительной общеобразовательной программы «Нам не страшны интернет-угрозы» заключена в достижении метапредметных результатов и предметных умений дисциплины «Информатика» по формированию навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в сети интернет, умений соблюдать нормы информационной этики и права.

Уровень программы – стартовый.

Адресат программы.
Программа предназначена для обучающихся 15-18 лет.

Формы обучения по программе.
Программа может быть реализована как дистанционно, так и в очной форме.

Практические работы в содержании программы возможно использовать в качестве вариативных, индивидуальных практических заданий разного уровня углубленности, доступности и степени сложности исходя из диагностики и стартовых возможностей каждого из участников рассматриваемой программы.

Формы организации деятельности: групповая, индивидуально-групповая.

Занятия проводятся в комбинированной, теоретической и практической форме:

- теоретическая часть занятия: основы безопасного поведения при работе с компьютерными программами, информацией в сети интернет, изучение терминов, беседа;

- практическая часть занятия: работа с мобильными устройствами; тесты, квесты, квизы.

Объем и сроки освоения программы, режим занятий.
Объем программы – 4 часа. Занятия по данной программе могут проводиться один раз в неделю в соответствии с нормами СП 2.4. 3648-20.

ЦЕЛЬ И ЗАДАЧИ ПРОГРАММЫ

Цель: изучить риски сети Интернет и методы борьбы с ними;

Задачи:

Образовательная: познакомиться с понятием «интернет-риски», изучить основные правила при работе в сети Интернет, рассмотреть ситуации при столкновении с какой-либо интернет-угрозой, рассказать о Лиге безопасного интернета;

Развивающая: развитие интереса к предмету, информационной культуры; формирование приёмов логического мышления; развитие способность анализировать и обобщать, делать выводы;

Воспитательная: воспитание аккуратности, точности, самостоятельности, привитие навыки групповой работы, сотрудничества.

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Название темы	Количество часов			Формы аттестации, контроля
		Всего	Теорет	Практ.	
1.	Классификайия рисков. Контентные риски. Коммуникационные риски.	1,5	0,5	1	
2.	Электронные риски. Потребительские риски. Лига безопасного интернета	1,5	0,5	1	
3.	Квест «безопасность в интернете»	1		1	
	ИТОГО	4	1	3	

СОДЕРЖАНИЕ

Классификация рисков.

1. *Контентные риски*

Это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д. Столкнуться с ними можно практически везде. Это и сайты, и социальные сети, и блоги, и торренты, и видеохостинги, фактически все, что сейчас существует в Интернете. Зачастую подобный материал может прийти от незнакомца по почте в виде спама или сообщения.

Негативные контентые материалы можно условно разделить на:

Незаконные, к которым могут относиться: детская порнография (включая изготовление, распространение и хранение); наркотические средства (изготовление, продажа, пропаганда употребления), все материалы, имеющие отношение к расовой или религиозной ненависти (экстремизм, терроризм, национализма и др.), а также ненависти или агрессивного поведения по отношению к группе людей, отдельной личности или животным), азартные игры и т.д.

Внутреннее законодательство каждой страны предусматривает различные виды наказания за распространение такой информации. В Российском законодательстве есть возможность в соответствии со статьями Уголовного кодекса РФ привлечь к административной и уголовной ответственности за распространение подобного негативного контента владельцев сайтов, а также авторов таких электронных текстов и видеопродукции.

Неэтичные, противоречащие принятым в обществе нормам морали и социальным нормам.

Подобные материалы не попадают под действие уголовного кодекса, однако могут оказывать негативное влияние на психику столкнувшимися с ними человека, особенно ребенка. Примерами таких материалов могут служить широко распространенные в сети изображения сексуального характера, в том числе и порнография, агрессивные онлайн игры, азартные игры, пропаганда нездорового образа жизни (употребление наркотиков, алкоголя, табака, анорексии, булимии), принесения вреда здоровью и жизни (различных способов самоубийства, аудионаркотиков, курительных смесей), нецензурная брань, оскорбления, и др. Информация, относящаяся к категории неэтичной может быть также направлена на манипулирование сознанием и действиями различных групп людей.

Контентные риски связаны с другими типами рисков Сети. Например, просмотр тех или иных видео-материалов может привести к заражению компьютера вирусами и потере важных данных. Очень многие распространители подобного негативного контента преследуют цель заразить компьютер, чтобы в дальнейшем иметь возможность манипулировать данными и действиями зараженного компьютера. Пропаганда негативных материалов также может идти через социальные сети, блоги, различные форумы. В данном случае контентные риски пересекаются с коммуникационными.

2. *Коммуникационные риски*

Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают в себя риск подвергнуться оскорблениям и нападкам со стороны других. Примерами таких рисков могут быть: незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др. Для подобных целей используются различные чаты, онлайн-мессенджеры (ICQ, Google talk, Skype и др.), социальные сети, сайты знакомств, форумы, блоги и т.д.

Даже если большинство пользователей существующих чат-систем (веб-чатов или IRC) обладают добрыми намерениями, существует, к сожалению, растущее число людей, использующих эти беседы со злым умыслом. В некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в интернете и др. В других случаях они могут оказаться педофилами в поисках жертвы. Выдавая себя за сверстника и устанавливая дружеские отношения с ребенком, они выведывают о нем много информации и понуждают к личной встрече.

Оказаться жертвой намного проще, чем кажется. Каждый участник той или иной социальной сети может признаться, что хотя бы один раз ему приходило непристойное предложение от неизвестного человека. Это беда не только социальных сетей. На любом популярном форуме, в блоговом сообществе и чате появляются такие участники, которые хамят и оскорбляют других участников.

3. *Электронные риски*

Электронные (кибер-) риски — это возможность столкнуться с хищением персональной информации, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке, шпионским программам и т.д.

К вредоносным программам относятся вирусы, черви и «троянские кони» – это компьютерные программы, которые могут нанести вред вашему семейному компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной Сети. Защита в социальных сетях — это

задача, которая не так давно стала актуальна для их пользователей. Буквально несколько месяцев назад, взлом страниц в социальных сетях превратился в один из основных способов распространения спама в Интернете.

В частности, теперь вирусное ПО (программное обеспечение), которое рассылает спам в социальной сети может быть установлено на ваш компьютер с любого сайта. И от вашего лица могут регулярно рассылаться абсолютно любые сообщения, избавиться от которых не поможет ни одна защита самого сайта. Хотя бы просто по той причине, что в этом случае потребуется не защита вашей страницы, а современное антивирусное программное обеспечение. Поэтому не забывайте обновлять свою антивирусную программу и следить за защитой своего компьютера.

К сожалению, вероятность наткнуться на подобные вредоносные программы очень велика. Помимо негативного воздействия на компьютер и мобильное устройство, можно стать жертвой еще одного вида кибер-преступления — кибер-мошенничества. В самом широком смысле мошенничество — это умышленный обман или злоупотребление доверием с целью получения какой-либо выгоды.

Мошенничество в сети Интернет (кибермошенничество) — один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный и финансовый ущерб.

4. *Потребительские риски. Лига безопасного интернета.*

Потребительские риски – злоупотребление в интернете правами потребителя. Включают в себя: риск приобретения товара низкого качества, различные поделки, контрафактная и фальсифицированная продукция, потеря денежных средств без приобретения товара или услуги, хищение персональной информации с целью кибер-мошенничества, и др.

Также дети, зачастую совершая онлайн покупки, могут растратить значительные суммы своих родителей, если каким-либо способом имели или получили к ним доступ.

Одним из самых распространенных видов данного типа рисков является мошенничество — это умышленный обман или злоупотребление доверием с целью получения какой-либо выгоды. Мошенничество, как правило, является преступлением.

Деятельность Лиги безопасного интернета.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ.

Требования к знаниям и умениям.

Предметные:

1. Сформированы знания о безопасном поведении при работе с компьютерными программами, информацией в сети интернет;

2. Сформированы умения соблюдать нормы информационной этики;

3. Сформированы умения безопасно работать с информацией, анализировать и обобщать полученную информацию.

Метапредметные:

1. Развиваются компьютерная грамотность и информационная культура личности в использовании информационных и коммуникационных технологий;
2. Развиваются умения анализировать и систематизировать имеющуюся информацию;
3. Развиваются познавательная и творческая активность в безопасном использовании информационных и коммуникационных технологий.

Личностные:

1. Вырабатывается сознательное и бережное отношение к вопросам собственной информационной безопасности;
2. Формируются и развиваются нравственные, этические, патриотические качества личности;
3. Стимулируется поведение и деятельность, направленные на соблюдение информационной безопасности.

Формы аттестации.

Способы определения планируемых результатов - педагогическое наблюдение, тесты, педагогический анализ результатов анкетирования, тестирования.

Формами подведения итогов реализации дополнительной общеобразовательной программы могут быть проведение квестов, квизов; выступления обучающихся по актуальным вопросам информационной безопасности с собственными мультимедийными презентациями на ученических мероприятиях.

Оценочные материалы.

Для отслеживания результативности можно использовать: педагогический мониторинг, включающий контрольные задания и тесты, диагностику личностного роста и продвижения, анкетирование, педагогические отзывы, ведение журнала учета или педагогического дневника, мониторинг образовательной деятельности, включающий самооценку обучающегося, оформление фотоотчета и т.д.

РАБОЧАЯ ПРОГРАММА ВОСПИТАНИЯ

Цели и задачи воспитания

Цель воспитания в МБУДО «Центр информационных технологий» - воспитание социально-активной, творческой, нравственно и физически здоровой личности, способной на сознательный выбор жизненной позиции, а также к духовному и физическому самосовершенствованию, саморазвитию в социуме. Данная цель ориентирована на обеспечение положительной динамики личностного развития обучающихся:

- ✓ освоение социально значимых знаний и норм и приобретении опыта социального взаимодействия;
- ✓ формирование опыта самоопределения (личного или профессионального) в различных сферах жизни;
- ✓ формирование современных компетентностей и грамотностей, соответствующих стратегиям социально-экономического развития РФ, актуальным вызовам будущего.

Для достижения поставленной воспитательной цели необходимо решить следующие ***задачи:***

1. использовать в воспитании обучающихся возможностей занятий по дополнительным общеобразовательным общеразвивающим программам, как источника поддержки и развития интереса детей к познанию и творчеству;
2. реализовывать потенциал событийного воспитания для формирования духовно-нравственных ценностей, укрепления и развития традиций детского объединения и образовательной организации, развития субъектной позиции обучающихся;
3. развивать социально-педагогическое партнерство МБУДО «Центр информационных технологий», для более эффективного достижения целей воспитания и социализации обучающихся;
4. поддерживать различные формы детской активности и самоуправления через развитие деятельности детских общественных объединений;
5. организовать содержательное партнерство с семьями обучающихся, их родителями (законными представителями) для более эффективного достижения целей воспитания.

Формы и методы воспитательной работы.

Главное в образовательном процессе дополнительного образования – успешность ребенка как результат педагогической деятельности, а мера этой успешности определяется только относительно личностного роста каждого ребенка.

Реализация воспитательного потенциала занятия предполагает следующее*:*

- использование воспитательных возможностей содержания учебного занятия по определенному направлению деятельности через демонстрацию детям примеров ответственного, гражданского поведения, проявления человеколюбия и добросердечности, через подбор соответствующих текстов для чтения, задач для решения, проблемных ситуаций для обсуждения в объединении;

-применение на занятии интерактивных форм работы обучающихся: интеллектуальных игр, стимулирующих познавательную мотивацию обучающихся; дискуссий, которые дают обучающимся возможность приобрести опыт ведения конструктивного диалога; групповой работы или работы в парах, которые учат командной работе и взаимодействию с другими детьми;

-включение в занятие игровых процедур, которые помогают поддержать мотивацию детей к получению знаний, налаживанию позитивных межличностных отношений в объединении, помогают установлению

доброжелательной атмосферы во время занятия;

-организация шефства мотивированных и эрудированных обучающихся над их слабоуспевающими сверстниками, дающего обучающимся социально- значимый опыт сотрудничества и взаимной помощи;

- инициирование и поддержка исследовательской деятельности обучающихся в рамках реализации ими индивидуальных и групповых исследовательских творческих проектов, что даст обучающимся возможность приобрести навык самостоятельного решения теоретической проблемы, навык генерирования и оформления собственных идей, навык уважительного отношения к чужим идеям, оформленным в работах других исследователей, навык публичного выступления перед аудиторией, аргументирования и отстаивания своей точки зрения.

Работа педагога со всем детским объединением включает в себя:

- инициирование и поддержку участия детского объединения в ключевых культурно-образовательных событиях образовательной организации, оказание необходимой помощи детям в их подготовке, проведении/ участии и анализе;

- организацию в творческом объединении интересных и полезных для личностного развития обучающихся совместных воспитательных событий, коллективных творческих дел, способствующих укреплению традиций, формирование и развитие коллектива, в том числе разновозрастного, а также способствующих самореализации детей и подростков и получение ими социального опыта, формирование поведенческих стереотипов, одобряемым в обществе;

- выработка с обучающимися детского объединения норм и правил совместной жизнедеятельности;

- создание условий для проявления инициатив по самоуправлению жизнедеятельностью детского объединения.

Индивидуальная работа педагога дополнительного образования с обучающимися детского объединения:

- изучение особенностей личностного развития обучающихся объединения через наблюдение за поведением, отношением к выбранному виду деятельности, взаимодействием и коммуникацией с другими обучающимися в специально создаваемых педагогических ситуациях, в организуемых педагогом беседах по тем или иным нравственно-этическим темам или событиям, участником которых стал ребенок;
- поддержка ребенка в решении важных для него жизненных проблем (налаживание взаимоотношений с другими детьми, личный и социальный опыт в конкретных видах и направлениях деятельности, в том числе в рамках программного содержания);
- коррекция поведения ребенка через индивидуальные беседы с ним, его родителями (законными представителями), с другими членами детского объединения; через привлечение узких специалистов для решения выявленных проблем.

Основные направления самоанализа воспитательной работы.

Основными направлениями анализа воспитательного процесса являются следующие показатели:

1. Результаты воспитания, социализации и саморазвития обучающихся (какова динамика личностного развития обучающихся каждого объединения; какие прежде существовавшие проблемы личностного развития школьников удалось решить; какие проблемы решить не удалось и почему; какие новые проблемы появились, над чем далее предстоит работать?).

2. Воспитательная деятельность педагога (испытывает ли педагог проблемы с реализацией воспитательного потенциала совместной с детьми деятельности);

Итогом анализа организуемого воспитательного процесса является перечень выявленных проблем, над которыми предстоит работать в дальнейшем.

№	Аспекты исследования	Диагностические средства
1.	Уровень воспитанности	• Методика определения общественной активности обучающихся МОУ ДО «РЦВР» (составленная Е.Н.Степановым) • Методика «Акт добровольцев» (сост. Л.В.Байбородовой)

2.	Личностное развитие обучающихся МОУ ДО «РЦВР»в участии массовых мероприятий МОУ ДО «РЦВР»	• наблюдение • опрос • анализ
3.	Изучение качества воспитанности обучающихся	• Методика оценки воспитанности обучающихся
4.	Самооценка воспитанников	• Методика самооценки «Дерево» (ав. Д. Лампен, в адапт. Л.П. Пономаренко)

План воспитательной работы 2022-2023 учебный год.

	Мероприятия	Срок
	1. Организация муниципальных конкурсов	
1.1	Ежегодный муниципальный конкурс	апрель
	2. Участие в международных, республиканских, областных и муниципальных конкурсах и акциях	
2.3	«Отечество»	в соответ. с планом
2.5	Всероссийская акция «Час кода»	декабрь
2.6	Участие в муниципальном конкурсе: «Я исследователь»	по плану
2.7	Участие в интернет - каникулах	ноябрь, январь, март
	3. Работа по формированию детского коллектива, органов детского самоуправления и выработке традиций учреждения	
3.1	Выборы Совета обучающихся, составление плана работы	октябрь
3.2	Конкурс между объединениями на лучший сайт или страничку в соц.сетях	ноябрь
3.4	Организация и проведение праздника по итогам года «Наши достижения»	май
3.5	Организация и проведение новогодних праздников.	декабрь
	4. Работа по пропаганде здорового образа жизни и безопасности и по профилактике правонарушений	
4.1	Акции, посвященные Международному дню отказа от курения и Дню борьбы с курением - Неделя здоровья,	2 раза в год

	- Всемирный день здоровья.	
4.2	Проведение мероприятий по профилактике нарушений и безопасности в сети интернет	сентябрь-май
4.4	Участие во всероссийском уроке безопасности школьников в сети интернет	по плану
5. Проведение тематических занятий		
5.1	Тематические часы «Поговорим о важном»	1 раз в квартал
5.2	Викторина «День народного единства»	ноябрь
5.3	К Международному дню инвалидов «Уроки добра»	1-2 декабря
5.4	Познавательная игра, посвященная Дню рождения города Волхова	декабрь
5.5	Рождественская викторина	декабрь-январь
5.6	«Был город фронт, была блокада» конкурс презентаций	январь
5.7	Компьютерный рисунок «День защитника отечества»	февраль
5.8	Международная неделя информатики	март
5.9	Викторина «День космонавтики»	апрель
5.10	День Победы	май
6. Диагностика учебно-воспитательного процесса		
6.1	Проведение промежуточной и итоговой аттестации обучающихся	декабрь, май
6.2	Диагностика успешности учащихся в районных, республиканских и другого уровня конкурсах.	в течение года
6.3	Диагностика участия учащихся в культурно-массовых мероприятиях.	в течение года

УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.

Материально техническое, кадровое и информационное обеспечение.

Методические обеспечение.

№ п\п	Разделы программы	Форма занятий	Приемы и методы организации и проведения занятия	Дидактический материал, техническое оснащение занятий	Формы подведения итогов
1.	Классификация рисков. Контентные риски. Коммуникаци-онные риски.	Комплексное. Объяснение нового материала, презентация, практическая работа	Метод проблемного изложения Эвристические методы	Мультимедийный проектор	Викторина. Тест «Есть у меня игровая зависимость»
2.	Электронные риски. Потребитель-ские риски. Лига безопасного интернета	Комплексное. Объяснение нового материала, презентация, практическая работа	Практическая проверка правильности выводов и обобщений	Мультимедийный проектор, компьютеры https://ege.yandex.ru/security/ - Тесты по безопасности	Практическая работа «Выявление признаков заражения вирусом» Викторина «Кибер-преступления»
3.	Квест «безопасность в интернете»	Выполнение заданий по станциям	Игровые	Мультимедийный проектор, компьютеры	Практическое выполнение заданий по всем темам

Литература.

Для педагога

1. Бирюков А.А. Информационная безопасность защита и нападение 2- е издание: Издательство: ДМК-Пресс., 2017, 434 с.
2. Колесниченко Денис. Анонимность и безопасность в интернете. От чайника к пользователю. Самоучитель Издательство: БХВ-Петербург, 2012, 240с.
3. Методическое пособие для работников системы общего образования Солдатова Г., Зотова Е., Лебешева М., Шляпников В. «Интернет: возможности, компетенции, безопасность», 2015 - 156с.

4. Мэйволд Э. Безопасность сетей (2-е изд.) Книги» Сетевые Технологии. Название: Безопасностьсетей: Издательство: М.: НОУ "Интуит", 2016,571 с.
5. Платонов В.В. Программно-аппаратные средства защитыинформации: учебник для студ. Учрежд.высш.проф. образования / В. В.Платонов. — М.: Издательский центр «Академия», 2013, 336 с.
6. Проскурин В.Г Защита в операционных системах: Издательство: Горячая линия-Телеком, 2014, 192 с.
7. Савченко Е. Кто, как и зачем следит за вами через интернет: Москва -Третий Рим, 2012, 100 с.
8. Яковлев В.А. Шпионские и антишпионские штучки: Техническая литература Издательство: Наука и Техника, 2015, 320 с.

Для обучающихся

1. «Березовый лес» или «лес березовый» /П. Лауфер//Юный эрудит. - 2014. - № 3. - С. 24-26
2. Доценко С.М., Шпак В.Ф. Комплексная информационная безопасность объекта. От теории к практике, Издательство: ООО «Издательство Полигон», 2000, 215 с.
3. Клепа и железный друг//Клепа. - 2014. - № 8. - С. 1-33.Электронная версия журнала: http://klepa.ru.
4. Мазаник Сергей. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей: издательство: ЭКСМО, 2014, 256 с.
5. Сорокина Е.В., Третьяк Т.М. Здоровье и безопасность детей в мире компьютерных технологий и Интернет. [Текст] Учебно-методический комплект. - М.: СОЛОНПРЕСС, 2010. - 176 с.: ил

Интернет ресурсы

Полезные ссылки для педагога:

1. Левский Н.А. Чего опасаться в Интернете. Самые опасные сайты. Вредоносные программы. [Электронный ресурс] // Журнал ComputerBild – 2013, - Режим доступа - http://www.windxp.com.ru/acpeg.htm , свободный.
2. Добреля Т.В. Чего опасаться в Интернете [Электронный ресурс] / Тимофей В. Добреля – 2013, Режим доступа - http://tim-plus.ru/opasnost-v-internete-i-kak-ee-izbezhat.html, свободный.

1. http://www.kaspersky .ru - антивирус «Лаборатория Касперского»;
2. http://www.onlandia.org.ua/rus/ - безопасная web-зона;
3. http:// www.interneshka.net - международный онлайн-конкурс по безопасному использованию Интернета;
4. Рыжков В.Н. Методика преподавания информатики// http://nto.immpu.sgu.ru/sites/default/files/3/ 12697.pdf;
5. http://www.saferinternet.ru - портал Российского Оргкомитета по безопасному использованию Интернета;
6. http://content-filtering.ru - Интернет СМИ «Ваш личный Интернет»;

7. http://www.rgdb.ru - Российская государственная детская библиотека
8. http://www.saferinternet.ru/ - Безопасный Интернет. Портал Российского Оргкомитета по проведению Года Безопасного Интернета. Мероприятия, Интернет и законодательство, проблемы и решения, международные ресурсы;
9. http://www.saferunet.ru/ - Центр Безопасного Интернета в России. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Интернете. Интернет-угрозы и эффективное противодействием им в отношении пользователей;
10. http://www.fid.su/ - Фонд развития Интернет. Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности и безопасности Интернета;
11. http://www.microsoft.com/Rus/athome/security/kids/etusivu. html - Безопасность в Интернете. "Основы безопасности детей и молодежи в 30 Интернете"

Полезные ссылки для детей и родителей:

1. http://www.interneshka.net/children/index.phtml - «Интернешка» - детский онлайн-конкурс по безопасному использованию сети Интернет. Советы детям, педагогам и родителям, «полезные ссылки». Регистрация и участие в конкурсе по безопасному использованию сети Интернет;
2. http://www.oszone.net/6213/-OS.zone.net-Компьютерный информационный портал. Статья для родителей «Обеспечение безопасности детей при работе в Интернет». Рекомендации по программе «Родительский контроль»;
3. http://www.rgdb .ru/innocuous-internet - Российская государственная детская библиотека. Ресурс для детей и родителей. Правила безопасного Интернета. Обзор программных продуктов для безопасного Интернета. Как защититься от Интернет-угроз. Ссылки на электронные ресурсы, информирующие об опасностях и защите в Сети;
4. https://www.google.ru/safetycenter/families/start/basics/ - Центр безопасности. Краткие рекомендации помогут обеспечить безопасность членов семьи
5. http://shperk.ru/v-seti/prokrustovo-lozhe. html - Прокрустово ложе для информационной картины. Как мы читаем тексты в интернете;
6. http://shperk.ru/sovety/avtoritet.html - Как отличить фейк от настоящего материала? Дело о летающем дьяке Крякутном;
7. http://habrahabr.ru/company/mailru/blog/252091/ - Советы по безопасности.
8. Международный квест по цифровой грамотности для школьников "Сетевичок" http://xn--b1afankxqj2c.xn--p1ai/

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ.

Тест по безопасности в сети Интернет

1. Как могут распространятся компьютерные вирусы?
   a. Посредством электронной почты.
   b. При просмотре веб-страниц.
   c. Через клавиатуру.
   d. Их распространяют только преступники.
2. Зачем нужен брандмауэр?
   a. Он не дает незнакомцам проникать в компьютер и просматривать файлы.
   b. Он защищает компьютер от вирусов.
   c. Он обеспечивает защиту секретных документов.
   d. Он защищает компьютер от пожара.
3. Всегда ли можно быть уверенным в том, что электронное письмо было получено от указанного отправителя?
   a. Да
   b. Да, если вы знаете отправителя
   c. Нет, поскольку данные отправителя можно легко подделать
   d. Может быть.
4. На компьютере отображается непонятное сообщение. Какое действие предпринять?
   a. Продолжить Будто ничего не произошло.
   b. Нажать кнопку «ОК» или «ДА»
   c. Обратится за советом к учителю, родителю или опекуну.
   d. Больше никогда не пользоваться Интернетом
5. Что нужно сделать при получении подозрительного сообщения электронной почтой?
   a. Удалить его, не открывая.
   b. Открыть его и выяснить, содержится ли в нем какая-нибудь важная информация.
   c. Открыть вложение, если такое имеется в сообщении.
   d. Отправить его родителям
6. В ящик входящей почты пришло «письмо счастья». В письме говорится, чтобы его переслали пяти друзьям. Какое действие предпринять?
   a. Переслать его пяти друзьям.
   b. Переслать его не пяти друзьям, а десяти друзьям.
   c. Не пересылать никакие «письма счастья»
   d. Ответить отправителю, что вы больше не хотите получать от него/нее письма.

7. В каких случаях можно, не опасаясь последствий, сообщать в Интернете свой номер телефона или домашний адрес?

   a. Во всех случаях.
   b. Когда кто-то просит об этом.
   c. когда собеседник в чате просит об этом.
   d.Такую информацию следует с осторожностью сообщать людям, которым вы доверяете.

8. Вы случайно прочитали пароль, который ваш друг записал на листочке бумаг. Как вы должны поступить?

a. Запомнить его.
b. Постараться забыть пароль.
c. Сообщить другу, что вы прочитали пароль, и посоветовать сменить пароль и никогда больше не записывать на листе бумаги.
d. Сообщить пароль родителям.

9. Что такое сетевой этикет?

a. Правила поведения за столом.
b. Правила дорожного движения.
c. Правила поведения в Интернете.
d. Закон, касающийся Интернета.

10. Что запрещено в интернете?

a. Запугивание других пользователей.
b. Поиск информации.
c. Игры.
d. Общение с друзьями

Тест «Осторожно, вирус!»

1. Что является основным каналом распространения компьютерных вирусов?
   a. Веб-страницы
   b. Электронная почта
   c. Флеш-накопители (флешки)
2. Для предотвращения заражения компьютера вирусами следует:
   a. Не пользоваться Интернетом
   b. Устанавливать и обновлять антивирусные средства
   c. Не чихать и не кашлять рядом с компьютером
3. Если вирус обнаружен, следует:
   a. Удалить его и предотвратить дальнейшее заражение
   b. Установить какую разновидность имеет вирус
   c. Выяснить, как он попал на компьютер
4. Что не дает хакерам проникать в компьютер и просматривать файлы и документы:
   a. Применение брандмауэра
   b. Обновления операционной системы
   c. Антивирусная программа
5. Какое незаконное действие преследуется в России согласно Уголовному Кодексу РФ?
   a. Уничтожение компьютерных вирусов
   b. Создание и распространение компьютерных вирусов и вредоносных программ
   c. Установка программного обеспечения для защиты компьютера Осторожно, Интернет!

1. Какую информацию нельзя разглашать в Интернете?
   a. Свои увлечения
   b. Свой псевдоним
   c. Домашний адрес

2. Чем опасны социальные сети?
   a. Личная информация может быть использована кем угодно в разных целях
   b. При просмотре неопознанных ссылок компьютер может быть взломан
   c. Все вышеперечисленное верно
3. Виртуальный собеседник предлагает встретиться, как следует поступить?
   a. Посоветоваться с родителями и ничего не предпринимать без их согласия
   b. Пойти на встречу одному
   c. Пригласить с собой друга

4. Что в Интернете запрещено законом?
   a. Размещать информацию о себе
   d. Размещать информацию других без их согласия
   c. Копировать файлы для личного использования

4. Действуют ли правила этикета в Интернете?
   a. Интернет - пространство свободное от правил
   b. В особых случаях
   c. Да, как и в реальной жизни

Тест:

Закончите предложение: Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно…

Административному кодексу

Трудовому кодексу

Уголовному кодексу

Гражданскому кодексу

Какой классификации вирусов на сегодняшний день не существует?

По поражаемым объектам

По поражаемым операционным системам и платформам

По количеству поражаемых файлов

По дополнительной вредоносной функциональности

Какой из приведенных паролей является более надежным

Для того, чтобы антивирусные программы обеспечивали наилучшую безопасность вашего ПК, необходимо:

Установить несколько антивирусных программ

Удалить все файлы, загруженные из сети Интернет

Своевременно обновлять антивирусные базы

Отключить компьютер от сети Интернет

Какой из браузеров считается менее безопасным, чем остальные:

Mozilla Firefox

Internet Explorer

Google Chrome

Какие действия не рекомендуется делать при работе с электронной почтой?

Отправлять электронные письма

Добавлять в свои электронные письма фотографии

Открывать вложения неизвестной электронной почты

Оставлять электронные письма в папке Отправленные

Что необходимо сделать, если на экране появилось окно с просьбой отправить SMS для дальнейшей работы?

Отправить SMS сообщение

Выполнить форматирование жесткого диска

Перезагрузить компьютер

Не отправлять SMS сообщение

Согласно какому документу в России проводится правой ликбез по вопросам защиты информации в ЭВМ?

Трудовому кодексу РФ

Доктрине информационной безопасности РФ

Стратегии развития информационного общества РФ

Конвенции о правах ребенка

Зачем необходимо делать резервные копии?

Чтобы информация могла быть доступна всем желающим

Чтобы не потерять важную информацию

Чтобы можно было выполнить операцию восстановления системы

Чтобы была возможность распечатать документы

Что необходимо сделать, если на сайте в Интернет, вдруг появилось сообщение о быстрой проверке ПК с просьбой перезагрузки компьютера?

Перезагрузить компьютер

Отформатировать жесткий диск

Закрыть сайт и выполнить проверку ПК

Выключить компьютер.