Муниципальное казенное общеобразовательное учреждение
«Средняя общеобразовательная школа пгт Хасан
Хасанского района» Приморского края

«Рассмотрено»
Протокол заседания
методического объединения
№ 1 от 31.08.2022 г.
_____/Карпова Н.В. /

«Утверждено»
Приказ руководителя
образовательного учреждения
№ 71-А от 31.08.2022 г.
_____/Карпов В.А./

Рабочая программа
факультатива
Информационной безопасность. Кибербезопасность.
11 класс

Ф.И.О. педагога-составителя программы: Резинкова И.В.

Педагогический стаж: 17 лет

Квалификационная категория: первая

пгт Хасан
2022 г.

Пояснительная записка

Особенности курса по информационной безопасности

Безопасность в сети Интернет в свете быстрого развития социальных 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, появление сетевых средств вмешательства в личное информационное пространство на персональных устройствах, работающих в Интернете, массовое использование детьми электронных социальных/банковских карт, имеющих персональные настройки доступа к ним, резко повышает потребность в воспитании у учащихся культуры информационной безопасности в целях предотвращения негативных последствий массового использования Интернета детьми и их защиты от негативной информации.

При реализации требований безопасности в сети Интернет для любого пользователя, будь это школьник или учитель, образовательное учреждение должно обеспечивать защиту конфиденциальных сведений, представляющих собой, в том числе, персональные данные школьника. 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. Для этого необходимо проводить непрерывную образовательно-просветительскую работу с детьми, начиная с младшего школьного возраста, формировать у родителей и учащихся ответственное и критическое отношение к источникам негативной информации, 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 является важной задачей для вовлечения детей в современную цифровую образовательную среду, отвлечения их от бесполезного, отвлекающего контента, бесцельной траты времени в социальных сетях и мессенджерах.

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

Задачи курса по информационной безопасности детей:

– формировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей, как человеческая жизнь, свобода, равноправие и достоинство людей, здоровье, опыт 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 по следствий 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, осознавать 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.

Структура и содержание курса

Особенностью курса является поэтапное развитие учебного материала для разных возрастных групп учащихся.

Курс для школьников 10-11 классов отражает особенности современного цифрового мира как киберпространства, насыщенного сетевыми сервисами и интернет-коммуникациями, доступными детям, в том числе негативной направленности:

- ✓ 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 детьми электронных социальных/банковских карт, имеющих персональные настройки доступа к ним.

Все это резко повышает потребность в воспитании у учащихся культуры информационной безопасности с одной стороны и профориентации в мире профессий будущего — с другой, а также популяризации полезных интернет-ресурсов.

«Информационные войны» в глобальном цифровом пространстве породили новые угрозы для общества — кража персональных данных, призывы к агрессии и террору, склонение к насилию, суициду. С учетом последних тенденций, названных «фейковые новости», в киберпространстве появились: навязчивый ложный контент деструктивного, очерняющего людей и события содержания, пропаганда наркотических средств под видом ложной информации о продукции, в том числе распространяемый автоматически, ложные новости и постановочные репортажи. Навыки обдуманного поведения при поиске информации в сети Интернет, критического анализа полученной информации, умения работать с информацией избирательно и ответственно, знакомство с профессиями в сфере информационной безопасности — это важная часть современной цифровой грамотности школьников 10-11 классов, которая востребована в жизни и учебе при работе в сети Интернет, социальных сетях и мессенджерах.

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. При этом в сети Интернет есть много позитивного контента, СМИ, позволяющих получать информацию о профессиях будущего, использованию цифровых технологий в быту на основе «умных» технологий, направлениях развития современного киберискусства, использования Интернета для электронного обучения и др.

Все это потребовало расширить тему информационной безопасности в сети Интернет для школьников 10-11 классов такими понятиями, как:

– киберагент;
– кибермир,
– киберискусство,
– киберобщество,
– киберугрозы,
– кибератака,
– киберпреступность,
– киберкультура…

Важную часть практического содержания курса составляет выполнение заданий по информационной безопасности с использованием сети Интернет, ознакомление с позитивным контентом познавательного, учебного и развивающего назначения, выполнение практической работы, предложенной в открытых практикумах ИТ-компаний и операторов мобильной телефонии для разных возрастных групп учащихся (практикумы встроены к содержание модулей курса).

Планируемые предметные результаты освоения курса

В соответствии с ФГОС общего образования необходимо сформировать у учащихся такие **личностные результаты,** которые позволят подростку ориентироваться в информационном мире с учетом имеющихся в нем угроз:

- ✓ Принимать ценности человеческой жизни, семьи, гражданского общества, многонационального российского народа, человечества.
- ✓ Быть социально активным, уважающим закон и правопорядок, соизмеряющим свои поступки с нравственными ценностями, осознающим свои обязанности перед семьей,
- ✓ обществом, Отечеством.
- ✓ Уважать других людей, уметь вести конструктивный диалог, достигать взаимопонимания, сотрудничать для достижения общих результатов.

Осознанно выполнять правила здорового и экологически целесообразного образа жизни, безопасного для человека и окружающей его среды.

В результате обучения по модулям курса акцентируется внимание на такие **метапредметные результаты** освоения основной образовательной программы основного общего образования, как:

– 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 информационных и коммуникационных технологий (далее — ИКТ) в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности.

Также планируется достижение некоторых предметных результатов, актуальных для данного курса в интеграции с предметами: «Обществознание» и «Информатика» (раздел «Социальная информатика») для 10–11 классов, например:

– формирование основ правосознания для соотнесения собственного поведения и поступков других людей с нравственными ценностями и нормами поведения, установленными законодательством Российской Федерации;

– освоение приемов работы с социально значимой информацией, ее осмысление; развитие способностей обучающихся делать необходимые выводы и давать обоснованные оценки

социальным событиям и процессам;

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

Планируется достижение некоторых **предметных результатов,** актуальных для данного курса в предметах.

В результате освоения курса учащиеся будут **знать и понимать:**

- источники угроз, поступающих на мобильный телефон, планшет, компьютер
- виды угроз
- проблемные ситуации в сетевом взаимодействии
- правила поведения для защиты от угроз
- правила поведения в проблемных ситуациях
- этикет сетевого взаимодействия
- роль близких людей, семьи для устранения проблем и угроз в сети Интернет и мобильной телефонной связи
- телефоны экстренных служб
- личные данные
- позитивный Интернет;

уметь:

- правильно использовать аватар с учетом защиты личных данных
- формировать и использовать пароль
- использовать код защиты телефона
- регистрироваться на сайтах без распространения личных данных
- вести общение в социальной сети или в мессенджере сообщений
- правильно вести себя в проблемной ситуации (оскорбления, угрозы, предложения, агрессия, вымогательство, ложная информация и др.)
- отключиться от нежелательных контактов
- использовать позитивный Интернет.

Виды учебной деятельности обучающихся на уроках

Уроки информационной безопасности несут практическую направленность.

Познавательная часть урока основана на постановке учителем проблемы в качестве темы урока, ее рекомендуется проводить в форме беседы-дискуссии, опираясь на видео-материалы и факты по теме. Рекомендуется на каждом уроке в рамках изучаемой темы:

– рассказать школьникам о возможных негативных последствиях, которые могут наступить при работе в сети Интернет;

– мотивировать школьников использовать ресурсы сети Интернет для определенных целей;

– выстроить беседы в максимально доверительном тоне.

Доверие между ребенком и взрослым — залог успеха в таком важном деле;

– использовать компьютерный класс, где установлена аппаратная защита — постоянно обновляемый антивирус, программа защиты (контент-фильтр) для сортировки и отсеивания информации негативного характера;

– активно вовлекать детей в обсуждение проблемы по теме.

Практическая часть урока основана на выполнении заданий по работе с информацией по теме, в том числе практических работ от ведущих ИТ-компаний, специально разработанных для детей и представленных в открытом до ступе. Все уроки по темам курса снабжены тестами для промежуточного контроля, которые удобно проводить в форме мини-викторин.

Для достижения планируемых результатов предусмотрены учебно-методические

комплекты по информационной безопасности для 10–11 классов, снабженных открытыми электронными материалами на сайте издательства БИНОМ.

В состав интернет-ресурсов для проведения занятий по информационной безопасности включены открытые курсы и электронные материалы, видеоролики от ведущих ИТ-компаний и операторов мобильных сетей.

Тематическое планирование учебного курса для 10-11 классов

Курс «Кибербезопасность» разработан для учащихся 10-11 классов и предлагается к изучению как курс по выбору образовательной организации в рамках рамках предметов «Информатика» или ОБЖ. Курс рассчитан на 33 часа как одногодичный курс в 10 или в 11 классах.

К курсу разработано учебное пособие «Кибербезопасность».

К учебному пособию на сайте издательства размещено бесплатное электронное приложение. Оно включает ресурсы для выполнения практических заданий к урокам из пособия, а также открытые электронные документы и ресурсы http://lbz.ru/metodist/authors/ib/7-9.php

Все электронные ресурсы выложены на основе наличия открытого доступа к ним.

К каждому модулю предлагается практическая работа на компьютерах. По итогам изучения модуля учащимся предлагается тест.

К каждому параграфу предусмотрен набор заданий по теме для обсуждения и выполнения на уроке, в том числе с использованием электронного приложения.

Организация учебной деятельности на уроке включает теоретическую, понятийную часть, с использованием видео материалов и документов в электронном приложении, дискуссию по вопросам к параграфу, выполнение практической части в задании к параграфу на компьютере.

В курсе используется ряд новых терминов, которые сформировались недавно. Кибернетика (от др.греч. Κυβερνητικη#υυυυ) — это «искусство управления». Теперь можно говорить не только о безопасности в интернете, но и о возможности управления информационным пространством в преступных или негативных целях. Достижения науки и техники, создание всемирной сети Интернет позволили преступности выйти на новый уровень и захватить киберпространство. Теперь преступнику не нужен прямой контакт с жертвой и всего несколько человек могут стать угрозой для каждого пользователя «глобальной паутины», крупных корпораций и целых государств.

Кибертерроризм и использование виртуального пространства для совершения актов насилия, а также другие деяния, посягающие на общественную безопасность, включаются в пятую группу киберпреступлений.

Количество киберпреступлений, совершаемых в мире, неуклонно растет. Меняется и их качественный состав, и размер причиненного ущерба. Такое торжество преступности в виртуальном пространстве не может обойтись безнаказанно. Законодательство большинство стран мира предполагает уголовную ответственность за совершение преступлений данного вида.

Пособие включает четыре раздела.

Введение.

Раздел 1. Киберпространство. (11 часов)

Киберпространство. Кибермиры. Киберфизическая система. Киберобщество. Киберденьги. Кибермошенничество.

Практикум к разделу 1. Практическая работа на основе онлайн-курса Академии Яндекс «Безопасность в Интернете» по теме «Безопасные онлайн-платежи».

Тест к разделу 1.

Раздел 2. Киберкультура. (11 часов)

Киберкультура. От книги к гипертексту. Киберкнига. Кибер искусство. Социальная инженерия. Классификация угроз социальной инженерии.

Практикум к разделу 2. Практическая работа от компаний мобильной связи Билайн,

МТС и Мегафон (по выбору учащихся).
Тест к разделу 2.
Раздел 3. Киберугрозы (11 часов)
Кибервойны. Киберпреступность. Примеры киберпреступлений. Уязвимости кибербезопасности. Угрозы информационной безопасности. Запрещенные и нежелательные сайты. Новые профессии в кибероблестве.
Практикум к разделу 3 Практическая работа на основе онлайнкурса Академии Яндекса «Безопасность в Интернете» (продолжение), по темам:

- ✓ Защита от вредоносных программ.
- ✓ Безопасность аккаунтов. Логины и пароли от электронной почты, социальных сетей и других сервисов.

Тест к разделу 3.
Раздел 4. Проверь себя
Содержит тесты к трем тематическим разделам.

Методическое обеспечение программы
Материально-техническое и учебно-методическое обеспечение образовательного процесса

1. Роскомнадзор, официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, URL: http://rkn.gov.ru/
2.Цветкова М. С., Хлобыстова И. Ю. Информационная безопасность. Кибербезопасность. 7–9 классы : учебное пособие. — М.: БИНОМ. Лаборатория знаний, 2020. — 64 с.
3. Сайт электронного приложения к пособиям по информационной безопасности, URL: http://lbz.ru/metodist/authors/ib/
4. «Безопасный Билайн», компания Билайн, URL: http://moskva.beeline.ru/customers/help/safebeeline/
5. «Безопасность», компания МТС, URL: http://www.safety.mts.ru/ru/
6. «Безопасное общение», компания Мегафон, URL: http://moscow.megafon.ru/bezopasnoe_obschenie/
7. «Памятка по безопасному общению», компания Мегафон, URL: http://moscow.megafon.ru/download/~msk/~moscow/stopfraud/brochure.pdf
8. Открытый онлайнкурс «Безопасность в Интернете», «Ака демия Яндекс», компания Яндекс, URL: https://academy.yandex.ru/events/online-urses/internet_security/
9. Солдатова Г.У., Чигарькова С.В.Тренажер по курсу «Кибербезопасность» для общеобразовательных организаций. - М.: ООО «Руоское слово — учебник», 2020. - 80 с. - (ФГОС. Внеурочная деятельность)

Тематическое планирование факультатива по информатике
«Информационная безопасность. Кибербезопасность» 11 класс
1 ч в неделю (34 ч)

№ урока	Дата проведения	Тема урока	
		Раздел 1. Киберпространство — 11 ч	
1		Киберпространство	
2		Кибермиры	
3		Киберфизическая система	
4		Кибероблщество	
5		Кибероблщество. Викторина «Азбука Кибербезопасности. Медиаграмотность»	
6		Киберденьги	
7		Электронные платежи: правила безопасности	Из книги «Тренажер по Кибербезопасности» 8 класс, стр. 39
8		Кибермошенничество	
9		Практическая работа «Безопасные онлайн-платежи».	
10		Практическая работа «Безопасные онлайн-платежи».	
11		Тест к разделу 1.	
		Раздел 2. Киберкультура — 11 ч	
12		Киберкультура	
13		От книги к гипертексту	
14		Киберкнига	
15		Киберкнига	
16		Киберискусство	
17		Социальная инженерия	
18		Классификация угроз социальной инженерии	
19		Профессии будущего	
20		Практическая работа Практическая работа от компаний мобильной связи Билайн, МТС и Мегафон (по выбору учащихся)	
21		Практическая работа Практическая работа от компаний мобильной связи Билайн, МТС и Мегафон (по выбору учащихся)	
22		Тест к разделу 2	
		Раздел 3. Киберугрозы — 11 ч	

23		Кибервойна	
24		Киберпреступность	
25		Примеры киберпреступлений	
26		Уязвимости кибербезопасности	
27		Угрозы информационной безопасности	
28		Запрещенные и нежелательный сайты	
29		Новые профессии в киберобществе	
30		Практическая работа «Защита от вредоносных программ»	
31		Практическая работа на основе онлайн-курса Академии Яндекса «Безопасность в Интернете» по темам: Безопасность аккаунтов. «Логины и пароли от электронной почты, социальных сетей и других сервисов»	
32		Практическая работа на основе онлайн-курса Академии Яндекса «Безопасность в Интернете» по темам: Безопасность аккаунтов. «Логины и пароли от электронной почты, социальных сетей и других сервисов»	
33		Тест к разделу 3.	
34		Итоговый урок	