



ИЗДАТЕЛЬСТВО «РУССКОЕ СЛОВО»

КИБЕРБЕЗОПАСНОСТЬ

ФГОС



РУССКОЕ-СЛОВО.РФ



КИБЕРБЕЗОПАСНОСТЬ. 5–9 КЛАССЫ

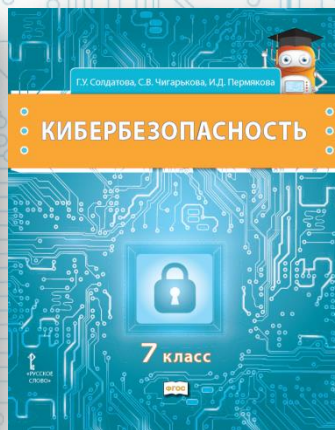
Приказ Минпросвещения России № 858 от 21 сентября 2022 года



ФП 2.1.2.2.2.2.1



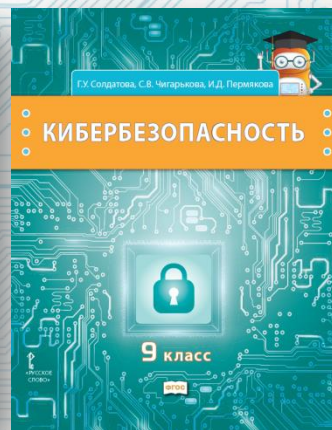
ФП 2.1.2.2.2.2.2



ФП 2.1.2.2.2.2.3



ФП 2.1.2.2.2.2.4



ФП 2.1.2.2.2.2.5

Цели курса

- Формирование цифровой компетентности школьников
- Расширение возможностей полезного, критичного, ответственного и безопасного использования Интернета

АВТОРСКИЙ КОЛЛЕКТИВ

СОЛДАТОВА

Галина Уртанбековна

Доктор психологических наук, академик РАО, профессор кафедры психологии личности факультета психологии МГУ им. М.В. Ломоносова, директор Фонда Развития Интернет, лауреат Премии Правительства РФ в области образования

ЧИГАРЬКОВА

Светлана Вячеславна

Кандидат психологических наук, научный сотрудник кафедры психологии личности факультета психологии МГУ им. М.В. Ломоносова, заместитель директора Фонда Развития Интернет

ПЕРМЯКОВА

Ирина Дмитриевна

Практикующий психолог, финалист конкурса «Педагог года Москвы» в номинации «Педагог-психолог»

СОСТАВ УМК



01

Учебники в печатной форме

02

ЭФУ

03

Методические пособия

04

Рабочие программы

05

Программа курса

СКВОЗНЫЕ ПЕРСОНАЖИ КУРСА

Персональный помощник

Кибернешка / профессор Кибер Нетович



Имя пользователя: Кибернешка

Статус: Готов прийти на помощь!

Местоположение: Интернет

Увлечения: кибербезопасность, обучение школьников



Сообщения

Добавить в друзья



Имя пользователя: магистр Кибер Нетов

Статус: Всегда приду на помощь!

Местоположение: Интернет

Увлечения: кибербезопасность, обучение школьников

Любимая книга: «Галактика Интернет»



Сообщения

Добавить в друзья

Школьники

Гоша Геймеров, Рита Картинкина, Игорь Неюзеров



Имя пользователя: Игорь Неюзеров

Статус: Пошёл гулять!

Местоположение: скрыто

Увлечения: лонгборд, бас-гитара, общение, робототехника, настольные игры, фотография, музыка, футбол, собаки

Любимый фильм: их слишком много

Любимая книга: Джек Лондон «Любовь к жизни»

Сообщения

Добавить в друзья



Имя пользователя: Маргарита Картинкина

Статус: Хочу болтать!)

Местоположение: Москва

Увлечения: селфи, фотки, общение, музыка, кино, фотошоп, коты

Любимый фильм: «Гарри Поттер и философский камень»

Любимая книга: Л. Кэрролл «Алиса в Зазеркалье»

Сообщения

Добавить в друзья



Имя пользователя: Гоша Геймеров

Статус: Играю

Местоположение: Москва

Увлечения: Need for Speed, World of Tanks, Fifa 17, Minecraft

Любимый фильм: давно не смотрел

Любимая книга: нет

Сообщения

Добавить в друзья

Текст учебников оформлен как «посты» персонального помощника в социальной сети.

Характеры этих персонажей соответствуют разным типам пользователей.



Кибернешка



#Любопытный_факт

На английском языке символ @ обычно именуют commercial at. Носители других языков почему-то ассоциируют этот символ с разными животными. Например, на итальянском @ называют chiosciola — «улитка». На шведском — snabel-a, то есть «а» с хоботом». На русском — «собака». В других языках встречаются «спящий кот», «мышинный хвост», «утёнок» и «червячок».



Кибернешка



#Мини-тренировка

Найдите 7 различий между двумя корзинами онлайн-покупок Риты Картиной.



Кибернешка



Я буду публиковать здесь посты с разной полезной и интересной информацией. У моих постов есть постоянные рубрики. Вот они:

#Словарик — важные слова и их значения.

#Из истории Интернета — справки об истории Интернета.

#Любопытный_факт — интересная информация, связанная с использованием Интернета, и не только.

#Советы Кибернешки — советы о безопасном поведении в Интернете.

Ещё одна рубрика называется **#Мини-тренировка**, это небольшие разминки для памяти и внимания.



Магистр Кибер Нетов



#Советы Кибера Нетова

1. Совершайте покупки только в крупных интернет-магазинах, надёжных сервисах, которыми пользуются ваши близкие.
2. Прежде чем купить что-то в Интернете, советуйтесь со взрослыми.
3. Внимательно читайте условия покупки и пользовательское соглашение — чтобы убедиться, что в нём нет трудных для вас обязательств.
4. Уточняйте по телефону условия заказа и доставки.
5. Знакомьтесь с отзывами о сайте или товаре, но помните, что они могут быть написаны на заказ.
6. Помните, что магазин ни при каких условиях не будет запрашивать ПИН-код от банковской карты.

МОДУЛИ



Цифровой мир
и интернет-зависимость



Техносфера
и технические риски



Информация
и контентные риски



Общение
и коммуникационные риски



Цифровая экономика
и потребительские риски



Персональные данные



Цифровое будущее



ПРЕДСТАВЛЕНЫ В КАЖДОМ КЛАССЕ

МОДУЛЬ 1.

ЦИФРОВОЙ МИР И ИНТЕРНЕТ-ЗАВИСИМОСТЬ

Формируются способность и готовность:

- ответственно выбирать безопасные пути освоения цифровых технологий;
- понимать и адекватно оценивать риски, возникающие в процессе освоения Интернета;
- находить оптимальные способы решения проблем, возникающих в процессе освоения Интернета и цифровых технологий;
- оценивать количество личного времени, проводимого за использованием Интернета, и качество содержательного наполнения этого времени;
- находить оптимальные пути решения проблемы чрезмерного использования Интернета и цифровых устройств.



Тема 1 ДРУГАЯ РЕАЛЬНОСТЬ — ДОПОЛНЕННАЯ И ВИРТУАЛЬНАЯ



Магистр Кибер Нетов

#Словарик



Виртуальная реальность (от *англ.* virtual reality, VR) — искусственная реальность, образ которой складывается из ощущений, передаваемых человеку через органы чувств (зрения, слуха, осязания и др.) при помощи цифровых технологий.

Термин «виртуальная реальность» ввёл изобретатель Джарон Ланье (Jaron Lanier) в конце 1980-х гг., но попытки создавать при помощи техники образы искусственной реальности предпринимались и раньше.



Дополненная реальность (от *англ.* augmented reality, AR) — «смешанная» реальность, которая возникает путём добавления к истинной реальности виртуальных образов, смоделированных при помощи цифровых технологий.

Считается, что этот термин предложил исследователь авиакосмической корпорации «Боинг» Том Коделл (Tom Caudell) в 1990 г.

Дополненная и особенно виртуальная реальности создают эффект погружения: можно сражаться с нарисованным персонажем и при этом испытывать реальные ощущения, например чувство полёта или спуска с горы. Как будто то, что мы наблюдаем, происходит на самом деле.



Задание 1

1. Найдите в Интернете и запишите в тетради год появления и название первой технологии виртуальной реальности.
2. Найдите в Интернете статьи по истории дополненной и виртуальной реальностей, прочитайте их. Выпишите 3–5 фактов, которые вас заинтересовали.



Магистр Кибер Нетов



#Словарик

Вредоносные программы — программное обеспечение, предназначенное для получения неразрешённого доступа к информации, причинения вреда устройству, его программному обеспечению или его владельцу.



Задание 1

Дайте определение понятию «компьютерный вирус».



Задание 2

Напишите в тетради ответы на вопросы:

1. Что такое троянская программа?
2. Чем троянская программа отличается от компьютерного вируса или червя?



Задание 3

Определите, насколько верны следующие утверждения. Приведите аргументы в пользу вашего решения.

Утверждение 1. На большинстве персональных компьютеров нет никаких важных данных, используя которые злоумышленник может заработать деньги или нанести пользователю какой-либо ущерб.

Утверждение 2. Если в компьютер попадает вредоносная программа, то компьютер ломается.

Утверждение 3. Если просто просматривать веб-странички и ничего не скачивать, невозможно поймать вредоносную программу.

Утверждение 4. Невозможно поймать вредоносную программу на сайтах крупных и уважаемых компаний (например, «Яндекса», «Википедии» и др.).

Утверждение 5. Если установить антивирус и регулярно его обновлять, ни один вирус компьютеру не страшен.



Задание 4

Сформулируйте выводы и правила безопасного поведения в Интернете на основании ответов к заданию 3.

МОДУЛЬ 2.

ТЕХНОСФЕРА И ТЕХНИЧЕСКИЕ РИСКИ

Формируются способность и готовность:

- ответственно и безопасно использовать различные способы подключения к Интернету и возможности их настройки в соответствии с текущими задачами;
- ответственно и безопасно использовать современное программное обеспечение для работы в Интернете;
- уметь защищать личные данные в Интернете от несанкционированного доступа;
- ответственно и безопасно использовать программные средства для защиты технических устройств от вирусов;
- оценивать основные риски, связанные с различными способами подключения к Сети.

МОДУЛЬ 3.

ИНФОРМАЦИЯ И КОНТЕНТНЫЕ РИСКИ

Формируются способность и готовность:

- ответственно и безопасно использовать различные поисковые системы для поиска в Интернете информации;
- оценивать качество информации / информационных ресурсов в Интернете;
- ответственно и безопасно использовать различные интернет-ресурсы для создания и размещения в Интернете оригинальной позитивной информации;
- ответственно потреблять и распространять информацию в соответствии с этическими нормами, текущим законодательством РФ;
- оценивать основные риски использования информации в Интернете.



Тема 4
ФЕЙКИ В ИНТЕРНЕТЕ:
КАК ИХ РАСПОЗНАТЬ



Магистр Кибер Нетов



#Любопытный_факт

Распространение фейковых новостей привело к созданию проектов, посвящённых проверке новостей — фактчекингу (от *англ.* fact checking — проверка фактов). Растёт число сайтов, на которых занимаются разоблачением фейков. В качестве примера можно привести российский сайт с говорящим названием «Лапшеснималочная».

Разрабатываются руководства, подробно описывающие технологию проверки разного рода информации. Так, на русский язык переведено с английского «Руководство по верификации для журналистских расследований» (верификация — от *англ.* verification — проверка): https://verificationhandbook.com/book2_ru/about.php.



Задание 1

Напишите эссе на одну из тем:

- «Фейковые новости — явление XXI в.»;
- «Мой опыт столкновения с фейковыми новостями»;
- «Как я отношусь к фейковым новостям».



Задание 2

Это задание для работы в парах. Придумайте одну фейковую новость и найдите одну реальную новость, похожую на фейковую. Поменяйтесь с вашим партнёром по паре новостями, не рассказывая, какая новость реальная, а какая фейковая. Задача каждого — предположить, какая из новостей реальная.

После того как вы оба оцените новости, ответьте на вопросы:

1. Сложно ли догадаться, какая новость реальная, а какая нет?
2. Какими критериями вы пользовались, чтобы отличить фейк от правды?



Задание 3

Назовите признаки, по которым можно предположить, что новость фейковая.



Задание 4

Найдите и опишите способы определения фейковых видео или фотографий.



#Любопытный_факт

В Интернете, как и в реальной жизни, общение бывает разным. В 2021 г. российская компания Brand Analytics решила выяснить, каких высказываний в социальных сетях больше — позитивных или негативных. Было проанализировано 894 млн постов и комментариев, оставленных российскими пользователями в популярных социальных сетях. Учитывались слова и высказывания, которые передают положительные или отрицательные эмоции, испытываемые по отношению к другим людям (например, «я люблю», «обожаю», «я без ума», «я счастлив» и «я ненавижу», «меня раздражает», «бесит», «твит ненависти» и т.п.). В итоговый анализ вошло 813,5 тысяч сообщений, сделанных пользователями от своего имени. Подавляющее большинство проанализированных сообщений (82,4%) выражали положительные эмоции и только 17,6% — отрицательные.

Получается, что в Интернете доброты и любви гораздо больше, чем злости и агрессии. И тем не менее негатив тоже встречается. По результатам исследования Фонда Развития Интернет, 86% подростков сталкивались с агрессией в Интернете.



Задание 1

Опровергните письменно следующие утверждения.

1. В Интернете можно оставаться анонимным и безнаказанно писать что угодно.
2. Даже если я знаю, что про моего знакомого распускают в Интернете слухи и пишут неприятные вещи, я не должен вмешиваться, так как это меня не касается.
3. Агрессия в Интернете не может навредить здоровью и самочувствию человека, на которого она направлена.



Задание 2

Познакомьтесь с ситуациями и ответьте на вопросы к ним.

МОДУЛЬ 4.

ОБЩЕНИЕ И КОММУНИКАЦИОННЫЕ РИСКИ

Формируются способность и готовность:

- ответственно и безопасно взаимодействовать с другими пользователями на различных Интернет-ресурсах в соответствии с общечеловеческими нормами поведения, текущим законодательством РФ, правилами конкретного интернет-ресурса;
- ответственно и безопасно выбирать стратегии коммуникации на различных интернет-ресурсах;
- ответственно и безопасно управлять собственной репутацией и социальным капиталом в Интернете;
- адекватно оценивать риски, возникающие в процессе коммуникации в Интернете;
- ответственно и безопасно выбирать стратегии поведения при столкновении с проявлениями агрессии (с троллингом, кибербуллингом и т. д.) в Интернете.

ЦИФРОВАЯ ЭКОНОМИКА И ПОТРЕБИТЕЛЬСКИЕ РИСКИ

Формируются способность и готовность:

- использовать различные интернет-ресурсы для поиска информации о товарах и услугах;
- оценивать качество продуктов, предоставляемых на различных интернет-ресурсах, а также потенциальные риски, связанные с их потреблением;
- оценивать достоверность информации, представленной на различных рекламных носителях в Интернете;
- ответственно и безопасно использовать интернет-ресурсы, соблюдая пользовательские соглашения и общие правила безопасности;
- оценивать основные потребительские риски, связанные с приобретением и потреблением товаров и услуг.



Магистр Кибер Нетов

#Словарик

Цифровая экономика — экономическая деятельность, основанная на цифровых технологиях и взаимодействии между виртуальным и реальным миром; система производства и потребления цифровых товаров и услуг (программного обеспечения, онлайн-образования, контента).



Задание 1

Пробовали ли вы покупать что-то в Интернете? Если да — что именно и каким способом?



Магистр Кибер Нетов

#Любопытный_факт

По данным опроса Фонда Развития Интернет, проведённого в 2018 г. в России более половины подростков используют Интернет для поиска информации о товарах или для их покупки. При этом каждый девятый подросток сообщает, что потерял деньги из-за обмана в Сети, а каждый десятый считает, что потратил слишком много денег в онлайн-играх или в приложениях для покупок. Интересно, что в 2013 г. цифры были совсем другими: тогда, к примеру, только каждый двенадцатый подросток использовал Интернет для покупки товаров или услуг. Это говорит о том, что школьники с каждым годом становятся всё более активными участниками цифровой экономики.



Задание 2

Проведите небольшое исследование на тему покупок в Интернете. Для этого задайте нескольким взрослым вопросы:

- Как часто они делают покупки в Интернете?
 - Какие категории товаров покупают?
 - В чём, по их мнению, преимущества покупок в Интернете?
 - Какие правила безопасности они соблюдают при покупках в Интернете?
- На основании опроса ответьте на вопросы:
- В каких случаях лучше совершать покупки в Интернете?



Тема 9 ЧТО НУЖНО ЗНАТЬ О ЦИФРОВЫХ СЛЕДАХ



Кибернешка

#Словарик

Цифровой след, цифровой отпечаток — совокупность персональных данных о пользователе, а также обо всех его действиях в Интернете, которые хранятся в Сети.



Задание 1

Как вы думаете, в чём заключается разница между отпечатком ноги на песке у моря и цифровыми следами?



Кибернешка



#Словарик

Приватность — сфера частной жизни и право на её неприкосновенность и защиту.

Настройки приватности — специальный раздел на цифровых устройствах, ресурсах, приложениях или сайтах, где пользователь может сам определить, какой информацией он делится с другими пользователями или ресурсами.



Задание 2

Пользуетесь ли вы настройками приватности? Если да, то какими?



Задание 3

Придумайте и запишите какой-нибудь секрет. Если бы этот секрет не был выдуманным, с кем вы могли им поделиться?



Кибернешка



#Советы Кибернешки

Почему приватность так важна? Всё, что вы делаете в Интернете — выставляете фотографии, видео, аудио, пишете свои посты, — всё это оставляет

МОДУЛЬ 6.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Формируются способность и готовность:

- различать виды персональных данных и понимать последствия небрежного обращения с ними;
- уметь пользоваться различными средствами управления персональными данными в Интернете;
- ответственно и безопасно использовать методы защиты конфиденциальных персональных данных;
- ответственно и безопасно использовать специальные безопасные режимы работы в браузерах;
- ответственно и безопасно использовать приёмы, позволяющие контролировать распространение персональных данных в Интернете;
- ответственно и безопасно использовать настройки приватности в социальных сетях и на других онлайн-ресурсах;
- оценивать риски, связанные с предоставлением и распространением персональных данных.

ЦИФРОВОЕ БУДУЩЕЕ

Формируются способность и готовность:

- разбираться в изменениях, которые происходят в технологической и социальной сферах;
- понимать, адекватно и ответственно использовать возможности, которые появляются благодаря новым технологиям;
- понимать и адекватно оценивать риски, возникающие вследствие изменений в технологической и социальной сферах;
- находить личные жизненные ориентиры, соответствующие нравственным и этическим нормам;
- реализовывать личностный потенциал в условиях цифрового общества.

**Задание 1**

Познакомьтесь с информацией об интересных современных технологиях, которые применяют в школах разных стран.

**Кибернешка****#Любопытный_факт**

Для нас ещё привычна ручка, которой мы пишем на бумаге. Но недавно появилась ручка, с помощью которой можно создавать объёмные предметы! Она заправлена не чернилами, а специальным пластиком. Такой же пластик используется в 3D-принтерах. 3D-ручка открывает своему владельцу огромный простор для творчества, возможность создавать объёмные картины и трёхмерные объекты.

**Кибернешка****#Любопытный_факт**

Школьная форма тоже меняется — она становится «умной». Одна японская компания выпустила школьную форму для учащихся начальной школы со встроенной системой спутниковой навигации GPS. Эта одежда даёт родителям возможность отслеживать, где в данный момент находится их ребёнок. Кроме того, система, зашитая в форму, заботится о безопасности её владельца. Почувствовав угрозу, ребёнок может просто нажать кнопку на пиджаке — и в службу безопасности будет послан сигнал тревоги.

«Умная» школьная форма была введена и в Бразилии. Оснащённая специальными датчиками одежда бразильских школьников информирует их родителей о том, находится их ребёнок в школе или прогуливает уроки. А вот в США попытки повысить безопасность школьников посредством электронных систем потерпели неудачу. Родители усмотрели в новом проекте излишнее вмешательство в личную жизнь их детей.

АКТИВНЫЕ МЕТОДЫ ОБУЧЕНИЯ

- Работа в группах
- Участие в играх
- Обсуждение кейсов
- Выполнение проектов
- Подготовка выставок

- 1. ответить на вопрос
- 2. найти информацию в Интернете
- 3. выполнить задание, применив свои знания и навыки; провести самостоятельное исследование или эксперимент; собрать информацию по заданной теме; дать определение понятию; сформулировать правило; пройти тест
- 4. придумать что-то новое и необычное; написать текст-размышление на заданную тему; осуществить проект
- 5. прочитать кейс (случай) и ответить на вопросы (выполнить задания) к нему
- 6. выполнить задание в игровой форме
- 7. сформулировать, что для вас оказалось самым важным в изучаемой теме

- Решение творческих задач
- Участие в конференциях
- Анализ несплошных текстов
- Выполнение практико-ориентированных заданий



Задание 1

Опишите, что вы видите на этих фотографиях.



Задание 2

На какой фотографии в задании 1 изображена персональная (личная) информация, а на какой — общедоступная?



Задание 6

Кейс. Вы сидите в кафе со своей бабушкой и обсуждаете совместную поездку. Вы обнаружили сеть Wi-Fi и подключились к ней. Бабушка попросила посмотреть наличие билетов на поезд в другой город на сайте железных дорог и купить их, если есть свободные места. Вы знаете, что для покупки билетов нужно ввести данные паспортов.

Вопрос. Какую из этих просьб вы выполните, пока находитесь в кафе? Объясните почему.



Реализация курса – **за счёт вариативной части учебного плана**, содержание которой формируется участниками образовательных отношений.

Частота проведения занятий – **1 час в неделю**
(34 часа в год).

Продолжительность обучения – **5 лет.**



Курс «Кибербезопасность» могут вести **учителя, классные руководители, педагоги-психологи, социальные педагоги, педагоги дополнительного образования.**



ИЗДАТЕЛЬСТВО «РУССКОЕ СЛОВО»

ИЗДАТЕЛЬСТВО «РУССКОЕ СЛОВО»

115035, Москва, Овчинниковская наб., д. 20, стр. 2
Тел./факс: (495) 969-24-54 (многоканальный)
E-mail: rs@russlo.ru

ИНФОРМАЦИОННО-МЕТОДИЧЕСКИЙ ОТДЕЛ

115035, Москва, Овчинниковская наб., д. 20, стр. 2
Тел./факс: (499) 689-01-65 (многоканальный)
E-mail: metod@russlo.ru

ОТДЕЛ БЮДЖЕТНЫХ ПРОДАЖ

115035, Москва, Овчинниковская наб., д. 20, стр. 2
Тел./факс: (499) 689-01-65 (многоканальный)
E-mail: info@russlo.ru

ОТДЕЛ РЕАЛИЗАЦИИ

115035, Москва, Овчинниковская наб., д. 20, стр. 2
Тел./факс: (499) 689-02-65 (многоканальный)
E-mail: sale@russlo.ru



РУССКОЕ-СЛОВО.РФ