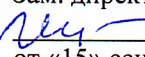


Министерство образования и молодежной политики Свердловской области  
Государственное казенное общеобразовательное учреждение  
Свердловской области «Екатеринбургская вечерняя школа № 2»

620085 г. Екатеринбург, ул. Монтерская, 5  
Тел: (343) 2-564-024 доб. 241  
Электронная почта: [gouvsoshik10@yandex.ru](mailto:gouvsoshik10@yandex.ru)  
Сайт: [евш2.рф](http://евш2.рф)

РАССМОТРЕНО  
на заседании ШМО  
Протокол № 2  
от «08» сентября 2023 г.

Согласовано  
Зам. директора по УВР  
 Езимова И.И.  
от «15» сентября 2023 г.



Рабочая программа  
по элективному курсу  
«Информационная безопасность»  
7-8 класс

Составитель: Меркурьев А.А.,  
учитель,  
высшая квалификационная категория

Екатеринбург  
2023 г.

Настоящая рабочая программа является составной частью Образовательной программы среднего общего образования ГКОУ СО «Екатеринбургская ВШ № 2». Рабочая программа составлена на основании следующих нормативно-правовых документов и материалов:

1. Федерального закона от 29.12. 2012 № 273-ФЗ «Об образовании в Российской Федерации».
2. Федерального государственного образовательного стандарта среднего общего образования с изменениями и дополнениями Приказа Минобрнауки РФ от 17.05.12 № 413 «Об утверждении федерального государственного образовательного стандарта среднего общего образования» (Зарегистрирован в Минюсте РФ 7 июня 2012 г. № 24480).
4. Приказа Минобрнауки РФ от 29.12.2014 № 1645 «О внесении изменений в приказ Министерства образования и науки Российской Федерации от 17 мая 2012 г. № 413 «Об утверждении федерального государственного образовательного стандарта среднего общего образования» (Зарегистрировано в Минюсте России 09.02.2015 № 35953).
5. Приказа Минобрнауки РФ от 31.12.2015 № 1577 «О внесении изменений в федеральный государственный образовательный стандарт среднего общего образования, утвержденный приказом Министерства образования и науки Российской Федерации от 17 мая 2012 г. № 413. (Зарегистрировано в Минюсте России 09.02.2016 № 41020).
6. Федерального перечня учебников, рекомендованных Министерством образования РФ к использованию в образовательном процессе в общеобразовательных учреждениях на текущий учебный год.
7. Учебного плана школы на текущий учебный год.

Главная **цель элективного курса** - вооружить обучаемых знаниями информационного самообеспечения познавательной, изучения правовой грамотности в сфере информационной безопасности

Результатом изучения этого курса будет являться овладение рациональными приемами самостоятельного ведения поиска информации;

освоение формализованными методами аналитико-синтетической переработки информации; овладение традиционной и компьютерной технологией подготовки и оформления результатов своей самостоятельной познавательной деятельности.

Принцип преемственности предполагает постепенное, от класса к классу, усложнение материала при сохранении целостности курса, призванного не только вооружить обучающихся совокупностью знаний и умений по работе с информацией, но и сформировать системное представление об информационной картине мира, информационное мировоззрение.

Для этого элективный курс «Информационная безопасность» предусматривает разнообразие форм, методов, средств обучения, выбор таких их сочетаний, которые стимулируют активность и самостоятельность обучаемых. Формирование устойчивой мотивации, необходимости повышения информационной культуры личности невозможно также без увлеченного преподавания, показа практического применения знаний в связи с жизненными планами и ориентациями учащихся, использования новых и нетрадиционных форм обучения, чередования форм и методов обучения, проблемного и эвристического обучения.

Особое место в элективном курсе «Информационная безопасность» занимает обучение с компьютерной поддержкой, применение мультимедиа систем, использование интерактивных компьютерных средств. Формируя мотивацию, преподаватель, параллельно с выполнением главной своей задачи - изложением основ информационной культуры и формированием знаний и умений на требуемом учебной программой уровне помогает обучающимся осознать, что овладение ими информационной культурой делает их более уверенными в себе.

### **Требования к уровню подготовки обучающихся**

Содержание программы элективного курса соответствует темам основной образовательной программы основного общего образования (ООП ООО) по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», а также расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических устройств (персональных компьютеров, планшетов, и пр.), позволяет правильно

вести обучающегося в цифровое пространство и корректировать его поведение в виртуальном мире.

Рабочая программа по элективному курсу «Информационная безопасность» составлена для обучающихся 7-8 классов, с учетом того, что школа имеет очно-заочную форму обучения и находится на территории закрытого учреждения, где отбывают наказания по приговору суда за тяжкие преступления граждане в возрасте от 18 лет, которые имеют значительный перерыв обучения в образовательных учреждениях. Программа разработана на основе учебника Наместниковой М.С. «Информационная безопасность, или на расстоянии одного вируса» для 7-9 классов, Просвещение 2019 год и направлена на достижение следующих планируемых результатов Федерального государственного образовательного стандарта основного общего образования:

личностных;

метапредметных (регулятивных, познавательных, коммуникативных);

предметных.

Курс является важной составляющей частью работы с обучающимися, которые задумываются о своей личной безопасности, безопасности своей семьи и своих друзей, а также проявляющими интерес к изучению истории и технологических основ информационной безопасности. Направление программы элективного курса – общеинтеллектуальное.

Программа курса ориентирована на выполнение требований Федерального государственного образовательного стандарта основного общего образования. Ее реализация даёт возможность раскрытия индивидуальных способностей обучающихся, развития интереса к различным видам индивидуальной и групповой деятельности, закрепления умения самостоятельно организовать свою учебную деятельность.

#### **Цель курса:**

- формирование активной позиции обучающихся в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им;
- обеспечение условий для профилактики негативных тенденций в информационной культуре учащихся, повышения защищенности от информационных рисков и угроз.

#### **Задачи курса:**

- дать представление о современном информационном обществе, информационной безопасности личности и государства;
- сформировать навыки ответственного и безопасного поведения современной информационно-телекоммуникационной среде;
- сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом;
- сформировать общекультурные навыки работы с информацией (умений грамотно пользоваться источниками информации, правильно организовать информационный процесс);
- дать представление о видах и способах распространения вредоносных кодов, способов защиты личных устройств;
- познакомить со способами защиты от противоправных посягательств в сети Интернет, защиты личных данных.

#### **МЕСТО элективного курса «Информационная безопасность» В УЧЕБНОМ ПЛАНЕ**

Учитывая специфику образовательного учреждения ГКОУ СО «Екатеринбургская вечерняя школа № 2» как режимного объекта, а также Основную образовательную программу вечерней школы, формы получения образования (очно-заочное обучение), возрастные и социально-психологические особенности обучающихся, на методическом объединении учителей ГКОУ СО «Екатеринбургская ВШ № 2» была проведена и согласована корректировка

настоящей рабочей программы с целью внесения в неё соответствующих изменений. Таким образом, обязательность изучения предмета «Информационная безопасность» сохраняется в 7-8 классах в соответствии с указанными выше программными документами, приказами и рекомендациями Министерства образования и науки Российской Федерации. В текущем учебном году в учебном плане школы на предмет «Информационная безопасность» запланировано 68 часов в год, в том числе: 7 - 8 классы – по 1 часу в неделю (34 учебных недели);

ИТОГО – 68 часов в год.

## **ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ЭЛЕКТИВНОГО КУРСА 7-8 КЛАСС**

### **Личностные:**

- осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно - осуществлять выбор виртуальных собеседников;
- готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;
- освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;
- сформированность ценности безопасного образа жизни;
- интериоризация правил индивидуального и коллективного безопасного поведения в информационно- телекоммуникационной среде.

### **Метапредметные результаты**

#### **Межпредметные понятия**

В ходе изучения элективного курса, обучающиеся усваивают опыт учебной деятельности и навыки работы с информацией, в том числе в текстовом, табличном виде, в виде диаграмм.

#### **Регулятивные универсальные учебные действия**

В результате освоения элективного курса обучающийся сможет:

- идентифицировать собственные проблемы и определять главную проблему;
- выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;
- ставить цель деятельности на основе определенной проблемы и существующих возможностей;
- формулировать учебные задачи как шаги достижения поставленной цели деятельности;
- обосновывать целевые ориентиры и приоритеты ссылками на ценности, указывая и обосновывая логическую последовательность шагов;
- определять необходимые действие(я) в соответствии с учебной и познавательной задачей и составлять алгоритм их выполнения;
- обосновывать и осуществлять выбор наиболее эффективных способов решения учебных и познавательных задач;
- определять/находить, в том числе из предложенных вариантов, условия для выполнения учебной и познавательной задачи;
- выстраивать жизненные планы на краткосрочное будущее (заявлять целевые ориентиры, ставить адекватные им задачи и предлагать действия, указывая и обосновывая логическую последовательность шагов);
- выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;

- составлять план решения проблемы;
- определять потенциальные затруднения при решении учебной и познавательной задачи и находить средства для их устранения;
- описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;
- определять совместно с педагогом и сверстниками критерии планируемых результатов и критерии оценки своей учебной деятельности;
- систематизировать (в том числе выбирать приоритетные) критерии планируемых результатов и оценки своей деятельности;
- отбирать инструменты для оценивания своей деятельности, осуществлять самоконтроль своей деятельности в рамках предложенных условий и требований;
- оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;
- находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;
- работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;
- устанавливать связь между полученными характеристиками продукта и характеристиками процесса деятельности и по завершении деятельности предлагать изменение характеристик процесса для получения улучшенных характеристик продукта;
- сверять свои действия с целью и, при необходимости, исправлять ошибки самостоятельно;
- определять критерии правильности (корректности) выполнения учебной задачи;
- анализировать и обосновывать применение соответствующего инструментария для выполнения учебной задачи;
- свободно пользоваться выработанными критериями оценки и самооценки, исходя из цели и имеющихся средств, различая результат и способы действий;
- оценивать продукт своей деятельности по заданным и/или самостоятельно определенным критериям в соответствии с целью деятельности;
- обосновывать достижимость цели выбранным способом на основе оценки своих внутренних ресурсов и доступных внешних ресурсов;
- фиксировать и анализировать динамику собственных образовательных результатов.
- наблюдать и анализировать собственную учебную и познавательную деятельность и деятельность других обучающихся в процессе взаимопроверки;
- соотносить реальные и планируемые результаты индивидуальной образовательной деятельности и делать выводы; принимать решение в учебной ситуации и нести за него ответственность.

### **Познавательные универсальные учебные действия**

В результате освоения элективного курса обучающийся сможет:

- выделять общий признак двух или нескольких предметов, или явлений, объяснять их сходство;
- объединять предметы и явления в группы по определенным признакам, сравнивать, классифицировать и обобщать факты и явления;
- выделять явление из общего ряда других явлений;
- определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений;
- строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;

- строить рассуждение на основе сравнения предметов и явлений, выделяя при этом общие признаки;
- излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
- самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;
- вербализовать эмоциональное впечатление, оказанное на него источником информации;
- объяснять явления, процессы, связи и отношения, выявляемые в ходе познавательной и исследовательской деятельности;
- объяснять, детализируя или обобщая;
- объяснять с заданной точки зрения;
- делать вывод на основе критического анализа разных точек зрения, подтверждать вывод собственной аргументацией или самостоятельно полученными данными;
- переводить сложную по составу (многоаспектную) информацию из графического или формализованного (символьного) представления в текстовое, и наоборот;
- анализировать/рефлексировать опыт разработки и реализации учебного проекта, исследования (теоретического, эмпирического) на основе предложенной проблемной ситуации, поставленной цели и/или заданных критериев оценки продукта/результата;
- критически оценивать содержание и форму текста;
- определять необходимые ключевые поисковые слова и запросы;
- формировать множественную выборку из поисковых источников для объективизации результатов поиска;
- соотносить полученные результаты поиска со своей деятельностью.

#### **Коммуникативные универсальные учебные действия**

В результате освоения элективного курса обучающийся сможет:

- определять возможные роли в совместной деятельности;
- играть определенную роль в совместной деятельности;
- принимать позицию собеседника, понимая позицию другого, различать в его речи: мнение (точку зрения), доказательство (аргументы), факты; гипотезы, аксиомы, теории;
- определять свои действия и действия партнера, которые способствовали или препятствовали продуктивной коммуникации;
- строить позитивные отношения в процессе учебной и познавательной деятельности;
- корректно и аргументированно отстаивать свою точку зрения, в дискуссии уметь выдвигать контраргументы, перефразировать свою мысль (владение механизмом эквивалентных замен);
- критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;
- предлагать альтернативное решение в конфликтной ситуации;
- выделять общую точку зрения в дискуссии;
- договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
- организовывать учебное взаимодействие в группе (определять общие цели, распределять роли, договариваться друг с другом и т. д.);
- устранять в рамках диалога разрывы в коммуникации, обусловленные непониманием/неприятием со стороны собеседника задачи, формы или содержания диалога;
- определять задачу коммуникации и в соответствии с ней отбирать речевые средства;
- отбирать и использовать речевые средства в процессе коммуникации с другими людьми (диалог в паре, в малой группе и т. д.);
- представлять в устной или письменной форме развернутый план собственной деятельности;

- соблюдать нормы публичной речи, регламент в монологе и дискуссии в соответствии с коммуникативной задачей;
- высказывать и обосновывать мнение (суждение) и запрашивать мнение партнера в рамках диалога;
- принимать решение в ходе диалога и согласовывать его с собеседником;
- создавать письменные «клишированные» и оригинальные тексты с использованием необходимых речевых средств;
- использовать вербальные средства (средства логической связи) для выделения смысловых блоков своего выступления;
- использовать невербальные средства или наглядные материалы, подготовленные/отобранные под руководством учителя;
- делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его;
- целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
- выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;
- использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;
- использовать информацию с учетом этических и правовых норм;
- соблюдать информационную гигиену и правила информационной безопасности.

#### **Предметные результаты:**

- умение анализировать доменные имена компьютеров и адреса документов в интернете;
- овладение безопасными приемами пользования средствами коммуникации;
- научатся безопасно вести и применять способы самозащиты при попытке мошенничества;
- безопасно использовать ресурсы интернета;
- овладеют приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных;
- сформируют основы самоконтроля, соблюдения норм информационной этики и права;
- получат навыки самостоятельного принятия решения и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности.

#### **Содержание элективного курса**

Отбор тематики содержания курса осуществлен с учетом целей и задач ФГОС основного общего образования, возрастных особенностей и познавательных возможностей, обучающихся 7-8 классов.

В преподавании элективного курса «Информационная безопасность» будут использоваться разнообразные форматы обучения: традиционный урок (коллективная и групповая формы работы), тренинги, наглядное обучение (электронные курсы, видеоролики) смешанный формат.

Содержание программы элективного курса соответствует темам основной образовательной программы основного общего образования (ООП ООО) по учебным предметам «Информатика» и «Основы безопасности жизнедеятельности», а также расширяет их за счет привлечения жизненного опыта обучающихся в использовании всевозможных технических

устройств (персональных компьютеров, планшетов, и пр.), позволяет правильно ввести обучающегося в цифровое пространство и корректировать его поведение в виртуальном мире.

### **БЕЗОПАСНОСТЬ ОБЩЕНИЯ 7 КЛАСС**

Тема 1. Общение в социальных сетях и мессенджерах

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Тема 2. С кем безопасно общаться в интернете

Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Тема 3. Пароли для аккаунтов социальных сетей

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях

Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты

Настройки приватности публичных страниц. Правила ведения публичных страниц.

Тема 9. Фишинг

Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

### **БЕЗОПАСНОСТЬ УСТРОЙСТВ 8 КЛАСС**

Тема 1. Что такое вредоносный код

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода

Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Тема 3. Методы защиты от вредоносных программ

Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов. Правила безопасности в виртуальных контактах.

Тема 4. Распространение вредоносного кода для мобильных устройств

Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Тема 5. Резервное копирование данных

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Социальная инженерия: распознать и избежать



Приемы социальной инженерии. Правила безопасности в виртуальных контактах.

Тема 7. Ложная информация в Интернете

Фейковые новости. Поддельные страницы.

Тема 8. Безопасность при использовании платежных карт в Интернете

Транзакции и связанные с ними риски. Правила совершения онлайн покупок.

Безопасность банковских сервисов

Тема 9. Беспроводная технология связи

Уязвимости Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

### ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ 7 КЛАСС

№ п/п	Содержание	Общее количество часов	Теория	Практика	Виды деятельности
1	Тема 1. Общение в социальных сетях и мессенджерах	5	2	3	Выполняет базовые операции при использовании мессенджеров и социальных сетей. Изучает историю и социальную значимость личных аккаунтов в сети Интернет
	Тема 2. С кем безопасно общаться в интернете	5	3	2	Руководствуется в общении социальными ценностями и установками коллектива и общества в целом
3	Тема 3. Пароли для аккаунтов социальных сетей	4	2	2	Изучает основные понятия регистрационной информации и шифрования
4	Тема 4. Безопасный вход в аккаунты	4	3	1	Объясняет причины использования безопасного входа при работе на чужом устройстве
5	Тема 5. Настройки конфиденциальности в социальных сетях	3	2	1	Раскрывает причины установки закрытого профиля. Меняет основные настройки приватности в личном профиле
6	Тема 6. Публикация информации в социальных сетях	3	2	1	Осуществляет поиск использует информацию, необходимую для выполнения поставленных задач
7	Тема 7. Кибербуллинг	4	4		Реагирует на опасные ситуации, распознает провокации и попытки манипуляции со стороны виртуальных собеседников
8	Тема 8. Публичные аккаунты	2	1	1	Решает экспериментальные задачи. Самостоятельно изучает источники информации
9	Тема 9. Фишинг	6	4	2	Разработка и распространение чеклиста (памятки) по противодействию фишингу

**Поурочное планирование «7» класс 34 часа (1 час в неделю)**

№ п/п		Тема урока	Кол-во часов			Сроки проведения	Электронные (цифровые) образовательные ресурсы
			всего	теория	практика		
		<b>Общение в социальных сетях и мессенджерах</b>	5	2,5	1,5		
1	1	Социальная сеть	1	1		1 неделя	презентация
2	2	История социальных сетей	1	0,5	0,5	2 неделя	<a href="http://school-collektion.edu/ru">http://school-collektion.edu/ru</a>
3	3	Мессенджеры	1	0,5	0,5	3 неделя	
4	4	Назначение социальных сетей и мессенджеров	1	0,5	0,5	4 неделя	<a href="http://school-collektion.edu/ru">http://school-collektion.edu/ru</a>
5	5	Пользовательский контент	1		1	5 неделя	
		<b>С кем безопасно общаться в интернете</b>	3	2,5	0,5		
6	1	Правила добавления друзей в социальных сетях	1	0,5	0,5	6 неделя	<a href="http://school-collektion.edu/ru">http://school-collektion.edu/ru</a>
7	2	Профиль пользователя	1	1		7 неделя	
8	3	Анонимные социальные сети	1	1		8 неделя	<a href="http://school-collektion.edu/ru">http://school-collektion.edu/ru</a>
		<b>Пароли для аккаунтов социальных сетей</b>	4	2	2		
9	1	Сложные пароли	1	1		9 неделя	<a href="http://windows.edu/ru">http://windows.edu/ru</a>
10	2	Онлайн генераторы паролей	1		1	10 неделя	<a href="http://windows.edu/ru">http://windows.edu/ru</a>
11	3	Правила хранения паролей	1		1	11 неделя	
12	4	Использование функции браузера по запоминанию паролей	1	1		12 неделя	<a href="https://kids.kaspersky.ru/">https://kids.kaspersky.ru/</a>
		<b>Безопасный вход в аккаунты</b>	4	3	1		
13	1	Виды аутентификации	1	1		13 неделя	

14	2	Настройки безопасности аккаунта	1		1	14 неделя	презентация
15-16	3-4	Работа на чужом компьютере с точки зрения безопасности личного аккаунта	2	1	1	15-16 недели	<a href="https://kids.kaspersky.ru/">https://kids.kaspersky.ru/</a>
<b>Настройки конфиденциальности в социальных сетях</b>			3	2	1		
17-18	1-2	Настройки приватности и конфиденциальности в разных социальных сетях	2	2		17-18 недели	презентация
19	3	Приватность и конфиденциальность в мессенджерах	1		1	19 неделя	<a href="https://kids.kaspersky.ru/">https://kids.kaspersky.ru/</a>
<b>Публикация информации в социальных сетях</b>			3	2	1		
20-21	1-2	Персональные данные	2	2		20-21 недели	<a href="http://windows.edu/ru">http://windows.edu/ru</a>
22	3	Публикация личной информации	1		1	22 неделя	презентация
<b>Кибербуллинг</b>			4	4			
23	1	Определение кибербуллинга	1	1		23 неделя	презентация
24	2	Возможные причины кибербуллинга и как его избежать?	1	1		24 неделя	<a href="https://kids.kaspersky.ru/">https://kids.kaspersky.ru/</a>
25	3	Как не стать жертвой кибербуллинга	1	1		25 неделя	<a href="https://kids.kaspersky.ru/">https://kids.kaspersky.ru/</a>
26	4	Как помочь жертве кибербуллинга	1	1		26 неделя	<a href="http://windows.edu/ru">http://windows.edu/ru</a>
<b>Публичные аккаунты</b>			2	1	1		
27	1	Настройки приватности публичных страниц	1	1		27 неделя	презентация
28	2	Правила ведения публичных страниц	1		1	28 неделя	
<b>Фишинг</b>			<b>6</b>	<b>4</b>	<b>2</b>		

29-30	1-2	Фишинг как мошеннический прием	2	2		29-30 недели	<a href="https://kids.kaspersky.ru/">https://kids.kaspersky.ru/</a>
31	3	Популярные варианты распространения фишинга	1		1	31 неделя	<a href="http://school-collektion.edu/ru">http://school-collektion.edu/ru</a>
32-33	4-5	Отличие настоящих и фишинговых сайтов	2	2		32-33 недели	<a href="http://school-collektion.edu/ru">http://school-collektion.edu/ru</a>
34	6	Как защититься от фишеров в социальных сетях	1		1	34 неделя	презентация

### ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ 8 класс

№	Содержание	Общее количество часов	Теория	Практика	Виды деятельности
<b>БЕЗОПАСНОСТЬ ИНФОРМАЦИИ</b>					
1	Тема 1. Что такое вредоносный код	4	4	2	Соблюдает технику безопасности при эксплуатации компьютерных систем. Используют инструментальные средства и сервисы адекватно задаче
2	Тема 2. Распространение вредоносного кода	6	3,5	2,5	Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности
3	Тема 3. Методы защиты от вредоносных программ	4	2,5	1,5	Изучает виды антивирусных программ и правила их установки
4	Тема 4. Распространение вредоносного кода для мобильных устройств	4	2	2	Разрабатывает презентацию, инструкцию по обнаружению, алгоритм установки приложений на мобильные устройства для учащихся более младшего возраста Приводят примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска)

5	Тема 5. Резервное копирование данных	2	1,5	0.5	Самостоятельная работа. Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позицию другого, различает в его речи: мнение (точку зрения), доказательство (аргументы), факты
6	Тема 6. Социальная инженерия: распознать и избежать	2	1,5	0,5	Находит нужную информацию в базах данных, составляя запросы на поиск. Систематизирует получаемую информацию в процессе поиска
7	Тема 7. Ложная информация в Интернете	4	2	2	Определяет возможные источники необходимых сведений, осуществляет поиск информации
8	Тема 8. Безопасность при использовании платежных карт в Интернете	4	2	2	Приводит примеры рисков, связанных с совершением онлайн покупок (умеет определить источник риска). Разрабатывает возможные варианты решения ситуаций, связанных с рисками использования платежных карт в Интернете
9	Тема 9. Беспроводная технология связи	4	3	1	Используя различную информацию, определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов
Всего часов: 34					

**Поурочное планирование  
«8» класс 34 часа (1 час в неделю)**

№ п/п		Тема урока	Кол-во часов			Сроки проведения	Электронные (цифровые) образовательные ресурсы
			всего	теория	практика		
<b>Что такое вредоносный код</b>			4	2	2		
1-2	1-2	Виды вредоносных кодов	2	1	1	1-2 неделя	презентация
3-4	3-4	Возможности и деструктивные функции вредоносных кодов	2	1	1	3-4 неделя	<a href="https://kids.kaspersky.ru/">https://kids.kaspersky.ru/</a>
<b>Распространение вредоносного кода</b>			6	3,5	2,5		
5	1	Способы доставки вредоносных кодов	1	0,5	0,5	5 неделя	презентация
6-7	2-3	Исполняемые файлы и расширения вредоносных кодов	2	1	1	6-7 неделя	<a href="https://kids.kaspersky.ru/">https://kids.kaspersky.ru/</a>
8	4	Вредоносная рассылка	1	0,5	0,5	8 неделя	презентация
9	5	Способы выявления наличия вредоносных кодов на устройствах	1	1		9 неделя	<a href="http://windows.edu/ru">http://windows.edu/ru</a>
10	6	Действия при обнаружении вредоносных кодов на устройствах	1	0,5	0,5	10 неделя	<a href="http://windows.edu/ru">http://windows.edu/ru</a>
<b>Методы защиты от вредоносных программ</b>			4	2,5	1,5		
11	1	Способы защиты устройств от вредоносного кода	1	1		11 неделя	<a href="https://kids.kaspersky.ru/">https://kids.kaspersky.ru/</a>
12	2	Антивирусные программы и их характеристики	1	0,5	0,5	12 неделя	презентация
13	3	Правила защиты от вредоносных кодов	1	0,5	0,5	13 неделя	презентация
14	4	Правила безопасности в виртуальных контактах	1	0,5	0,5	14 неделя	презентация
<b>Распространение вредоносного кода для мобильных устройств</b>			4	2	2		презентация

15	1	Расширение вредоносных кодов для мобильных устройств	1	0,5	0,5	15 неделя	<a href="https://kids.kaspersky.ru/">https://kids.kaspersky.ru/</a>
16	2	Правила безопасности при установке приложений на мобильные устройства	1	0,5	0,5	16 неделя	<a href="http://windows.edu/ru">http://windows.edu/ru</a>
17	3	Правила совершения онлайн покупок	1	0,5	0,5	17 неделя	презентация
18	4	Безопасность банковских сервисов	1	0,5	0,5	18 неделя	презентация
<b>Резервное копирование данных</b>			2	1,5	0,5		
19	1	Безопасность личной информации	1	1		19 неделя	<a href="https://kids.kaspersky.ru/">https://kids.kaspersky.ru/</a>
20	2	Создание резервных копий на различных устройствах	1	0,5	0,5	20 неделя	презентация
<b>Социальная инженерия: распознать и избежать</b>			2	1,5	0,5		
21	1	Приемы социальной инженерии	1	1		21 неделя	<a href="http://windows.edu/ru">http://windows.edu/ru</a>
22	2	Правила безопасности в виртуальных контактах	1	0,5	0,5	22 неделя	презентация
<b>Ложная информация в Интернете</b>			4	2	2		
23-24	1-2	Фейковые новости	2	1	1	23-24 неделя	презентация
25-26	3-4	Поддельные страницы	2	1	1	25-26 неделя	<a href="https://kids.kaspersky.ru/">https://kids.kaspersky.ru/</a>
<b>Безопасность при использовании платежных карт в Интернете</b>			4	2	2		
27-28	1-2	Транзакции и связанные с ними риски	2	1	1	27-28 неделя	презентация
29	3	Правила совершения онлайн покупок	1	0,5	0,5	29 неделя	презентация
30	4	Безопасность банковских сервисов	1	0,5	0,5	30 неделя	<a href="https://kids.kaspersky.ru/">https://kids.kaspersky.ru/</a>
<b>Беспроводная технология связи</b>			4	3	1		
31-32	1-2	Уязвимости Wi-Fi-соединений	2	1	1	31-32 неделя	<a href="https://kids.kaspersky.ru/">https://kids.kaspersky.ru/</a>



33	3	Публичные и непубличные сети	1	1		33 неделя	<a href="http://windows.edu/ru">http://windows.edu/ru</a>
34	4	Правила работы в публичных сетях	1	1		34 неделя	презентация
Всего часов: 34							

## УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

### ОБЯЗАТЕЛЬНЫЕ УЧЕБНЫЕ МАТЕРИАЛЫ ДЛЯ УЧЕНИКА

Наместникова М.С. «Информационная безопасность, или на расстоянии одного вируса» для 7-9 классов, / учебник; Просвещение 2019 г  
Цветкова М.С. Информационная безопасность. Правовые основы информационной безопасности 7-9 классы; /учебник – М.: Просвещение, 2021

### МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ УЧИТЕЛЯ

Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019 – 432 с  
Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014 – 182 с.  
Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017 – 384 с.  
Дети в информационном обществе <http://detionline.com/journal/about>  
Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИ-ДАНА, 2016 – 239 с.  
Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018 – 558 с.

### ЦИФРОВЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ И РЕСУРСЫ СЕТИ ИНТЕРНЕТ

<http://windows.edu/ru>

<http://school-collektion.edu/ru>

<http://fcior.edu.ru>, <http://eor.edu.ru>

<http://detionline.com/journal/about> <https://kids.kaspersky.ru/>

// <https://www.xn--d1abkefqip0a2f.xnp1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kurs>