МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ЮУрГГПУ»)

ФАКУЛЬТЕТ МАТЕМАТИКИ, ФИЗИКИ, ИНФОРМАТИКИ

КАФЕДРА ИНФОРМАТИКИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ИНФОРМАТИКЕ

Формирование основ информационной безопасности на уроках информатики

Выпускная квалификационная работа

по направлению 44.03.05 Педагогическое образование (с двумя профилями подготовки)

Направленность программы бакалавриата

«Информатика. Математика»

Форма обучения заочная

Проверка на объем заимствований:
63,82 % авторского текста

Работа допущена к защите
рекомендована/не рекомендована

«26» февраля 2024 г.
зав. кафедрой ИИТиМОИ

_____ Рузаков А.А.

Выполнил:
Студент группы ЗФ-613-111-5-1
Уголько Валерия Александровна

Научный руководитель:
к.п.н., доцент кафедры ИИТиМОИ

_____ Паршукова Н.Б.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ФАКУЛЬТЕТ МАТЕМАТИКИ, ФИЗИКИ, ИНФОРМАТИКИ

КАФЕДРА ИНФОРМАТИКИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ИНФОРМАТИКЕ

Формирование основ информационной безопасности на уроках информатики
Выпускная квалификационная работа
по направлению 44.03.05 Педагогическое образование (с двумя профилями подготовки)
Направленность программы бакалавриата
«Информатика. Математика»
Форма обучения заочная

Проверка на объем заимствований:
_____% авторского текста

Работа _____ к защите
рекомендована/не рекомендована

« ___ » _____ 20__ г.
зав. кафедрой И, ИТ и МОИ

_____ Рузаков А.А.

Выполнил:
Студент группы ЗФ-613-111-5-1
Уголько Валерия Александровна

Научный руководитель:
к.п.н., доцент кафедры И, ИТ и МОИ

_____Паршукова Н.Б.

Челябинск

2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность исследования основана на том, что в современном мире информационная безопасность становится все более важной и значимой темой. Образование, как и многие другие сферы, подверглось активному внедрению и использованию информационных и коммуникационных технологий. Обучающиеся, благодаря информатизации образования, имеют возможность: получать информацию из большого количества источников, исследовать и изучать различные точки зрения, принимать участие в интерактивном и групповом обучении с помощью онлайн-платформ.

Развитие информационных технологий и широкое использование интернета дают много возможностей и преимуществ, однако, они также приводят к появлению новых угроз и рисков, связанных с неправильным использованием информации и небезопасными действиями в сети. Дети и подростки активно используют компьютеры и интернет, но часто не осознают все возможные угрозы, с которыми могут столкнуться и не знают, как защитить себя в сети интернет.

Одной из основных проблем является проблема конфиденциальности и обмена личной информацией. Дети и подростки могут неосознанно раскрывать свои личные данные незнакомым людям в интернете или делиться конфиденциальной информацией, такой как их адрес или номер телефона, не осознавая возможных последствий. Это подвергает их риску стать жертвами кражи личных данных, киберзапугивания или даже офлайн-вреда со стороны лиц, извлекающих личную информацию в злонамеренных целях.

Социальные сети несут в себе угрозу киберзапугивания, которое может происходить анонимно и быстро распространяться на большую аудиторию. Кроме того, дети и подростки могут неосознанно встретить неподобающий контент. Воздействие таких материалов может негативно сказаться на их психическом и эмоциональном здоровье. Таким образом, на

сегодняшний день вопрос информационной безопасности в среде школьников является актуальной проблемой.

Успешная интеграция информационно-коммуникационных технологий в образование требует подготовки учителей и цифровой грамотности учащихся. Без этих ключевых элементов невозможно реализовать весь потенциал ИКТ в образовании. Поэтому, в условиях стремительного развития информационных технологий перед педагогами и школой ставится важная задача – формирование и развитие основ информационной безопасности, повышение информационной культуры.

Обучающийся, у которого сформирована и развита информационная безопасность получает возможность самостоятельно оценить угрозу получаемой информации, а значит способен обеспечить безопасную жизнь в условиях постоянно развивающегося информационного мира. Уделение особого внимания образованию в области информационной безопасности позволит учащимся стать ответственными и бдительными гражданами, эффективно противодействуя развивающимся цифровым угрозам, с которыми сталкивается наше общество.

Применяя на уроках современные педагогические методики, такие как информационно-коммуникационные и игровые технологии, личностно ориентированное обучение, методы проектов и интерактивные методы, педагог может научить обучающегося думать самостоятельно, принимать решения и нести ответственность за свой выбор. На уроках информатики стоит создавать такую ситуацию, которая даст возможность раскрыть личностные качества ученика, при этом развивая умения и навыки работы с информацией.

Следовательно, объективная общественная значимость исследуемого процесса, недостаточность теоретического обоснования и практической реализации исследуемых проблем обусловили выбор темы исследования «Формирование основ информационной безопасности на уроках информатики».

Цель исследования: поиск методических задач и эффективных методов, решающих проблему дефицита сформированности информационной безопасности обучающихся на уроках информатики.

Объект исследования: изучение вопросов информационной безопасности в школьном курсе информатики.

Предмет исследования: методика преподавания темы информационной безопасности в курсе Информатики для учеников 5-9 классов.

Для достижения поставленной цели определены следующие задачи:

1. Изучить теоретические основы по теме «Информационная безопасность».

2. Провести анализ изложения темы в учебных комплексах и учебно-методической литературе.

3. Создать методическую разработку по теме «Информационная безопасность».

4. Выполнить оценку и анализ эффективности внедрения методов по формированию информационной безопасности.

Методы исследования: педагогический эксперимент и анализ литературных источников и методической литературы.

Гипотеза исследования состоит в том, что, если использовать при изучении информационной безопасности активные методы обучения, такие как: разбор кейсов, обсуждение теоретического материала, то это сформирует знания в области информационной безопасности, что позволит учащимся более качественно противостоять угрозам безопасности.

Практическое значение полученных результатов исследования заключается в:

− апробации методов формирования информационной безопасности в образовательном процессе предмета информатика,

− разработке методики обучения по формированию

информационной безопасности у учащихся.

Предложенные рекомендации данного исследования могут быть использованы в практической работе учителей, классных руководителей и организаторов воспитательной работы.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ВОПРОСЫ ФОРМИРОВАНИЯ У ОБУЧАЮЩИХСЯ ОСНОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Теоретические основы обучения информационной безопасности школьников в школьном курсе информатики 5-9 классов

Для изучения информационной безопасности в рамках школьного курса «Информатика», необходимо предварительно определить суть терминов «информация» и «информационная безопасность».

Информация – абстрактное понятие в предмете «Информатика и ИКТ», которое рассматривается как объем данных [3].

Информационная безопасность – состояние защищенности информации и информационной среды от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, (в том числе владельцам и пользователям информации) [2].

Конфиденциальность информации – процесс обеспечения доступа к информации только авторизованным пользователям [3].

Целостность информации – обеспечение достоверности и полноты информации и методов её обработки [1].

Информационная безопасность состоит из нескольких аспектов:

− безопасность человека от информационных рисков заключается в его неподверженности разрушительному воздействию и сохранении личностной неприкосновенности. Социальная активность человека существенно зависит от осознания получаемой информации, обмена информацией с другими людьми и частого использования информации в качестве ключевого элемента своей деятельности,

− безопасность личности в информационной сфере обеспечивается путем создания условий для свободной реализации и защиты

информационных прав граждан, обеспечения защиты личной тайны и иной принадлежащей гражданам, конфиденциальной информации, а также защиты от правонарушений в области информационной безопасности, включая защиту от злоупотребления правами в информационной сфере.

Информационная безопасность общества крайне важна для его развития и функционирования. Она заключается в невозможности нанесения вреда его духовной сфере, культурным ценностям, информационной инфраструктуре [20]. Социальные регуляторы поведения людей, такие как законы, нормы, правила и этические принципы, обеспечивают гармоничное сосуществование в обществе. Однако, с развитием информационных технологий стали возможными новые виды преступлений и нарушений, которые наносят вред не только отдельным индивидам, но и обществу в целом. Нарушение информационной инфраструктуры безопасности может привести к утечке конфиденциальных данных, разрушению систем и сервисов, прерыванию коммуникации и прочим негативным последствиям. Информационная безопасность общества является сложной и многоуровневой задачей. Она требует постоянного внимания и защиты для обеспечения сохранение ценностей, значимых для общества, и защиты его устойчивого развития.

Информационная безопасность личности – это:

1) состояние защищенности, при котором отсутствует угроза (минимален риск) причинения вреда информации, которой владеет личность;

2) состояние и условие жизнедеятельности личности, при которых отсутствует угроза (минимален риск) нанесения вреда личности информацией [7].

Информационная безопасность личности (применительно в области образования) – состояние защищенности жизненно важных интересов личности, проявляющееся в умении выявлять и идентифицировать угрозы

информационного воздействия и умении скомпенсировать негативные эффекты информационного воздействия [12].

Понятие «информационная безопасность» в наше время имеет двойное толкование. В широком смысле оно означает состояние, когда личность, общество и государство надежно и всесторонне защищены от специфических угроз, представляющих собой организованные информационные потоки, направленные на искажение общественного и индивидуального сознания. В узком смысле понятие относится к безопасности информации и каналов передачи и приема, а также к организации защиты от применения информационного оружия противником во время вооруженных конфликтов. Характерно, что в узком смысле трактовка данного понятия имеет техническую ориентацию и является организационным инструментом обеспечения информационной безопасности в широком смысле.

Следовательно, информационная безопасность является важным аспектом в нашем современном мире. Она охватывает не только защиту конфиденциальных данных и информационных систем, но также и безопасность детей, личности, общества, государства и даже международную безопасность. В связи с этим, для обеспечения информационной безопасности необходимо разрабатывать методические рекомендации и образовательные программы, сфокусированные на обучении в системе непрерывного образования. Целью такого обучения должно быть обеспечение безопасного и адекватного использования информационных технологий и ресурсов среди детей, молодежи, взрослых и специалистов.

В образовательных стандартах основной и старшей школы явным образом указано понятие «информационная безопасность», в школьных учебниках информатики авторы, как правило, определяют и концентрируют внимание обучающихся на термине «защита информации», который упоминается только в примерной программе для основной школы

применительно к средствам защиты личной информации и учебной программе по предмету «Информатика» применительно к защите от вредоносного программного обеспечения и защите персональных данных.

Информационная безопасность личности включает в себя три аспекта безопасности: информационно-техническую, информационно-идеологическую и информационно-психологическую. Информационно-техническая безопасность личности означает защиту информации от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут причинить вред личности [16]. Информационно-идеологическая безопасность личности означает защиту личности от преднамеренного или непреднамеренного информационного воздействия, которое может привести к нарушению прав и свобод в области создания, потребления и распространения информации, использования информационной инфраструктуры и ресурсов, противоречащих нравственно-этическим нормам и имеющих деструктивное воздействие на личность [13]. Информационно-психологическая безопасность означает состояние защищенности отдельных лиц или групп лиц от негативного информационно-психологического воздействия, которое угрожает жизненно важным интересам личности, общества и государства в информационной сфере.

Безопасность информации – состояние защищенности данных, при котором обеспечиваются их конфиденциальность, доступность и целостность. Безопасность информации определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе [2].

Угрозы информационной безопасности – совокупность условий, факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [2].

Атакой называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, называется злоумышленником. Потенциальные злоумышленники называются источниками угроз [2].

Угроза является следствием наличия уязвимых мест или уязвимостей в информационной системе. Уязвимости могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ [2].

Угрозы информационной безопасности можно классифицировать по нескольким критериям. В первую очередь, угрозы могут быть направлены против свойств информации, таких как доступность, целостность и конфиденциальность [4]. Также, угрозы могут быть нацелены на различные компоненты информационных систем. Это могут быть данные, программы, аппаратура или поддерживающая инфраструктура. В зависимости от цели атаки, угрозы могут нанести вред различным аспектам информационной системы.

Другой важный критерий классификации – способ осуществления угроз. Атаки могут являться случайными или преднамеренными, а также могут быть вызваны действиями природного или техногенного характера. Это позволяет определить потенциальные источники угроз и разрабатывать соответствующие меры защиты [18]. Наконец, угрозы могут происходить как изнутри, так и извне рассматриваемой информационной системы. Часто угрозы со стороны сотрудников или пользователей системы могут иметь более серьезные последствия, так как они имеют легальный доступ к информации. Однако, не следует забывать и о внешних угрозах, которые могут быть вызваны злоумышленниками с целью получения незаконного доступа.

Поведение школьников в интернете имеет свои особенности, связанные с возрастными изменениями, уровнем критического мышления, внимательностью, кругом общения, интересами. Обучающиеся могут стать зависимыми от интернета, проводя много времени онлайн и

испытывая трудности с ограничением этого времени. Они могут предпочитать виртуальное общение реальному и пренебрегать учебой или другими физическими и социальными активностями. Также, многие увлекаются онлайн-играми и могут проводить в них значительное количество времени.

Часто злоумышленники провоцируют подростков критикой, угрозами или манипуляциями с целью воздействия на их эмоциональное состояние и самооценку. Это может привести к психологическому давлению, тревоге и даже депрессии у подростков. Интернет-буллинг или цифровое насилие на сегодняшний день достаточно распространённая проблема. Интернет-буллинг может проявляться через различные формы: публикация оскорбительных комментариев, угрозы, публикация компрометирующих материалов, распространение слухов и дезинформации, подделка личных данных и т.д. Часто целью интернет-буллинга является попытка покалечить эмоциональное состояние жертвы, вызвать страх или дискредитировать ее в глазах других людей. Школьникам нужно быть осведомленными об этих рисках и уметь защищать себя в интернете. Родители, учителя и другие взрослые должны помогать детям развивать навыки безопасного и ответственного поведения в интернете. Взаимодействие с детьми, открытая коммуникация, внедрение функции «родительский контроль» и обучение основам интернет-безопасности могут снизить риски и помочь школьникам использовать интернет в положительном и продуктивном направлении.

Еще одна проблема, требующая внимания, это – социальный инжиниринг. Социальная инженерия не подразумевает использования технических средств для сбора информации о цели [6]. Социальный инжиниринг – это совокупность психологических и социологических приёмов, методов и технологий, которые позволяют получить конфиденциальную информацию. Метод основан на использовании слабостей человеческого фактора и является очень эффективным,

включает в себя несколько техник. Одной из популярных техник является – фишинг. Фишинг является одной из разновидностей мошенничества. Киберпреступники используют электронную почту, мгновенный обмен сообщениями или социальные сети для сбора информации, такой как учетные данные для входа или данные учетной записи, маскируясь под уже известную организацию или человека. При фишинге киберпреступник отправляет мошенническое электронное сообщение, замаскированное под сообщение из доверенного, надежного источника. Это сообщение должно убедить получателя установить вредоносное ПО на свое устройство или сообщить личную или финансовую информацию [6]. Обычно фишинг осуществляется путем отправки электронных писем, которые похожи на официальные сообщения от известных компаний или организаций, и могут содержать просьбы о вводе личной информации на фальшивых веб-сайтах или поврежденных ссылках.

Следующий метод, так называемый, плечевой серфинг – это метод, используемый злоумышленниками для получения конфиденциальной информации, путем наблюдения личной информации жертвы через её плечо. Преступник следит за жертвой или буквально подглядывает через плечо, чтобы узнать PIN-код, код доступа или номер кредитной карты [6]. Такая атака может происходить в общественных местах, например, в кафе, аэропортах, общественном транспорте и т.д. Также, достаточно популярными методами социального инжиниринга являются фейки и дипфейки. Фейки – это выдуманные или поддельные сведения, информация или материалы, которые представляются как настоящие или истинные. Термин «фейки» также используется для обозначения поддельных документов, поддельных новостей или подделок в интернете. Дипфейк – это создание поддельных фото, аудио или видеофайлов с помощью искусственного интеллекта. Ситуация усугубляется тем, что на сегодняшний день данная технология доступна и для обычных пользователей интернета.

Другим примером методов социального инжиниринга является использование геоданных для отслеживания местоположения людей с целью совершения преступлений, таких как грабежи или вымогательство. Злоумышленники могут использовать слежку или мониторинг мобильных устройств, основываясь на их геоданных. Также существуют случаи, когда геоданные могут быть использованы для мошеннической продажи товаров или услуг. Например, злоумышленники могут использовать поддельные геоданные, чтобы представить свои товары или услуги, как доступные в определенной локации, чтобы привлечь покупателей.

Важно обучать детей навыку защиты персональных данных. Учить их быть внимательными к сообщениям и электронным письмам. Проверять отправителя и обращать внимание на формулировки, опечатки и странные запросы, не открывать подозрительные вложения или ссылки. Не раскрывать личную информацию без необходимости, быть осторожным с предоставлением паролей, номеров кредитных карт и других конфиденциальных данных. Также, важно объяснить школьникам всю пользу и важность двухфакторной аутентификации при входе в различные онлайн-сервисы, которая предоставляет возможность подтверждения личности с помощью ввода специального кода на электронную почту, sms-уведомления.

Поможет повысить уровень безопасности в сети также соблюдение некоторых правил при работе с информационными системами. Сложный пароль важен для обеспечения безопасности личной информации и защиты от попыток несанкционированного доступа к аккаунтам. Сложные пароли, состоящие из комбинации символов, букв и цифр, значительно увеличивают сложность для злоумышленников и программных атак. Кроме того, использование сложных паролей помогает защитить личные данные от угадывания и позволяет быть уверенным в безопасности своего онлайн-профиля. Существует специальное программное обеспечение для хранения и управления паролями, оно защищает пароли сильным

шифрованием и требует одного основного пароля для доступа к общему списку паролей. Также можно создать зашифрованный файл с паролями и хранить его в надежном месте.

Прежде чем вводить свою персональную информацию на сайт следует проверить его достоверность. Проверить контактную информацию: есть ли на сайте контактная информация, такая как телефон, адрес электронной почты или физический адрес. Изучить платежные методы сайта. Официальные сайты обычно предлагают безопасные способы оплаты, такие как кредитные карты или платежные системы с хорошей репутацией. Воспользоваться поисковыми системами, чтобы найти дополнительную информацию о сайте или компании. Если есть отчеты о мошенничестве или негативный опыт других пользователей, это может быть предупреждающим знаком. По возможности, подключать двухфакторную аутентификацию.

Также существуют криптографические способы защиты информации. Шифрация трафика – это процесс преобразования данных, передаваемых между двумя или более устройствами, таким образом, чтобы они были защищены от несанкционированного доступа или прослушивания [11]. Это важная мера безопасности, используемая во многих областях, включая интернет-связь, сети компаний и банковские операции. Для шифрования трафика обычно используются различные алгоритмы и протоколы шифрования, которые обеспечивают конфиденциальность и целостность передаваемых данных. При передаче данных через шифрованное соединение, информация кодируется с использованием ключа шифрования, который обеспечивает ее безопасность. Только устройства с правильным ключом могут расшифровать данные и прочитать их содержимое. Это обеспечивает защиту от несанкционированного доступа и подмены данных. Шифрация трафика играет важную роль в защите данных и конфиденциальной информации от злоумышленников и кибератак. Она обеспечивает доверие

и ощущение безопасности пользователям при обмене информацией через сеть.

Еще одним криптографическим способом защиты информации является электронно-цифровая подпись. Электронно-цифровая подпись (ЭЦП) – это криптографический метод, используемый для подтверждения подлинности и целостности электронных сообщений, документов или данных [9]. Она использует асимметричное шифрование, где создается пара ключей: приватный и публичный. Приватный ключ хранится у владельца, а публичный ключ распространяется для проверки подписи. Для создания ЭЦП отправитель хеширует сообщение (результат хэш-функции), а затем шифрует полученный хеш своим приватным ключом. Полученная цифровая подпись присоединяется к сообщению.

К техническим средствам защиты информации относятся: антивирусные программы, файерволы, регулярные обновления операционной системы. Антивирусные программы – это специальные программы, разработанные для защиты компьютера или других устройств от вирусов, троянов, шпионского ПО и других вредоносных программ [10]. Они обнаруживают, блокируют и удаляют вредоносные файлы, а также предотвращают их попадание на устройство. Важно отметить, что ни одна антивирусная программа не является 100% защитой от всех видов вредоносных программ. Поэтому рекомендуется использовать политику безопасности, такую как установка обновлений операционной системы, использование сильных паролей и аккуратное поведение в Интернете, в дополнение к установке антивирусного программного обеспечения.

Файерволы – это программное или аппаратное обеспечение, которое применяется для защиты компьютерных систем от несанкционированного доступа и вредоносного программного обеспечения [14]. Файерволы контролируют входящий и исходящий сетевой трафик, а также применяют различные методы фильтрации, чтобы позволить блокировать определенные типы запросов или данных. Файерволы могут быть

реализованы в виде софтверных приложений, работающих на операционной системе или в виде аппаратных устройств, предназначенных для обработки сетевого трафика на физическом уровне. Они широко применяются в организациях и домашних сетях для защиты от угроз в сети.

Регулярные обновления операционной системы включают в себя обновление драйверов, исправления ошибок, улучшение производительности и безопасности. Обновления проводятся разработчиками операционной системы и выходят по мере необходимости. Важность регулярных обновлений операционной системы заключается в защите от уязвимостей и вирусов. Киберугрозы постоянно развиваются, и хакеры ищут новые способы взлома систем. Обновления операционной системы содержат исправления, которые были предназначены для предотвращения таких угроз. Как правило, операционная система предлагает настройки автоматических обновлений, которые позволяют устанавливать все необходимые обновления без вашего вмешательства. Рекомендуется включить эти настройки и регулярно проверять наличие новых обновлений, чтобы ваша операционная система всегда была защищена и работала наилучшим образом.

Таким образом, классификация угроз информационной безопасности основывается на различных критериях, позволяя оценить и уделять должное внимание различным аспектам защиты информационных систем.

Обеспечение информационной безопасности является непростой задачей, для решения которой требуется комплексный подход. Выделяют следующие уровни защиты информации:

1) законодательный уровень – законы, нормативные акты и прочие документы РФ и международного сообщества;

2) административный уровень – комплекс мер, предпринимаемых

локально руководством организации;

3) процедурный уровень – меры безопасности, реализуемые людьми;

4) программно-технический уровень – непосредственно средства защиты информации.

Законодательный уровень является фундаментальным компонентом системы защиты информации, так как он предоставляет основные понятия в предметной области и устанавливает меры наказания для потенциальных злоумышленников [19]. Роль этого уровня заключается в координации и направлении, помогая поддерживать негативное (и карательное) отношение общества к тем, кто нарушает информационную безопасность.

Системный подход к информационной безопасности требует определения ее субъектов, средств и объектов, источников опасности, направленности опасных информационных потоков и принципов обеспечения информационной безопасности (рисунок 1).

Рисунок 1 – Системное понимание информационной безопасности личности

Информационная безопасность играет центральную роль в современном обществе, обеспечивая защиту данных и инфраструктуры, поддержание экономической стабильности, защиту прав и свобод индивидуумов, а также способствует развитию технологий и инноваций[17].

Информационная безопасность для школьников имеет большое значение, так как дети и подростки активно пользуются интернетом и могут быть не осведомлены о потенциальных рисках и угрозах. Школьники должны знать о своих правах в интернете и о том, как их защитить, а также об обязанностях, чтобы уважать чужую конфиденциальную информацию. Изучение информационной безопасности способствует развитию критического мышления, помогая анализировать информацию и принимать обоснованные решения в интернете. Таким образом, важность информационной безопасности для школьников не может быть переоценена. Она помогает обеспечить их безопасность в онлайн-пространстве и воспитывает ответственных и осведомленных пользователей цифровых технологий.

1.2 Основные аспекты информационной безопасности в школьной программе предмета «Информатика» 5-9 классов

Современный мир олицетворяет собой множество угроз, и в такой ситуации безопасность жизни становится главным фактором, определяющим качество нашего существования. Одной из ключевых составляющих безопасности является информационная безопасность. Отправная точка для достижения этой цели – формирование компетентности учащихся в области информационной безопасности.

Цель обучения информационной безопасности школьников заключается в том, чтобы они, по окончании школы, овладели компетенциями в сфере информационной безопасности, что позволит им успешно адаптироваться в современном информационном обществе. Соответственно, необходимо сформировать полное представление о предметной области обеспечения информационной безопасности, что включает информационную безопасность детей, личности, государства, общества и международную информационную безопасность. Все это

должно происходить в условиях информатизации общества, когда развитие информационных и коммуникационных технологий делает средства массовой информации основным институтом социализации, выполняющим функции традиционных социальных институтов, таких как школы, группы сверстников, семьи и государства.

В современном обществе активное использование информационных и коммуникационных технологий становится неотъемлемой частью жизни школьников. Развитие технологий значительно изменило способ взаимодействия и получения информации, и школьное обучение не осталось в стороне от этих изменений. Интернет предоставляет бесконечные источники знаний и информации на любую тему. Школьники могут проводить исследования, изучать новые темы и расширять свой кругозор. Кроме того, использование ИКТ в образовательной среде способствует развитию цифровой грамотности у школьников. Они учатся эффективно искать информацию в сети, оценивать ее достоверность и критически мыслить. Такие навыки в современном мире являются необходимыми для успешного функционирования и адаптации в информационном пространстве.

Однако развитие навыков свободной ориентации в современной информационной среде, организация поисковой деятельности, использование различных стратегий познания приводят к увеличению уровня информационных угроз, с которыми может столкнуться школьник. Обучающиеся взаимодействуют с информационным пространством больших масштабов, которое, к тому же, является неоднородным. При этом приоритеты информационного взаимодействия учащихся определяются динамикой их возрастного развития в процессе структурирования их информационной и общей социализации.

Исходя из вышеописанного, важно не только обучить обучающихся оценивать и объективно анализировать информацию, принимая во внимание возможные угрозы, но также необходимо сформировать у них

навыки, которые обеспечат их информационную безопасность как личностей, интегрированных в социальную структуру, и обеспечить полное понимание различных аспектов информационной безопасности как объекта.

Рассматривая ФГОС по Информатике основного общего образования, хотелось бы отметить, что целью обучения Информационной безопасности в ходе освоения общеобразовательной программы является формирование у учащихся навыков использования коммуникационных и информационных технологий для решения задач с соблюдением всех соответствующих норм информационной безопасности.

На сегодняшний день в соответствии с примерной основной образовательной программой основного общего образования, необходимость изучения информатики в 5-6 классах не включена в обязательную часть учебного плана. Однако, образовательная организация имеет возможность выделить время на данный курс путем распределения части учебного плана, что определяется взаимодействием участников образовательного процесса. Федеральная рабочая программа по учебному предмету «Информатика» реализована для 7-9 классов базового и углубленного уровней обучения. Она включает в себя: пояснительную записку, содержание обучения, планируемые результаты обучения и тематическое планирование.

Таблица 1 – Требование стандартов для основной школы по вопросам обеспечения информационной безопасности

Стандарт (средняя школа)	
Базовый уровень (7-9 классы)	Углубленный уровень (7-9 классы)
1	2
Личностные результаты изучения предметной области «информатика» в 7-9 классах должны отражать: *освоение обучающимися социального опыта, основных социальных ролей, соответствующих ведущей деятельности возраста, норм и правил общественного поведения, форм социальной жизни в группах и сообществах, в том числе существующих в виртуальном пространстве.*	Личностные результаты изучения предметной области «информатика» в 7-9 классах должны отражать: *получение опыта в области социального взаимодействия, осваивание основных социальных ролей, связанных с их возрастом и основными деятельностями. Они также учатся соблюдать общественные нормы и правила поведения, анализировать формы социальной жизни в различных группах и сообществах, включая виртуальное пространство.*

Продолжение таблицы 1

1	2
Метапредметные результаты изучения предметной области «информатика» в 7-9 классах должны отражать: *оценивать достоверность информации по критериям, предложенным учителем или сформулированным самостоятельно;* *проводить выбор в условиях противоречивой информации и брать ответственность за решение.* *осознавать невозможность контролировать всё вокруг даже в условиях открытого доступа к любым объёмам информации.*	Метапредметные результаты изучения предметной области «информатика» должны отражать: *Оценка достоверности информации и умение эффективно запоминать и систематизировать ее;* *Получение навыка делать выбор в условиях противоречивой информации и брать ответственность за решение.* *осознавать, что невозможно контролировать все аспекты окружающего нас мира, даже при наличии открытого доступа к огромным объемам информации*
Предметные результаты изучения предметной области «информатика» в 7 классе должны отражать: *кодировать и декодировать сообщения по заданным правилам, демонстрировать понимание (пояснять сущность) основных принципов кодирования информации различной природы.* *соблюдать сетевой этикет, базовые нормы информационной этики и права при работе с приложениями на любых устройствах и в Интернете, выбирать безопасные стратегии поведения в сети;* *использовать различные средства защиты от вредоносного программного обеспечения, обеспечивать личную безопасность при использовании ресурсов сети Интернет, в том числе защищать персональную информацию от несанкционированного доступа и его последствий (разглашения, подмены, утраты данных) с учётом основных технологических и социально-психологических аспектов использования сети Интернет (сетевая анонимность, цифровой след, аутентичность субъектов и ресурсов, опасность вредоносного кода);* *искать информацию в Интернете (в том числе, по ключевым словам, и по изображению), критически относиться к найденной информации, осознавая опасность для личности и общества распространения вредоносной информации, в том числе экстремистского и террористического характера;* *использовать современные сервисы интернет-коммуникаций, цифровые сервисы государственных услуг, цифровые образовательные сервисы;*	Предметные результаты изучения предметной области «информатика» в 7 классе должны отражать: *соблюдать сетевой этикет, базовые нормы информационной этики и права при работе с приложениями на любых устройствах и в Интернете, выбирать безопасные стратегии поведения в сети; использовать различные средства защиты от вредоносного программного обеспечения, обеспечивать личную безопасность при использовании ресурсов сети Интернет, в том числе защищать персональную информацию от несанкционированного доступа и его последствий (разглашения, подмены, утраты данных) с учётом основных технологических и социально-психологических аспектов использования сети Интернет (сетевая анонимность, цифровой след, аутентичность субъектов и ресурсов, опасность вредоносного кода); искать информацию в Интернете (в том числе по ключевым словам и по изображению), критически относиться к найденной информации, осознавая опасность для личности и общества распространения вредоносной информации, в том числе экстремистского и террористического характера;* Предметные результаты изучения предметной области «информатика» в 9 классе должны отражать: *приводить примеры сфер профессиональной деятельности, связанных с информатикой, программированием и современными информационно-коммуникационными технологиями; приводить примеры перспективных направлений развития информационных*

Окончание таблицы 1

1	2
Предметные результаты изучения предметной области «информатика» в 9 классе должны отражать: *приводить примеры сфер профессиональной деятельности, связанных с информатикой, программированием и современными информационно-коммуникационными технологиями; приводить примеры перспективных направлений развития информационных технологий, в том числе искусственного интеллекта и машинного обучения; распознавать попытки и предупреждать вовлечение себя и окружающих в деструктивные и криминальные формы сетевой активности (в том числе кибербуллинг, фишинг).*	*технологий, в том числе искусственного интеллекта и машинного обучения; распознавать попытки и предупреждать вовлечение себя и окружающих в деструктивные и криминальные формы сетевой активности (в том числе кибербуллинг, фишинг).*

В анализе результатов изучения предметной области «информатика» в 7-9 классах федеральной рабочей программы, можно отметить, что начиная с 7 класса у обучающихся должны формироваться и развиваться компетенции в области использования информационно-коммуникационных технологий, в том числе знаний, умений и навыков работы с информацией в современных цифровых средах в условиях обеспечения информационной безопасности личности обучающегося. Навыки, которые учащиеся получают в процессе изучения информатики, должны помочь им эффективно использовать информационные ресурсы и технологии для решения задач и достижения целей. Это включает умение находить и оценивать информацию, критически рассматривать ее и применять для решения практических задач, осознавать возможные риски.

1.3 Анализ учебной литературы курса «Информатика» для 5-9 классов

Выполнив анализ содержания учебников на наличие в них требований стандартов и примерных образовательных программ в области обучения вопросам информационной безопасности учащихся основной школы, хотелось бы отметить, что авторы включают в содержание учебника

практически все понятия стандарта. Но многие авторы не вводят понятие «информационная безопасность» несмотря на то, что оно указано в требованиях ФГОС для основной школы. Так, например, в учебниках авторов К.Ю. Полякова и Е.А. Еремина в 7 классе в главе «Введение в информатику» присутствует подпункт, описывающий вопрос достоверности информации в сети, в 9 классе в главе «Информационное общество» раскрыты такие понятия, как «информационное общество», «информационные технологии», но понятие «информационная безопасность» отсутствует. В учебнике 9 класса автора И.Г. Семакина, есть параграф «Информационная безопасность», в котором тоже отсутствует определение понятия. Параграф, посвященный данной теме описывает некоторые виды компьютерных преступлений, программно-технические способы защиты информации, также И.Г. Семакин приводит некоторые рекомендации по использованию социальных сетей.

Таким образом, точное определение можно найти в учебнике для 9 класса «Информатика» автора Л.Л. Босовой [5]: «информационная безопасность – это защищенность информации которой обладает человек, исключение рисков ее уничтожения, искажения и утечки, которые могут привести к невосполнимым потерям или ущербу для лица, обладающего этой информацией.». Понятие также раскрыто в учебнике для 9 класса «Информатика» автора А.Г. Гейн [7]: «информационная безопасность – это защищенность информационных систем от любых действий, в результате которых содержащаяся в них информация может быть искажена, утеряна, или использована во вред собственникам информации или её законным представителям».

В рамках модели содержания обучения учащихся средней школы предусматривается соблюдение принципа преемственности знаний по информационной безопасности с предыдущими этапами обучения, а также систематизация понятий в данной сфере. Для эффективного обучения школьников информационной безопасности, следует использовать принцип

спирального обучения, чтобы гарантировать соответствие уровня сложности материала возрастным особенностям учеников. Очень важно, чтобы понятия были раскрыты в подробностях, чтобы школьники проявили больший интерес к вопросам информационной безопасности, расширили свои знания и повысили мотивацию для усвоения нового материала. Однако, анализ учебной литературы привёл к выводу, что во многих учебниках данный принцип отсутствует.

Так, например, в учебнике автора И.Г. Семакина в 7 и 8 классах нет параграфов, касающихся информационной безопасности. В 7 классе в 1 главе «Человек и информация» рассматривается определение «информации» и способы её восприятия человеком, описаны информационные процессы. В 8 классе в 1 главе «Передача информации в компьютерных сетях» подробно описан процесс использования и назначение электронной почты, рассмотрены понятия телеконференции и коллективных проектов в сети. Таким образом, у данного автора понятия, касающиеся темы информационной безопасности раскрыты в учебнике «Информатика» для 9 класса в главе «Информационное общество».

Анализируя учебники автора К.Ю. Полякова, можно также отметить неравномерное раскрытие вопросов, касающихся информационной безопасности. В 7 классе описаны такие понятия, как «интернет» и «сервер», в конце первого параграфа главы есть раздел «достоверность информации в интернете», в которой делается акцент на достоверности информации, автор предлагает обращать внимание на авторитетность сайта и дает следующие определение данному понятию [15]: «для оценки достоверности информации важна авторитетность сайта – как часто на него ссылаются с других сайтов, как оценивают сайт поисковые системы (появляется ли ссылка на сайт на первой странице с результатами поиска или на 31-й». Также в учебнике есть параграф «Правовая охрана программ и данных», в котором рассматриваются понятие «авторские права», «лицензионное ПО». Далее в учебнике присутствует параграф на

тему «Защита от компьютерных вирусов». Таким образом в учебнике по информатике за 7 класс автора Полякова присутствуют темы, связанные с информационной безопасностью. Однако, в 8 классе не обнаружено тем, связанных с данным направлением. В последних параграфах учебника 9 класса есть тема «Информационное общество», где рассматриваются такие понятия как «информационные технологии», «информационное общество», но в других главах информации о безопасности в сети не найдено.

Далее для дополнительного подтверждения отсутствия принципа спирального обучения в некоторых учебниках можно привести в пример учебники по информатике автора А.Г. Гейн. В 7 классе не обнаружено тем, связанных с информационной безопасностью. В 8 классе есть глава под названием «Человек и информация», в ней раскрыты такие темы, как: «информация и её свойства», «информационная грамотность». Также, в параграфах, связанных с темой «Интернет», есть разделы, в которых ученикам рассказывают о возможностях интернета, поисковых сетей. В 9 классе в главе «Информация и общество» рассмотрена тема и дано определение понятию «информационная безопасность». Несмотря на то, что автор в своих учебниках рассматривает темы, связанные с информационной безопасностью в 8 и 9 классах, при этом обучающиеся в 7 классе не получают знаний по данной теме. В учебниках автора есть темы, связанные с информационной безопасностью, но стоит учитывать, что на сегодняшний день начинать обучение безопасности в интернете в 8 классе достаточно поздно.

Анализ содержания учебников также показывает взаимосвязь технологических научных понятий в области информационной безопасности и более широкого круга понятий, относящихся к информационной культуре, такие как: информационная этика, этика интернета, компьютерная этика, сетевой этикет, правила сетевого взаимодействия, нормы поведения при использовании информации. Это связано с тем, что информационная безопасность на сегодняшний день

является неотъемлемой частью жизни школьников, охватывая различные сферы и оказывая важное влияние на их учебный процесс, повседневную жизнь и будущую профессиональную деятельность.

Важно отметить, что школьникам часто бывает сложно понять некоторые определения, такие как «информационная культура» и «информационная этика». Действительно, эти термины могут показаться абстрактными и неочевидными. Для улучшения понимания этих понятий и развития информационной культуры у школьников на уроках информатики важно применять различные подходы и методы, которые помогут конкретизировать данные понятия.

Например, в учебнике «Информатика» для 9 класса автором А.Г. Гейн в главе «Информация и общество» рассмотрены темы «Этика в Интернете» и «Информационная безопасность. Защита информации». В главе устанавливается важная связь между понятием «информационная культура» и аспектами информационной безопасности [8]: «Информационная культура каждого человека подразумевает готовность человека к жизни и деятельности в высокоразвитой информационной среде, умение эффективно использовать ее возможности и защищаться от ее негативных воздействий». В описании составляющих элементов информационной культуры указаны не только аспекты, имеющие прямое отношение к информационной безопасности и этичному поведению при использовании информации, но и подчеркивается взаимосвязь между понятиями «информационная этика» и «информационная культура».

В учебнике Л.Л. Босовой «Информатика (базовый уровень)» для 7 класса [15] рассматриваются такие важные темы обеспечения информационной безопасности, как общение в интернете в режиме реального времени, современные мессенджеры и технология видео-конференц-связи с актуальными на сегодняшний день приложениями. Также в параграфе приведены правила сетевого этикета, автор в своем

тексте ссылается на сайт «Лаборатории Касперского», на котором учащиеся могут пройти тест на знание этикета в сети.

Интересно отметить, что такие важные и актуальные понятия как: «фишинг», «кибербуллинг» не рассматриваются авторами большинства учебников. На мой взгляд, понимание данных терминов является неотъемлемым условием, снижающим риск угроз для школьников, пребывающих в интернет-пространстве. В связи с этим, акцент должен быть сделан на обучении учащихся навыкам эффективного противодействия подобным угрозам в онлайн-мире. Одним из возможных объяснений данной ситуации является то, что школьные учебники обновляются редко и устаревают, но при этом развитие информационных технологий и новых явлений в сети происходит очень быстро.

В ходе анализа было рассмотрено обновленное 5-е издание учебника «Информатика» автора Л.Л. Босовой за 2023 год. В главе «Интернет-коммуникации и правила их использования» автор дает определение термину «фишинг» [15]: «Фишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (их логинам и паролям)». В разделе «вопросы и задания» присутствует задание, в котором автор предлагает обучающимся с помощью дополнительных источников самостоятельно найти определения терминов «кибербуллинг», «троллинг», то есть в главе учебника этих понятий нет.

Стоит также отметить, что в большинстве учебников, темы, связанные с информатизацией общества и информационной безопасностью описаны в последних главах, то есть обучающиеся рассматривают данный материал в конце учебного года, поэтому можно сделать вывод, что в течение остального учебного времени вопросы безопасности в сети практически не затрагиваются на уроках.

В целом, обучение информационной безопасности помогает школьникам стать более осознанными и безопасными пользователями

интернета и вносит вклад в формирование информационно-коммуникативных компетенций, которые являются неотъемлемой частью современного образования. Школьники должны учиться уважать чужие права и конфиденциальность, развивать критическое мышление и умение критически оценивать информацию, проверять источники, различать факты от мнений. Обучать этим навыкам следует системно и регулярно, потому как любой учащийся сегодня – в той или иной мере, пользователь сети Интернет, и чем раньше ученик получит основные навыки, связанные с информационной безопасностью, тем выше будет уровень его защищенности как пользователя сети.

Выводы по главе 1

Высокую актуальность данной темы косвенно подтверждает тот факт, что информационная безопасность важна не только как личные достижения, которые школьнику необходимо приобрести, но и как ключевой элемент государственной безопасности. Это подтверждается значительным числом нормативных документов, которые обосновывают необходимость обеспечения высокого уровня информационной безопасности для защиты граждан во всех сферах и особенно в информационной сфере.

Однако федеральный государственный стандарт образования не охватывает все необходимые результаты, так как не успевает учитывать новые угрозы и их различные изменения. Для решения этой задачи необходимо разработать основные элементы стандарта, которые удовлетворяли бы большинству требований информационной безопасности.

Чтобы достичь желаемых результатов, необходимо создать актуальные методические комплексы, которые включали бы современную учебно-методическую литературу, отражающую последние достижения в области информационной безопасности и стремящуюся быть в курсе

актуальных киберугроз.

Анализ учебных комплексов по информатике и ИКТ для 7-9 классов различных авторов выявил недостаточное содержание актуальной информации о безопасности в информационной сфере. Эта информация не способна обучить учащихся правильному реагированию на угрозы информационной безопасности. Методики, применяемые для обучения основам информационной безопасности, не могут быть достаточно оперативными в отношении быстро развивающихся технологий интернет-мошенничества и кибератак, и не могут обеспечить высокий уровень грамотности в этой сфере. Учебные комплексы должны обучать учащихся адекватным и действенным способам реагирования на большинство киберугроз, с которыми они могут столкнуться в информационной сфере.

ГЛАВА 2. РАЗРАБОТКА МЕТОДИКИ ОБУЧЕНИЯ ПО ТЕМЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

2.1 Методическая разработка по теме «Информационная безопасность» по предмету «Информатика»

С развитием мобильных и переносных устройств произошел существенный прорыв в доступности интернета. Мобильные сети совершенствуются, скорость передачи данных растет, а зоны покрытия расширяются. В результате каждый год наблюдается огромный прирост интернет-трафика, который будет продолжаться и расти далее. Но этому развитию присуща не только положительная сторона. Вместе с прогрессом мобильных и компьютерных технологий непрерывно развиваются и технологии мошенничества и киберугроз.

Для формирования у школьников навыков и знаний в области информационной безопасности нужно разработать современные методические комплексы. Они должны включать в себя актуальную учебно-методическую литературу, отражающую современную информацию о киберугрозах. Эти материалы должны быть способными оперативно реагировать на появляющиеся угрозы в информационной сфере. Главная цель методических материалов – научить школьников адекватному и эффективному реагированию на большинство киберугроз, с которыми они могут столкнуться в сфере информационной безопасности.

В рамках исследования было разработано содержание нескольких учебных занятий для учащихся 5-9 классов по изучению вопросов информационной безопасности и способов противостояния угрозам. Вопросы информационной безопасности лучше рассматривать циклично – посвящать 1-2 урока в каждом классе с 5 по 9, или включать материалы в занятия для активных методов работы на уроке. С учетом возрастных особенностей и уровня знаний учащихся целесообразно ввести следующее

содержание таких уроков.

Таблица 2 – Краткое содержание занятий по информационной безопасности

Класс	Урок	Тема	Цели	Изучаемые вопросы	Место в КТП предмета Информатика
1	2	3	4	5	6
5 класс	1 урок	«Основные правила безопасности в сети»	Рассмотреть преимущества и недостатки интернета, правила поведения в сети.	1) Что такое интернет? 2) Плюсы и минусы интернета 3) Каких правил следует придерживаться в интернете	Раздел «Передача информации», урок «Передача информации»
	2 урок	«Что такое кликбейт и как его избежать?»	Изучить понятие «кликбейт», Научиться определять какой информацией безопасно делиться в интернете, как определять подозрительные сайты и не переходить по подозрительным ссылкам в сети.	1) Что такое кликбейт? 2) Опасный и безопасный кликбейт, различия. 3) Как определять подозрительные сайты и ссылки.	Раздел «Передача информации», урок «Электронная почта»
6 класс	1 урок	«Как безопасно общаться в интернете?»	Научить определять какой информацией безопасно делиться в интернете, как определять мошенников и каких правил придерживаться при общении в сети.	Правила, которым стоит следовать при общении и обмене информацией в интернете	Раздел «Объекты и системы», урок «Персональный компьютер как система»
	2 урок	«Как защититься от фишинга?»	Рассказать учащимся про фишинг в сети и основные его виды. Научить определять вид фишинга и правильно реагировать на мошенничество в сети.	1) Понятие «персональные данные» 2) Что такое фишинг? 3) Виды фишинга 4) Как защитить себя от фишинга в сети?	Раздел «Информация вокруг нас», урок «Как мы познаем окружающий мир»
7 класс	1 урок	«Вирусы на устройствах»	Рассмотреть понятие «компьютерные вирусы», их виды, способы заражения Изучить способы защиты личной информации и устройств	1) Компьютерная программа 2) Компьютерный вирус 3) Вредоносные действия вирусов 4) Признаки заражения устройства вирусом	Раздел «Информация вокруг нас», урок «Компьютерные вирусы и антивирусные программы»

Продолжение таблицы 2

1	2	3	4	5	6
	2 урок	«Конфиденциальность в сети»	Рассмотреть понятие «конфиденциальность» Изучить способы защиты личной информации	1) Классификация компьютерных вирусов 2) Что такое конфиденциальность? 3) Что такое cookie-файлы? 4) Понятие «политика конфиденциальности»	Раздел «Информация и информационные процессы», урок «Сервисы интернет-коммуникаций. Сетевой этикет»
8 класс	1 урок	«Искусственный интеллект»	Рассмотреть понятие «Искусственный интеллект», основные концепции, примеры искусственного интеллекта.	1) Что такое «искусственный интеллект?» 2) Основные концепции 3) Машинное обучение 4) Нейронные сети Зачем нужен искусственный интеллект?	Раздел «Основы алгоритмизации», урок «Понятие алгоритма. Исполнители алгоритмов»
	2 урок	«Информационная безопасность»	Актуализировать пройденный материал: информация, защита информации, фишинг, правила поведения в сети	1) Что такое информация? 2) Защита информации 3) Фишинг 4) Правила поведения в сети	Резервный урок «Обобщение и систематизация знаний и умений по курсу информатики 8 класса»
9 класс	1 урок	«Кибербезопасность»	Рассмотреть понятие «кибербезопасность», угрозы кибербезопасности	1) Что такое кипербезопасность? 2) Угрозы кибербезопасности 3) Правила безопасности в сети	Раздел «Работа в информационном пространстве», урок «Информационная безопасность»
	2 урок	«Криптография»	Рассмотреть понятие «криптография», научиться применять некоторые способы шифрования.	1) Что такое криптография? 2) История развития криптографии 3) Виды шифров 4) Современная криптография	Раздел «Работа в информационном пространстве», урок «Виды деятельности в сети Интернет. Интернет сервисы»

Урок № 1.

Тема урока: Основные правила безопасности в сети.

Класс: 5.

Цели урока: рассмотреть преимущества и недостатки интернета, правила поведения в сети.

Тип урока: урок открытия новых знаний.

Основные понятия: интернет, вред при использовании интернета: кража данных, взлом аккаунтов, вирусная атака, правила поведения в сети.

ЦОРы для урока: для данного урока подготовлена презентация с основными понятиями и правилами, кейсы для работы на уроке (рисунок 2 и 3).

Рисунок 2 – Презентация для 5 класса

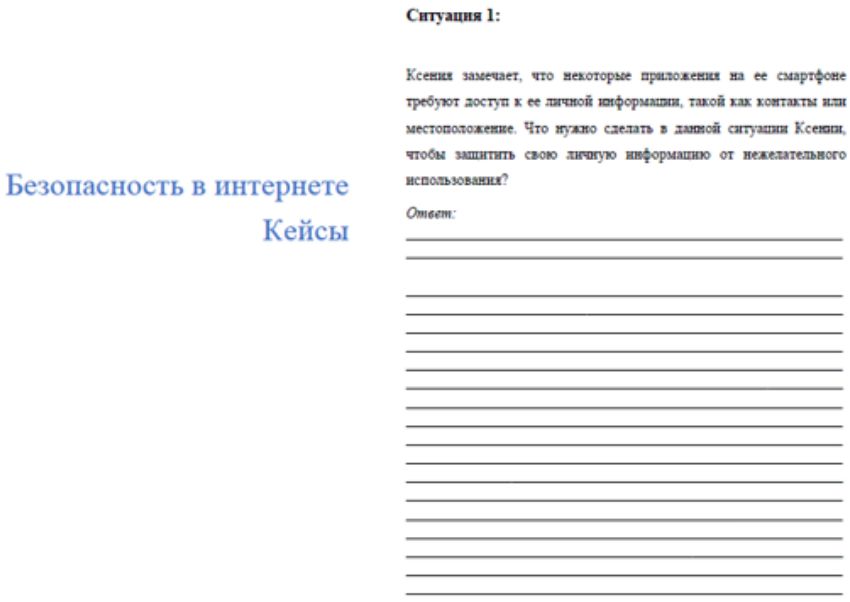


Рисунок 3 – Кейсы для 5 класса

Методические рекомендации к уроку: разработанные материалы можно применять при изучении темы 1 раздела в 5 классе «Информация вокруг нас».

Урок №2.

Тема урока: что такое кликбейт и как его избежать.

Класс: 5.

Цели урока: рассмотреть понятие «кликбейт», научить определять какой информацией безопасно делиться в интернете, как определять подозрительные сайты и не переходить по вредоносным ссылкам в сети.

Тип урока: урок открытия новых знаний.

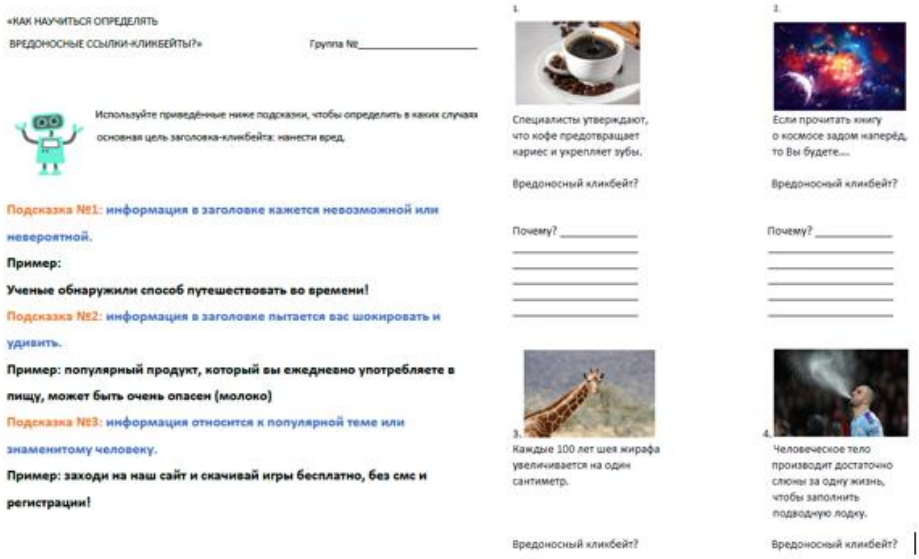
Основные понятия: кликбейт, способы определения заголовков-кликбейтов.

ЦОРы для урока: для данного урока подготовлена презентация с основными понятиями, рабочий лист (рисунок 4 и 5).

Рисунок 4 – Презентация для 5 класса

Методические рекомендации к уроку: В начале занятия можно актуализировать основные правила безопасного поведения в интернете, используя презентацию из предыдущего урока. Далее рассмотреть понятие «кликбейт» и организовать работу в группах или парах с рабочими листами. Обязательно провести этап рефлексии и прослушать ответы каждой группы,

чтобы помочь обучающимся подвести итоги.


«КАК НАУЧИТЬСЯ ОПРЕДЕЛЯТЬ ВРЕДОНОСНЫЕ ССЫЛКИ-КЛИКБЕЙТЫ?»

Группа №_____

Используйте приведённые ниже подсказки, чтобы определить в каких случаях основная цель заголовка-кликбейта: нанести вред.

Подсказка №1: информация в заголовке кажется невозможной или невероятной.

Пример:

Ученые обнаружили способ путешествовать во времени!

Подсказка №2: информация в заголовке пытается вас шокировать и удивить.

Пример: популярный продукт, который вы ежедневно употребляете в пищу, может быть очень опасен (молоко)

Подсказка №3: информация относится к популярной теме или знаменитому человеку.

Пример: заходи на наш сайт и скачивай игры бесплатно, без смс и регистрации!

1. Специалисты утверждают, что кофе предотвращает кариес и укрепляет зубы.

Вредоносный кликбейт?

Почему? _____

2. Если прочитать книгу о космосе задом наперёд, то Вы будете....

Вредоносный кликбейт?

Почему? _____

3. Каждые 100 лет шея жирафа увеличивается на один сантиметр.

Вредоносный кликбейт?

4. Человеческое тело производит достаточно слюны за одну жизнь, чтобы заполнить подводную лодку.

Вредоносный кликбейт?

Рисунок 5 – Рабочий лист

Урок №3.

Тема урока: как безопасно общаться в интернете.

Класс: 6.

Цели урока: научить определять какой информацией безопасно делиться в интернете, как определять мошенников и каких правил придерживаться при общении в сети.

Тип урока: урок открытия новых знаний.

Основные понятия: правила безопасного общения в сети.

ЦОРы для урока: для данного урока подготовлена презентация с правилами, кейсы и тест (рисунок 6 и 7).

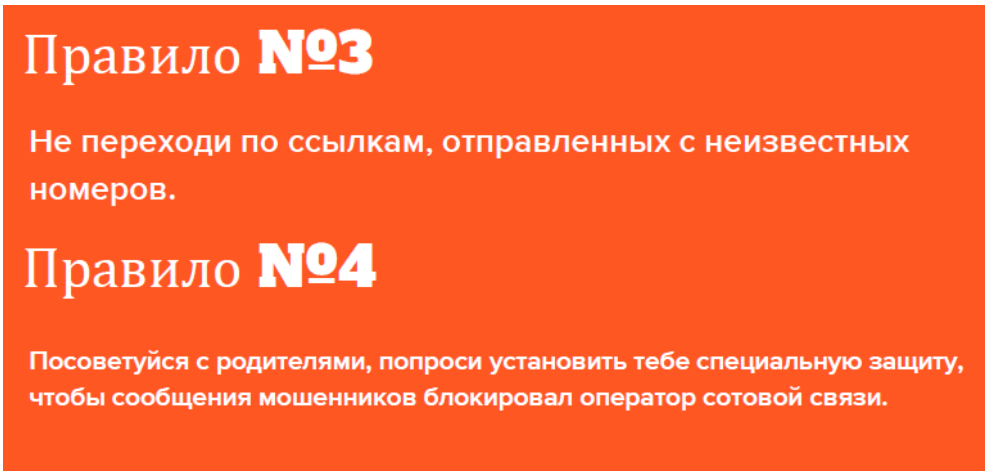


Рисунок 6 – Презентация для 6 класса

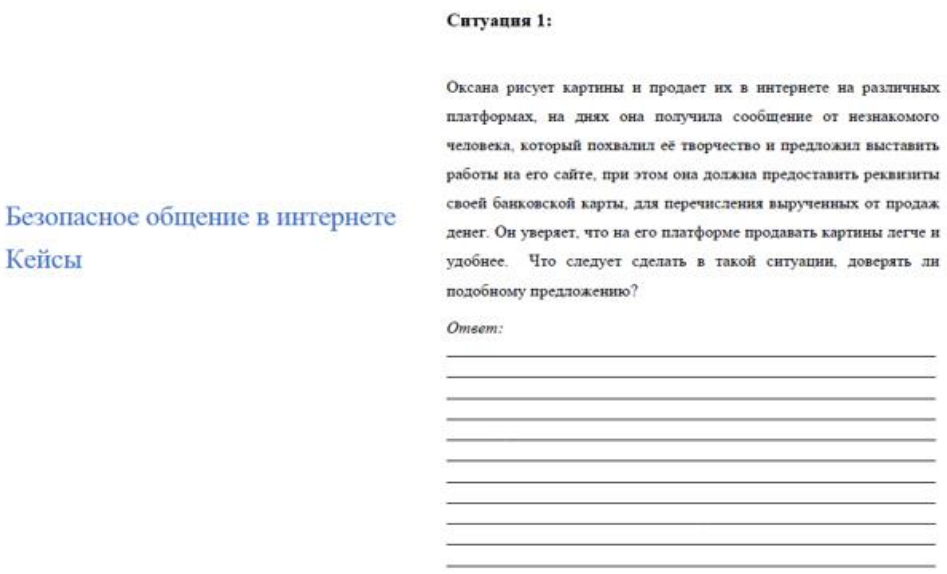


Рисунок 7 – Кейсы для 6 класса

Методические рекомендации к уроку: при работе с презентацией важно проводить активную фронтальную работу в классе, чтобы обучающиеся в процессе обсуждения самостоятельно вывели основные правила. Кейсы предусматривают как индивидуальную, так и групповую работу, с обязательной устной проверкой и обсуждением. Тестирование можно провести на заключительном этапе урока.

Урок № 4.

Тема урока: как защититься от фишинга.

Класс: 6.

Цели урока: рассмотреть понятие «фишинг» в сети и основные его виды. Научиться определять вид фишинга и правильно реагировать на мошенничество в сети.

Тип урока: урок открытия новых знаний.

Основные понятия: личные (персональные) данные, фишинг, распространённые виды фишинга.

ЦОРы для урока: для данного урока подготовлена презентация с основными понятиями, кейсы и тест (рисунок 8 и 9).

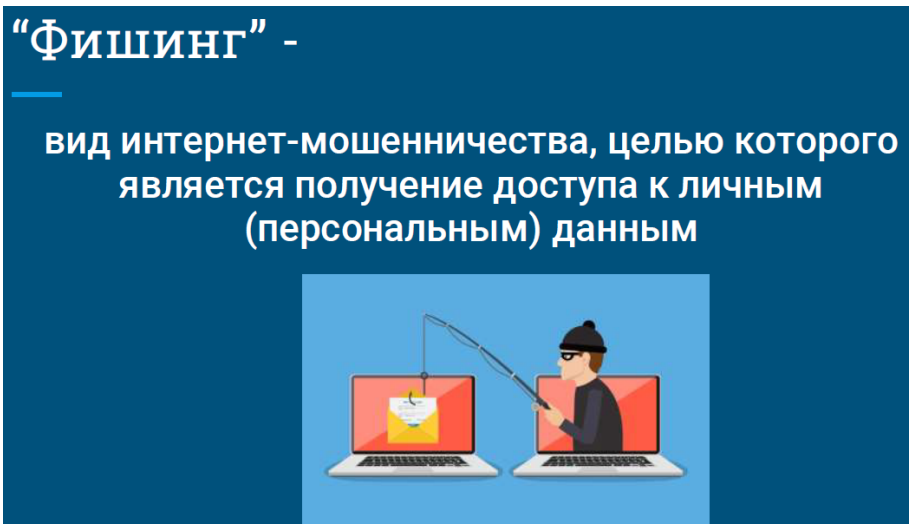


Рисунок 8 – Презентация для 6 класса

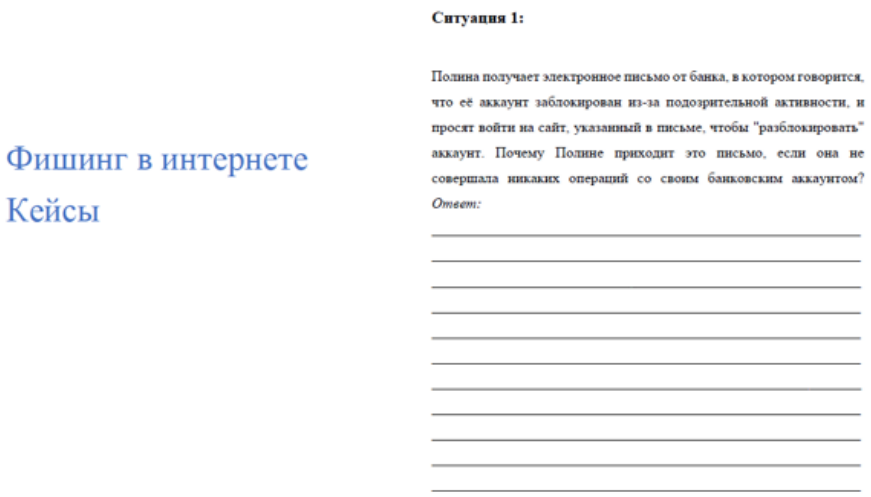


Рисунок 9 – Кейсы для 6 класса

Урок №5.

Тема урока: Компьютерные вирусы.

Класс: 7.

Цели урока: рассмотреть понятие «компьютерные вирусы», их виды, способы заражения. Изучить способы защиты личной информации и устройств.

Тип урока: урок открытия новых знаний.

Основные понятия: компьютерная программа, компьютерный вирус, виды вирусов, вредоносные действия вирусов.

ЦОРы для урока: для данного урока подготовлена презентация, кейсы

с заданиями, практическая работа (рисунок 10 и 11).

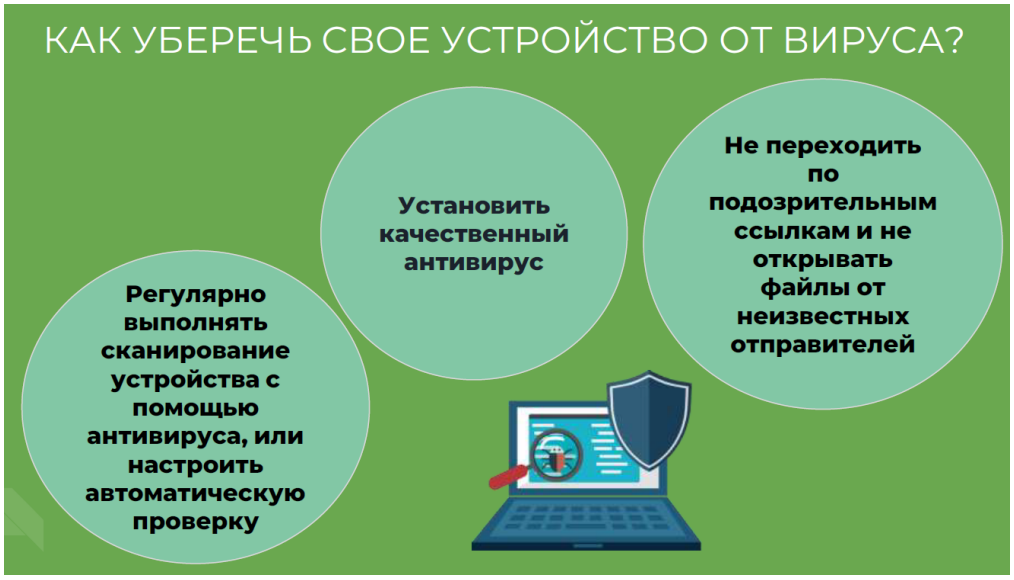


Рисунок 10 – Презентация для 7 класса

Практическая работа «Антивирусная защита»

Цель: изучить технологию тестирования компьютера на наличие вирусов и профилактические меры. Познакомиться со способами лечения зараженных объектов.

1. Проверка установленных на ПК программ

Вирусное ПО часто может устанавливать программы непонятного назначения на компьютер, проверка списка установленных программ и приложений помогает проверить последние установленные программы.

Шаг 1. Сделать щелчок левой кнопкой мыши по пункту «Поиск» (изображение лупы возле кнопки «Пуск») и ввести в строку фразу «Панель управления», после чего перейти в пункт «Панель управления» (рисунок 1).

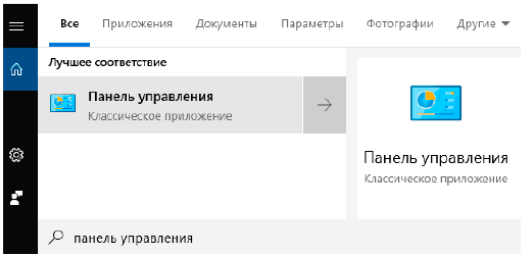


Рисунок 1- панель управления

Шаг 2. В открывшемся окне перейти на вкладку «Удаление программы» (рисунок 2).

Рисунок 11 – Практическая работа «Антивирусная защита» для 7 класса

Методические рекомендации к уроку: при изучении данной темы следует уделить внимание тому, насколько хорошо обучающиеся усвоило материал. В практической работе также дана примерная домашняя работа для закрепления материала.

Урок №6.

Тема урока: Конфиденциальность в сети

Класс: 7.

Цели урока: рассмотреть понятие «конфиденциальность» и способы защиты личной информации.

Тип урока: урок открытия новых знаний.

Основные понятия: конфиденциальность, cookie–файлы, политика конфиденциальности.

ЦОРы для урока: для данного урока подготовлена презентация с основными понятиями, рабочий лист и тест (рисунок 12 и 13).

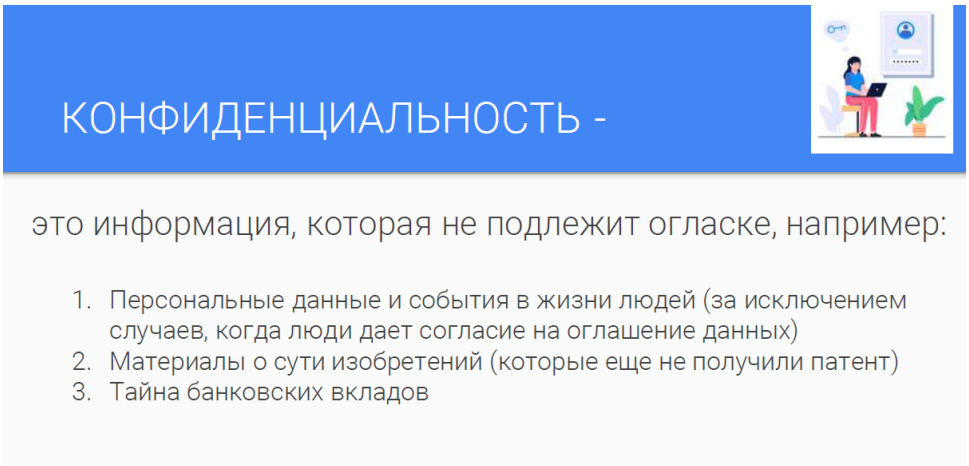


Рисунок 12 – Презентация для 7 класса

Методические рекомендации к уроку: при изучении темы «Конфиденциальность в сети» необходимо актуализировать полученные ранее знания, для этого можно применить презентации или кейсы с различными ситуациями. Данный урок лучше проводить используя активные методы работы, стараясь построить с обучающимися беседу и деятельность в группах. Заключительный этап можно провести, используя тест.

Реклама в сети

Прочитайте приведённый ниже текст и ответьте на вопросы:

Маша гуляла по улице и встретила девушку в кроссовках её любимого бренда. Она и не думала, что эта модель будет выглядеть так красиво в розовом цвете. Вернувшись домой, она зашла в интернет-магазин, но узнав, что модель в этом цвете стоит дорого, решила узнать мнение других и выставила эту модель на своей страничке в социальной сети, устроив опрос «стоит ли покупать?». На следующий день она начала видеть рекламу именно этой модели кроссовок и интернет-магазина, который она посетила. Она замечала, как реклама появляется, когда она набирает текст в поисковой системе, когда заходит на привычные сайты, и просматривает ленту в социальных сетях. Маша решила, что возможно это просто совпадение, но это продолжалось последующие несколько дней, она начала задаваться вопросом: «почему я вижу эти кроссовки повсюду»?

Вопрос №1. Как интересующая Машу модель кроссовок появилась в различных веб-сайтах?

_____

_____

_____

Вопрос №2. Если бы Маша захотела, чтобы её перестала «преследовать» реклама

Рисунок 13 – Рабочий лист для 7 класса

Урок №7.

Тема урока: Искусственный интеллект.

Класс: 8.

Цели урока: рассмотреть понятие «искусственный интеллект», основные концепции, примеры искусственного интеллекта.

Тип урока: урок открытия новых знаний.

Основные понятия:

Искусственный интеллект (ИИ), примеры искусственного интеллекта: голосовые помощники, самоуправляемые автомобили, медицинские системы.

ЦОРы для урока: для данного урока подготовлена презентация и практическая работа (рисунок 14 и 15).

Рисунок 14 – Презентация для 8 класса

Практическая работа на тему: ИИ «Sora»

Sora — это модель искусственного интеллекта, которая может создавать реалистичные и творческие сцены из текстовых инструкций.

1. Перейдите по ссылке: https://openai.com/sora
2. Ознакомьтесь с информацией на главной странице сайта, изучите основные особенности ИИ «Sora», опишите их.

Основные возможности и особенности ИИ «Sora»:

_____

_____

_____

_____

_____

_____

_____

_____

3. Сделайте скриншот понравившегося вам видеоролика, прикрепите его в данный пункт.

Рисунок 15 – Практическая работа для 8 класса

Методические рекомендации к уроку: при изучении данной темы в работе с презентацией важно организовать беседу и фронтальную работу, чтобы обучающиеся смогли определить преимущества и недостатки искусственного интеллекта, на второй половине урока провести практическую работу, в которой учащиеся познакомятся и проанализируют

новую модель искусственного интеллекта «Sora».

Урок №8.

Тема урока: Информационная безопасность.

Класс: 8.

Цели урока: актуализировать пройденный ранее материал.

Тип урока: урок повторения и обобщения материала.

Основные понятия: информация, защита информации, фишинг, правила поведения в сети.

ЦОРы для урока: для данного урока подготовлена викторина, проверяющая знание изученных ранее понятий и умение их применять, кейсы с заданиями по информационной безопасности (рисунок 16 и 17).

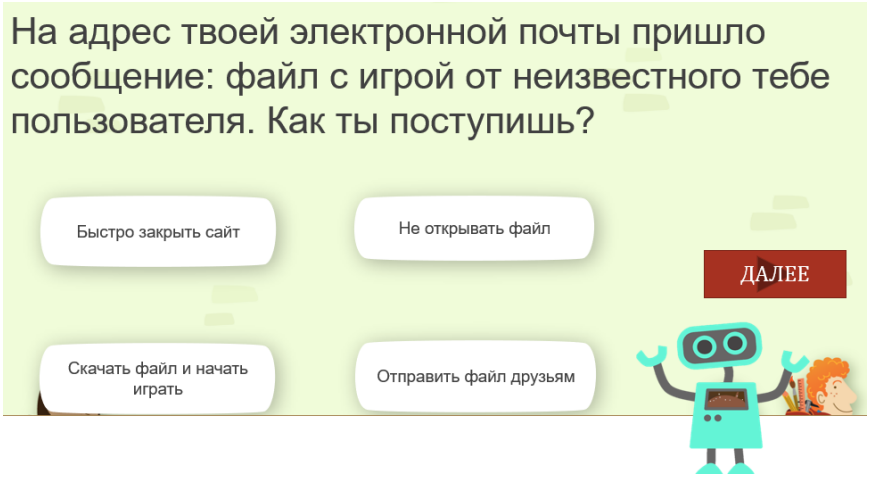
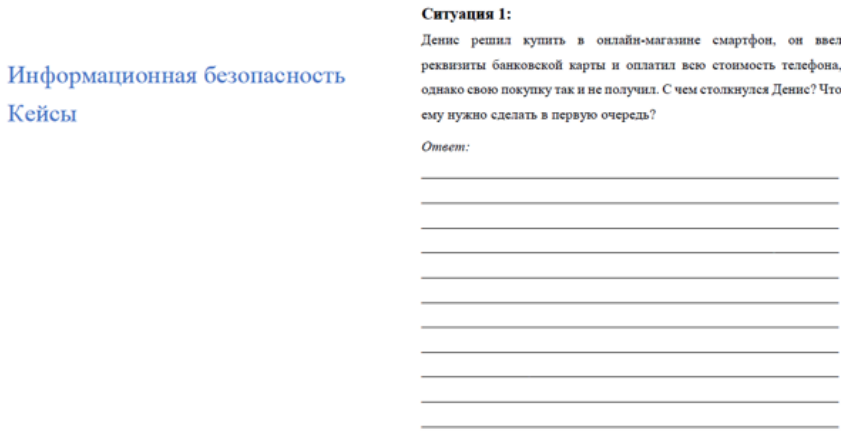


Рисунок 16 – Викторина для 7 класса


Информационная безопасность
Кейсы

Ситуация 1:

Денис решил купить в онлайн-магазине смартфон, он ввел реквизиты банковской карты и оплатил всю стоимость телефона, однако свою покупку так и не получил. С чем столкнулся Денис? Что ему нужно сделать в первую очередь?

Ответ:

Рисунок 17 – Кейсы для 7 класса

Урок №9.

Тема урока: Криптография.

Класс: 9.

Цели урока: рассмотреть понятие «криптография», научиться применять некоторые способы шифрования.

Тип урока: урок открытия новых знаний.

Основные понятия: криптография, история криптографии, шифр, виды шифрования, современная криптография.

ЦОРы для урока: для данного урока подготовлена презентация и практическая работа (рисунок 18 и 19).

Рисунок 18 – Презентация для 9 класса

Методические рекомендации к уроку: при изучении темы уделить внимание фронтальной работе, обучающиеся должны принимать участие в беседе, понять важность криптографии в современном мире. Далее провести практическую работу, часть заданий можно использовать в качестве домашней работы.

1. Имеется таблица замены для двух шифров простой замены: шифра №1 и шифра №2.

Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2		Откр. текст	Шифр 1	Шифр 2
А	В	^		М	Т	№		Ч	М	Σ
Б	И	@		Н	Ц	#		Ш	У	∇
В	О	)		О	.	-		Щ	Д	ϒ
Г	А	+		П	Ж	=		Ъ	Э	ℵ
Д	Щ	<		Р	Г	(		Ы	Н	⊕
Е	П	>		С	Л	?		Ь	Ю	×
Ж	К	∀		Т	Х	%		Э	Ы	⌀
З	Б	♦		У	С	⊗		Ю	Ш	$
И	Ъ	*		Ф	Ь	!		Я	Е	Δ
К	пробел	♥		Х	Ч	№		пробел	Ф	∞
Л	Р	♠		Ц	З	®		.	Я	♣

Расшифруйте сообщения, зашифрованные с помощью шифра №1

- И.РЮУ.ЪФОБГНО
- СЛХГ.ЪЛХО.ФОО.ЩВ

Расшифруйте сообщение, зашифрованное с помощью шифра №2:

∇*!(∞♦№ >*

2. Пусть исходный алфавит содержит следующие символы:

Рисунок 19 – Практическая работа для 9 класса

Урок №10.

Тема урока: Кибербезопасность.

Класс: 9.

Цели урока: рассмотреть понятие «кибербезопасность», угрозы кибербезопасности.

Тип урока: урок открытия новых знаний.

Основные понятия: кибербезопасность, задача кибербезопасности – предотвратить проблемы и обеспечить безопасную работу компаний и пользователей, виды угроз кибербезопасности.

ЦОРы для урока: для данного урока подготовлена презентация и кейсы (рисунок 20 и 21).

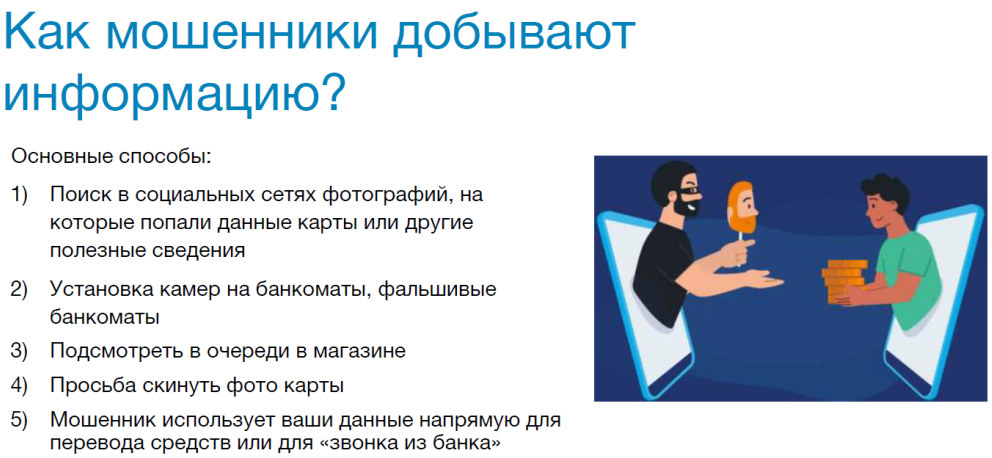


Рисунок 20 – Презентация для 9 класса

Выберите фразу, которую вы можете услышать от настоящего сотрудника банка:

1. Чтобы избежать возможных случаев мошенничества, необходимо осуществить перевод средств на специально защищенный банковский счет или банковскую ячейку. Для доступа к средствам Вам будет предоставлен специальный код.

2. Вам необходимо будет дойти до ближайшего банкомата и выполнить инструкции, которые вам сообщит по телефону наш сотрудник.

3. Пожалуйста, сообщите последние 4 цифры номера карты, которую вы дали мошенникам, чтобы мы могли блокировать ее и предотвратить неправомерные операции.

4. Мы получили заявку на оформление кредита на ваше имя и сейчас необходимо провести несколько проверок для подтверждения информации.

Рисунок 21 – Кейсы для 9 класса

2.2 Техническое и программное обеспечение формирования информационной безопасности обучающихся в образовательном процессе

Для программно-методической поддержки методических разработок была выбрана программа Microsoft Power Point. Power Point – программа, входящая в состав Microsoft.Office, является специализированным средством для создания и оформления презентаций.

Вначале была создана главная страница и кнопка, осуществляющая

переход к меню навигации с материалами, распределёнными по классам (рисунок 22 и 23).

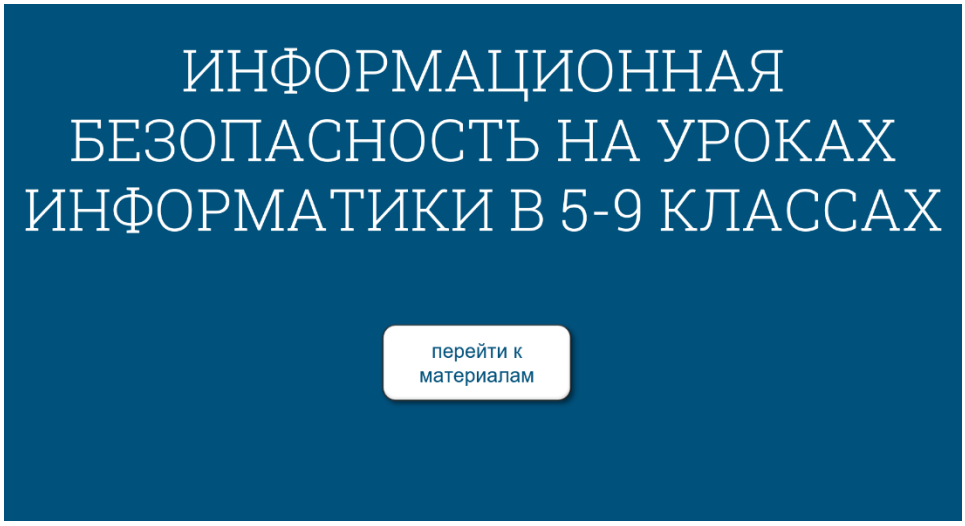


Рисунок 22 – Главная страница

Рисунок 23 – Меню навигации

Далее для каждого класса были добавлены кнопки, по которым осуществляется переход к нужной теме (рисунок 24).

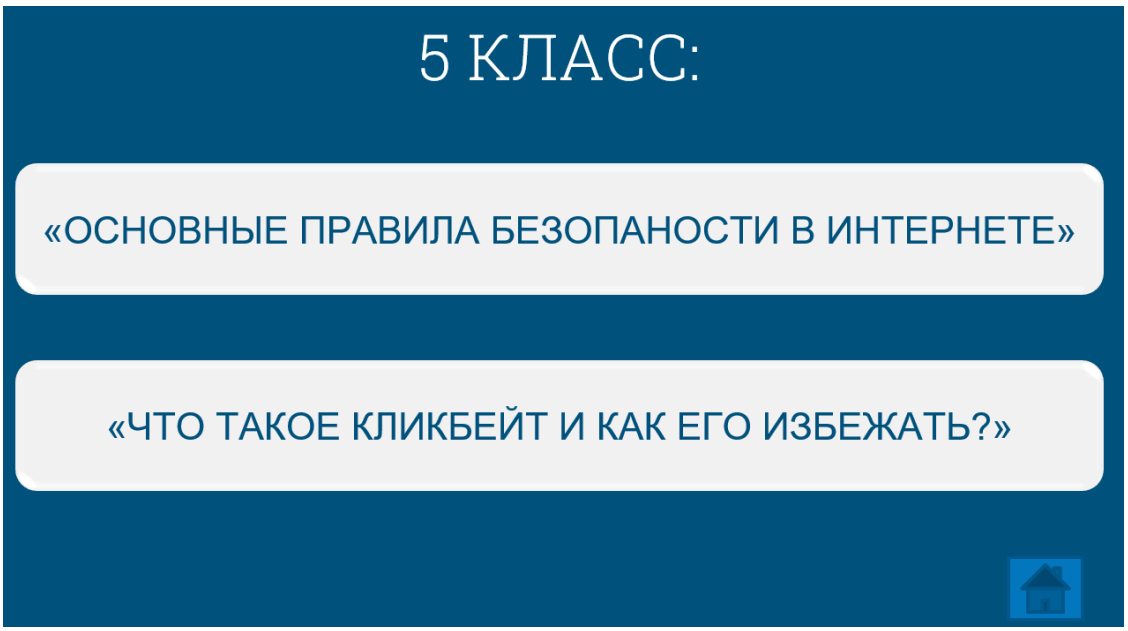


Рисунок 24 – Кнопки для перехода к теме

При переходе по кнопке открываются материалы к уроку, для каждого материала также создана отдельная ссылка (рисунок 25).

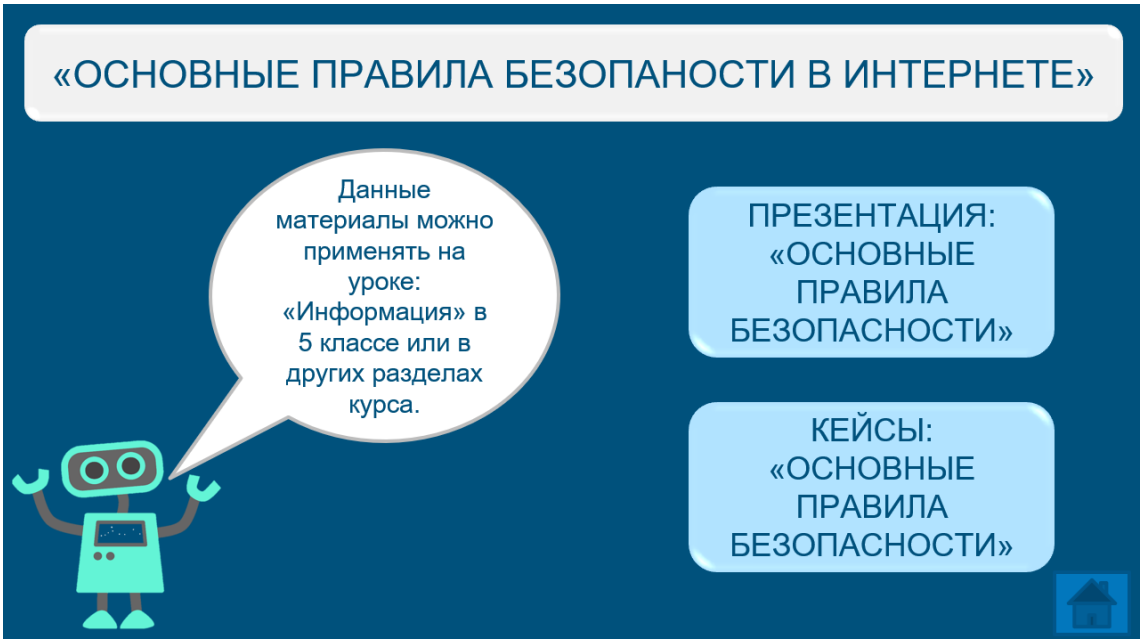


Рисунок 25 – Кнопки для перехода к уроку

Далее, с помощью навигационных кнопок, можно открыть нужный материал (рисунок 26).

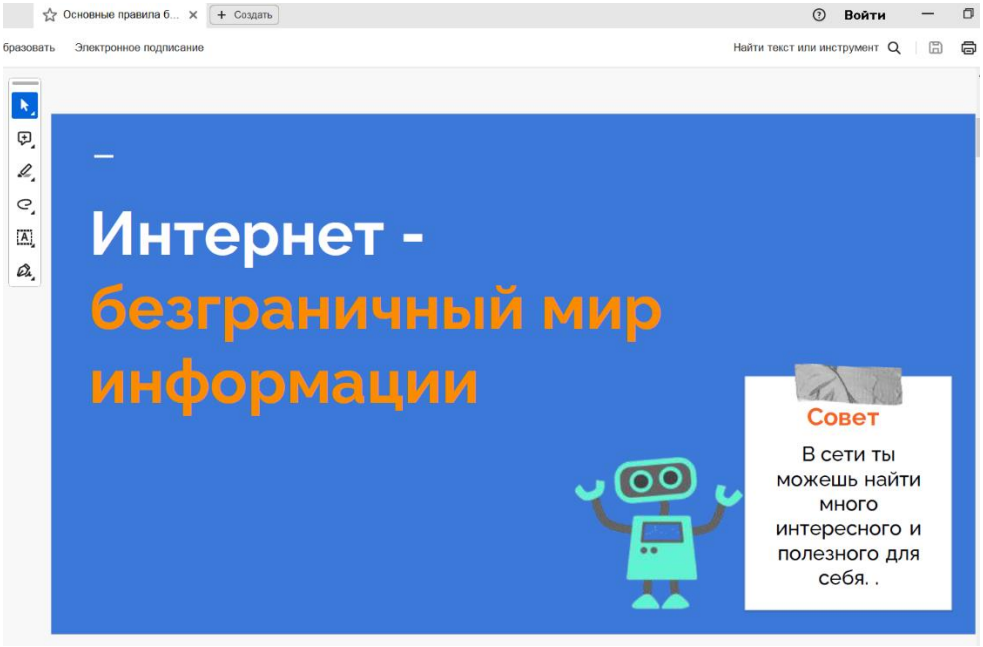


Рисунок 26 – Материалы к уроку при переходе по ссылке

По такому же алгоритму была выстроена навигация и в других классах, например, в разделе 8 класса есть 2 ссылки на уроки «Вирусы на устройствах» и «Искусственный интеллект» (рисунок 27).

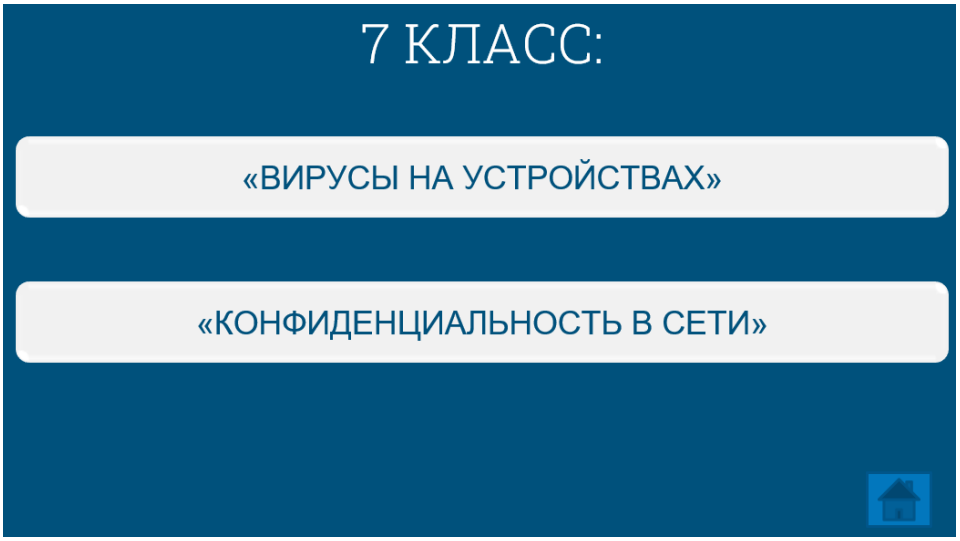


Рисунок 27 – Материалы для 7 класса

Урок на тему «Вирусы на устройствах» содержит 4 материала к занятию, на каждый материал есть отдельная ссылка (рисунок 28).

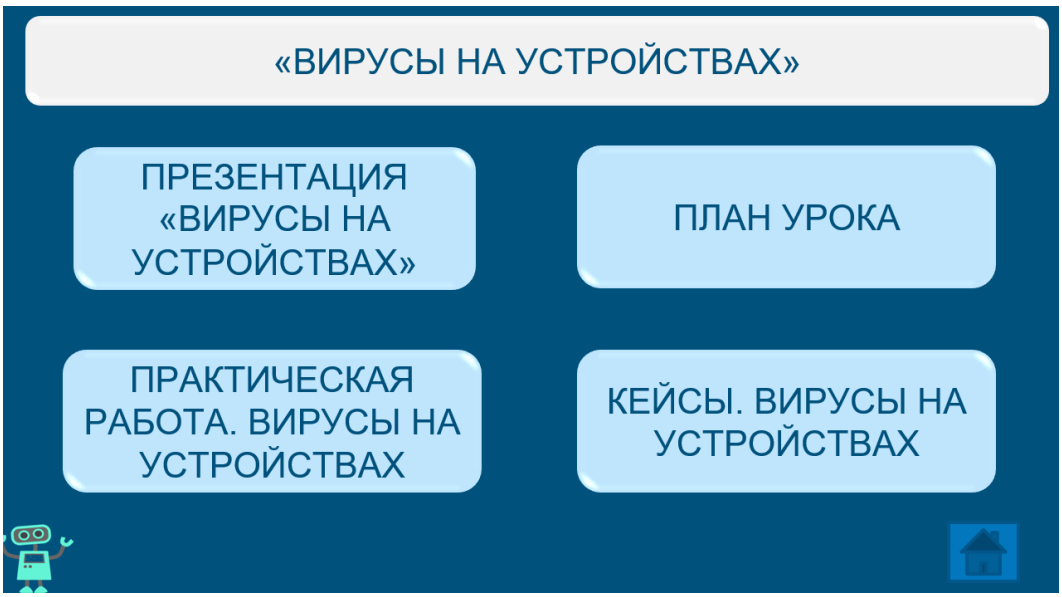


Рисунок 28 – Материалы для 7 класса

Также, в каждый раздел добавлена кнопка, осуществляющая переход на главную страницу, для возможности в любой момент вернуться в меню навигации (рисунок 29).

Рисунок 29 – Кнопка для перехода на главную страницу

2.3 Оценка и анализ эффективности внедрения методов по формированию информационной безопасности обучающихся на уроках информатики в 5-9 классах

Педагогическая апробация была проведена во время педагогической практики в МАОУ СОШ №5 г. Сатка. Тема информационной безопасности впервые изучалась в 5 классах. В течении двух занятий были рассмотрены темы:

1. Урок №1 «Основные правила безопасности в интернете» – 1час.

2. Урок №2 «Что такое кликбейт и как его избежать» – 1час.

В апробации участвовали 28 учащихся 5 класса, была рассмотрена презентация, ребята принимали активное участие в беседе, старались

самостоятельно выводить и предлагать правила, которых нужно придерживаться в сети. Во второй части урока по теме «Основные правила безопасности в интернете» была проведена работа в группах с кейсами. Обучающиеся рассмотрели различные ситуации, предлагали свои варианты, делились историями, касающимися информационной безопасности.

На втором уроке «Что такое кликбейт и как его избежать» вначале были актуализированы правила, рассмотренные на предыдущем уроке. Далее проведена фронтальная работа при определении темы урока. Практическая работа прошла в парах с последующей проверкой и обсуждением ответов.

Выводы по главе 2

Учитывая быстрое развитие угроз в информационной сфере, необходимо также быстро на них реагировать. Именно поэтому важно использовать для обучения школьников ЭОР (электронный образовательный ресурс). Используя технологии, которые позволяют быстро добавлять актуальные материалы для обучения школьников теме «Информационная безопасность», есть возможность своевременно и успешно готовить школьников к появляющимся угрозам.

Также тема «Информационная безопасность» в школе, в которой была пройдена педагогическая практика, была интересна ученикам, потому что вопросы, рассматриваемые в контексте данной темы актуальны на сегодняшний день и полезны в повседневной жизни, обучающиеся с интересом изучали данные темы.

Таким образом, методические материалы и программно-методическая поддержка к ним разработаны и апробированы на учениках.

ЗАКЛЮЧЕНИЕ

Подводя итоги данной работы, хотелось бы отметить, что проведенное исследование направлено на улучшение изучения темы информационной безопасности. Актуальность исследования обусловлена тем, что в условиях постоянного развития информационных технологий информационная безопасность имеет особое место в школьном курсе «Информатика».

В итоге работы были достигнуты цели и разработаны методические материалы по теме «Информационная безопасность», которые можно применять на уроках информатики.

В процессе исследования были выполнены следующие задачи:

1. Изучены теоретические основы по теме «Информационная безопасность».

2. Проведен анализ изложения темы в учебных комплексах и учебно-методической литературе.

3. Создана методическая разработка по теме «Информационная безопасность».

4. Выполнена оценка и анализ эффективности внедрения методов по формированию информационной безопасности.

В подтверждении гипотезы можно сказать, что разработанные методические материалы помогут своевременно и в краткие сроки доводить до учеников актуальную информацию, связанную с информационной безопасностью.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Амелин Р. В. Информационная безопасность. Конспект лекций / Амелин Р.В. // Лаборатория преподавателя. – 2017. – URL: https://rv-lab.ru (дата обращения: 10.03.2024).

2. Андреева Е.В. Математические основы информатики. Элективный курс: учебное пособие / Е.В. Андреева, Л.Л. Босова, И.Н.Фалина. – Москва : БИНОМ. Лаборатория знаний, 2005. – 328 с. – ISBN 5-94774-139-3.

3. Анин Б.Ю. Защита компьютерной информации / Б.Ю. Анин. – Санкт-Петербург : «BHVСанкт-Петербург», 2000. – 384 с. – ISBN 5-8206-0104-1.

4. Артемов А.В. Информационная безопасность: курс лекций / А.В. Артемов. – Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. – 256 с.

5. Босова Л.Л. Информатика. 9 класс. Базовый уровень: учебник / Л.Л. Босова, А.Ю. Босова. – 5-е изд., перераб. – Москва : Просвещение, 2023. – 248 с. – ISBN: 978-5-09-102544-6.

6. Ванина А.Г. Персональная кибербезопасность: учебное пособие (курс лекций) / А.Г. Ванина, Д.В. Орёл, С.В. Аникуев. – Ставрополь : Северо-Кавказский федеральный университет, 2022. – 137 с. – EDN FMIQOQ.

7. Галатенко В.А. Стандарты информационной безопасности / В.А. Галатенко. – 2-е изд. – Москва : ИНТУИТ, 2016. – 307 с. – ISBN 5-9556-0053-1.

8. Гейн А.Г. Информатика и информационные технологии. 9 класс: учеб. для общеобразоват. учреждений / А.Г. Гейн, Н.А. Юнерман. – Москва : Просвещение, 2014. – 110 с. – ISBN 978-5-09-085125-1.

9. Горбенко А.О. Основы информационной безопасности (введение в профессию): учебное пособие / А.О. Горбенко. – Санкт-

Петербург : Интермедия, 2017. – 335 с. – ISBN 978-5-4383-0136-3.

10. Киренберг А.Г. Информационная безопасность современных операционных систем: учебное пособие / А.Г. Киренберг. – Кемерово : Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. – 138 с. – ISBN 978-5-00137-320-9.

11. Лапчик М.П. Методика преподавания информатики: учеб. пособие для студ. пед. вузов / М.П. Лапчик, И.Г. Семакин Е.К.Хеннер; Под общей ред. М. П. Лапчика. – Москва : Издательский центр «Академия», 2001. – 624 с. – ISBN 5-7695-0825-6.

12. Малых Т.А. Педагогические аспекты информационной безопасности / Т.А. Малых // Народное образование. – 2007. – № 5. – С. 231 – 236.

13. Мифтахова Л.Х. Программно-аппаратные средства защиты информации: учебное пособие для студентов вузов по направлению подготовки «Информационная безопасность» / А.Р. Касимова, В.Н.Красильников, Л.Х. Мифтахова; под редакцией В. К. Головати. – Санкт-Петербург : Интермедия, 2018. – 408 с. – ISBN 978-5-4383-0157-8.

14. Петров С.В. Информационная безопасность: учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. – Москва : АРТА, 2016. – 296 с. – ISBN 978-5-93196-814-8.

15. Поляков К.Ю. Информатика. 7 класс: учеб. для общеобразоват. учреждений / К.Ю. Поляков, Е.А. Еремин. – Москва : БИНОМ. Лаборатория знаний, 2017. – 36 с. – ISBN 978-5-09-081131-6.

16. Прохорова О.В. Информационная безопасность и защита информации: учебник / О.В. Прохорова. – 3-е изд. – Санкт-Петербург : Лань, 2021. – 124 с. – ISBN 978-5-8114-7970-2.

17. Семененко В.А. Информационная безопасность: учебное пособие / В.А. Семененко. – Москва : МГИУ, 2017. – 277 с. – ISBN 978-5-276-00641-3.

18. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учебное пособие / Ю.Н.Сычев. – Москва : ИНФРА-М, 2023. – 223 с. – ISBN 978-5-16-014397-2.

19. Фомин Д.В. Информационная безопасность: учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения / Д.В.Фомин. – Саратов : Вузовское образование, 2018. – 54 с. – ISBN 978-5-4487-0298-3.

20. Шаньгин В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. – Москва : ИНФРА-М, 2017. – 416 с. – ISBN 978-5-16-003132-3.

ПРИЛОЖЕНИЕ 1

Разработка урока по теме «Что такое кликбейт?»

Класс: 5

Цель урока: научиться определять какой информацией безопасно делиться в интернете, как определять подозрительные сайты и не переходить по подозрительным ссылкам в сети.

Тип урока: Урок открытия новых знаний

Формы работы: Фронтальная, индивидуальная, работа в парах и группах.

Планируемые результаты:

предметные: учиться правилам безопасного общения в интернете

личностные: уметь осуществлять самооценку на основе критерия успешности деятельности;

регулятивные: определять и формулировать тему и цель урока;

коммуникативные: формулировать свои мысли в устной и письменной форме; организовывать и планировать учебное сотрудничество с одноклассниками;

познавательные: ориентироваться в своей системе знаний (отличать новое от известного).

Технологическая карта урока

Этапы урока	Обучающие и развивающие компоненты, задания и упражнения	Деятельность учителя	Деятельность учащихся	Время (в минутах)	Формируемые умения (универсальные учебные действия)
1	2	3	4	5	6
1. Организационный этап	Создать благоприятный настрой на работу	Приветствие обучающихся, проверка подготовленности к учебному занятию, проверка присутствующих.	Включаются в учебный процесс	1 мин.	Организация своей учебной деятельности;

2. Актуализация знаний	Актуализация опорных знаний и способов действий.	Напомнить ученикам основные правила безопасности в сети *(В качестве актуализации можно использовать презентацию «Основные правила поведения в сети» (см.приложение 1), чтобы повторить материал прошлого урока.*	Вспоминают правила безопасности в сети, работают с кейсами в группах	12 мин.	Наблюдение, внимательность, умение осознанно и произвольно строить речевое высказывание в устной форме.
3. Целеполагание, постановка проблемы	Поиск и анализ причины затруднения	Открывает слайд №1 и задаёт ученикам вопрос: - подумайте, на какой из этих заголовков вы бы кликнули первым? Почему? -Давайте проголосуем, чтобы увидеть, на какой заголовок большинство кликнуло бы первым. Я читаю по-порядку каждый заголовок, а вы выбираете и поднимаете руку. Далее идет подсчет количества голосов по	У*чащиеся изучают примеры со слайда, анализируют информацию и отвечают на вопрос учителя устно (голосуют)*	4 мин.	Умение осознанно и произвольно строить речевое высказывание в устной форме Анализирование информации, внимательность, Выдвижение гипотезы.

		каждому пункту. Учитель подводит итог, задавая вопрос: «Почему вы выбрали именно этот заголовок? Что привлекло ваше внимание?» Предлагает учащимся рассказать, почему они выбрали интересующий пункт.	- *отвечают на вопрос учителя устно*		
4. Постановка цели и задач урока	Обеспечение мотивации обучения детьми, формулирование ими темы и целей урока.	Учитель, подводит учеников к выводу, говоря о том, что каждый выбрал пункт в соответствие со своим интересом. Выводит на экран «слайд №2», открывая тему урока.	*Слушают учителя, записывают тему урока*	2 мин.	Умение осознанно и произвольно строить речевое высказывание в устной форме. Самоопределение. Умение вступать в диалог, участвовать в коллективном обсуждении вопроса
5. Изучение нового материала и усвоение новых знаний	Обеспечение восприятия, осмысления и первичного запоминания детьми изучаемой темы	Далее учитель знакомит класс с понятием «кликбейт», вначале предложив ученикам попробовать ответить на этот вопрос самостоятельно и предложить свои варианты определений,	- *Учащиеся отвечают на вопрос учителя, участвуют в беседе* - *Учащиеся подводят итог,*	10 мин.	Развитие самостоятельности, умения слушать и слышать. Развитие навыка участия в коллективном обсуждении тем. Познавательная активность. Формирование умения выделять и сравнивать стратегии решения задач.

		после беседы рассмотреть понятие, используя для этого 3 и 4 слайды. *Важно подвести учеников к пониманию, что есть кликбейты, привлекающие внимание, но не приносящие вред, а есть вредоносные ссылки-кликбейты.* - заголовки-кликбейты на сайтах, побуждают вас перейти по ссылке и тем самым: потенциально ведут на сайты, на которые вы не хотели заходить. Сайты, в которые ведут кликбейты как правило опасны, они могут заразить ваше устройство компьютерными вирусами или привести к тому, что кто-то украдет вашу информацию. Итак, если вы встретите заголовок, который, по	*выводят правило* *предлагают свои варианты, приходят к выводу*		

		вашему мнению, может быть кликбейтом, не нажимайте на него. Вместо этого выполните поиск по заголовку, чтобы узнать, есть ли другие источники, предоставляющие искомую информацию.			
6. Применение знаний и умений в новой ситуации	Выявление пробелов первичного осмысления изученного материала, обеспечение закрепления знаний и способов действий, которые необходимы для самостоятельной работы по новому материалу.	Организация и контроль за процессом выполнения заданий. Учитель делит учеников на группы для выполнений заданий в рабочих листах *По итогам работы учащиеся должны научиться определять разницу между просто рекламными заголовками и вредоносным кликбейтом.*	*Задание в рабочих листах (приложение 3)* *-ученики применяют правила*	4 мин	Уметь оформлять свои мысли в устной форме; слушать и понимать речь других. умение строить речевое высказывание в устной и письменной форме. выбор наиболее эффективных способов задач в зависимости от конкретных условий.
7.Первичное осмысление и закрепление знаний	Дать качественную оценку работы класса и отдельных обучаемых.	Учитель дает учащимся три минуты, чтобы написать собственный кликбейтный	*Учащиеся работают самостоятельно,*	5 мин	Формирование позитивной самооценки умение самостоятельно адекватно

		заголовок и одно предложение, объясняющее, почему это кликбейт. Далее учитель просит прочитать свои ответы учащихся (по желанию) и собирает письменные ответы у всех, чтобы оценить понимание темы.	*обсуждают свои ответы*		анализировать правильность выполнения действий и вносить необходимые коррективы.
8. Рефлексия учебной деятельности на уроке.	Дать количественную оценку работы учащихся	Подводит итоги класса. Ребята оцените свою работу на уроке и продолжите фразу. Было интересно…. Какое открытие мы сегодня сделали…. Как нам удалось открыть правила… Что понравилось на уроке… В чём затруднение	*Ученики отвечают на вопросы учителя*	2 мин.	Оценивание собственной деятельности на уроке, проверка усвоенных на уроке знаний.
9. Информация о домашнем задании	Обеспечение понимания детьми содержания и способов выполнения домашнего задания	Дает комментарий к домашнему заданию	*Записывают в дневники задание, задают вопросы по дом.заданию.*	3 мин.	

Разработка урока по теме «Как безопасно общаться в интернете»

Класс: 6

Цель урока: научиться определять какой информацией безопасно делиться в интернете, как определять мошенников и каких правил придерживаться при общении в сети.

Тип урока: Урок открытия новых знаний.

Формы работы: Фронтальная, индивидуальная, работа в парах и группах.

Планируемые результаты:

предметные: учиться правилам безопасного общения в интернете

личностные: уметь осуществлять самооценку на основе критерия успешности деятельности;

регулятивные: определять и формулировать тему и цель урока;

коммуникативные: формулировать свои мысли в устной и письменной форме; организовывать и планировать учебное сотрудничество с одноклассниками;

познавательные: ориентироваться в своей системе знаний (отличать новое от известного).

Технологическая карта урока

Этапы урока	Обучающие и развивающие компоненты, задания и упражнения	Деятельность учителя	Деятельность учащихся	Время (в минутах)	Формируемые умения (универсальные учебные действия)
1	2	3	4	5	6
1.Организационный этап	Создать благоприятный настрой на работу	Приветствие ·обучающихся, проверка подготов-ленности к учебному занятию, проверка присутствующих.	Включаются в учебный процесс	1 мин.	Организация своей учебной деятельности;

2. Актуализация знаний	Актуализация опорных знаний и способов действий.	Напомнить ученикам основные правила безопасности в сети	Вспоминают правила безопасности в сети	4 мин.	Наблюдение, внимательность, умение осознанно и произвольно строить речевое высказывание в устной форме.
3. Целеполагание, постановка проблемы	Поиск и анализ причины затруднения	-Ребята, какие приложения вы используете для общения в интернете? -подводит итог самого популярного приложения -Сегодня мы с вами поговорим о том, каких правил следует придерживаться при общении в интернете, независимо от социальной сети и мессенджера - тема нашего урока «Как безопасно общаться в интернете»	-Устная работа, ученики предлагают свои варианты, анализируют, какое приложение наиболее популярно - записывают тему урока.	4 мин.	Умение осознанно и произвольно строить речевое высказывание в устной форме Анализирова-ние информации, внимательность, Выдвижение гипотезы.
4. **Постановка цели и**	Обеспечение мотивации обучения детьми,	Мотивирует учащихся, вместе с ними		2 мин.	Умение осознанно и произвольно строить

задач урока	формулирование ими темы и целей урока.	определяет цель урока; акцентирует внимание обучающихся на значимости темы.			речевое высказывание в устной форме. самоопределение. умение вступать в диалог, участвовать в коллективном обсуждении вопроса
5. **Изучение нового материала и усвоение новых знаний**	Обеспечение восприятия, осмысления и первичного запоминания детьми изучаемой темы	-Ребята, предлагаю ознакомиться с несколькими диалогами из социальных сетей и попробовать найти в них проблему. Знакомит с первым диалогом (слайд 1) - как бы вы отреагировали на подобное сообщение? Давайте порассуждаем -а что, если бы сообщение пришло от знакомого вам человека, но с другого аккаунта?	*- учащиеся читают и анализируют предложенные диалоги* *- учащиеся отвечают на вопрос учителя, участвуют в беседе* *- учащиеся отвечают на вопрос учителя, участвуют в беседе* *- учащиеся подводят итог, выводят правило*	10 мин.	Развитие самостоятельности, умения слушать и слышать. Развитие навыка участия в коллективном обсуждении тем. Познавательная активность. Формирование умения выделять и сравнивать стратегии решения задач.

		Давайте подведем итог по первой ситуации и попробуем вывести правило. Открывает слайд 2 (правило) Включает слайд №3 Второй диалог - Что здесь не так? -Верно! Что следует сделать в таком случае? -Ребята, действительно, в таком случае лучше заблокировать абонента и не вступать с ним в	- *учащиеся читают и анализируют второй диалог* - *Сообщение пришло с одного номера, а вернуть деньги просят на другой* - учащиеся предлагают свои варианты и вместе приходят к выводу - *учащиеся подводят итог, выводят правило*		

		диалог. Самое главное – быть внимательным и не торопиться в принятии решений. Например, если не обратить внимание что деньги просят вернуть на другой номер, можно попасться на уловку. Открывает слайд 3 (правило) Включает слайд №4 Третий диалог -Какие возможные исходы есть в данной ситуации? - открывает слайд №5, в котором перечислены действия, которые следует предпринять в подобной ситуации	- *учащиеся предлагают свои варианты (при переходе по ссылке на устройство может установится вирус Деньги могут уйти мошенникам и тд.)* -приходят к выводу - *учащиеся читают и анализируют информацию* - *учащиеся предлагают свои варианты, приходят к выводу*		

		Включает слайд №5 Ситуация 4 -Как вы думаете, почему Маша отказалась делать перевод? Как бы поступили вы? Открывает слайд 6 (правило)			
6. Применение знаний и умений в новой ситуации	Выявление пробелов первичного осмысления изученного материала, обеспечение закрепления знаний и способов действий, которые необходимы для самостоятельной работы по новому материалу.	Организация и контроль за процессом выполнения заданий.	Работа в группах с карточками (приложение 2) -ученики читают ситуацию и применяют правила	4 мин	уметь оформлять свои мысли в устной форме; слушать и понимать речь других. умение строить речевое высказывание в устной и письменной форме. выбор наиболее эффективных способов задач в зависимости от конкретных условий.
7.Первичное осмысление и закрепление знаний	Дать качественную оценку работы класса и отдельных обучаемых.	Выявляет качество и уровень усвоения знаний, а также устанавливает причины выявленных ошибок.	Учащиеся работают в парах с последующей взаимопровер ой, анализируют свою работу, выражают вслух свои	5 мин	Формирование позитивной самооценки умение самостоятельно адекватно анализировать правильность выполнения действий и

			затруднения и обсуждают правильность решения заданий		вносить необходимые коррективы.
8. Рефлексия учебной деятельности на уроке.	Дать количественную оценку работы учащихся	Подводит итоги класса. Ребята оцените свою работу на уроке и продолжите фразу. Было интересно…. Какое открытие мы сегодня сделали…. Как нам удалось открыть правила… Что понравилось на уроке… В чём затруднение	*-ученики отвечают на вопросы учителя*	4 мин.	Оценивание собственной деятельности на уроке, проверка усвоенных на уроке знаний.
9. Информация о домашнем задании	Обеспечение понимания детьми содержания и способов выполнения домашнего задания	Дает комментарий к домашнему заданию	Учащиеся записывают в дневники задание, задают вопросы по дом.заданию.	3 мин.	

Разработка урока по теме «Как защититься от фишинга»

Класс: 6

Цель урока: изучить понятие «фишинг» и основные его виды, научиться определять вид фишинга и правильно реагировать на мошенничество в сети

Тип урока: Урок открытия новых знаний

Формы работы: Фронтальная, индивидуальная, работа в парах и группах.

Планируемые результаты:

предметные: учиться правилам безопасного общения в интернете

личностные: уметь осуществлять самооценку на основе критерия успешности деятельности;

регулятивные: определять и формулировать тему и цель урока;

коммуникативные: формулировать свои мысли в устной и письменной форме;

организовывать и планировать учебное сотрудничество с одноклассниками;

познавательные: ориентироваться в своей системе знаний (отличать новое от известного).

Формы работы: Фронтальная, индивидуальная, работа в парах и группах.

Технологическая карта урока

Этапы урока	Обучающие и развивающие компоненты, задания и упражнения	Деятельность учителя	Деятель-ность учащихся	Время (в минутах)	Формируемые умения (универсальные учебные действия)
1	2	3	4	5	6
1.Организационный этап	Создать благоприятный настрой на работу	Приветствие·обучающихся, проверка подготовленности к учебному занятию,	Включаются в учебный процесс	1 мин.	Организация своей учебной деятельности;

		проверка присутствующих			
2. Актуализация знаний	Актуализация опорных знаний и способов действий.	Напомнить ученикам основные правила безопасности в сети	Вспоминают правила безопасности в сети	4 мин.	Наблюдение, внимательность, умение осознанно и произвольно строить речевое высказывание в устной форме.
3. Целеполагание, постановка проблемы	Поиск и анализ причины затруднения	-Ребята, давайте сейчас поразмышляем над следующим вопросом (слайд 1) -слушает ответы учеников -итак, сейчас мы услышали самые разные ответы (телефон, одежда, карточка и т.д), все это вещи, но никто не назвал -есть еще варианты? - ребята, на самом деле, украсть могут не только предмет, если мы говорим про интернет, значит украсть могут и ваши личные данные. - в сети есть люди, которые могут использовать ваши данные в самых различных целях, и сегодня мы с вами	-Устная работа, ученики анализируют вопрос, предлагают свои варианты ответов -*личные вещи: телефон, карточка и тд.* предлагают другие варианты	4 мин.	Умение осознанно и произвольно строить речевое высказывание в устной форме Анализирование информации, внимательность, Выдвижение гипотезы.

		поговорим об этом виде мошенничества.			
4. **Постановка цели и задач урока**	Обеспечение мотивации обучения детьми, формулирование ими темы и целей урока.	Мотивирует учащихся, вместе с ними определяет цель урока; акцентирует внимание обучающихся на значимости темы.		2 мин.	Умение осознанно и произвольно строить речевое высказывание в устной форме. самоопределение. умение вступать в диалог, участвовать в коллективном обсуждении вопроса
5. **Изучение нового материала и усвоение новых знаний**	Обеспечение восприятия, осмысления и первичного запоминания детьми изучаемой темы	-что такое «личные данные», как вы понимаете это выражение? Слушает ответы, подводит итог с помощью слайда 2 -итак, мы разобрались с понятием «личные данные», но как вы думаете зачем мошенникам в интернете нужны наши данные, где они могут их использовать? - верно, вариантов использования личной информации другого человека много	*Ученики отвечают на вопрос, предлагают свои варианты* *Ученики отвечают на вопрос, предлагают свои варианты (создать фейковый профиль, украсть деньги с карты и тд)*	10 мин.	Развитие самостоятельности, умения слушать и слышать. Развитие навыка участия в коллективном обсуждении тем. Познавательная активность. Формирование умения выделять и сравнивать стратегии решения задач.

		- данный вид мошенничества имеет свое название «фишинг», давайте остановимся на нем подробнее -Далее рассмотрим распространенные на сегодняшний день виды фишинга учитель продолжает рассказывать о видах фишинга, используя для работы презентацию	*Работают со слайдами 3 и 4, записывают определение и примеры* *Слушают учителя, принимают участие в беседе, приводят свои примеры записывают определения*		
6. Применение знаний и умений в новой ситуации	Выявление пробелов первичного осмысления изученного материала, обеспечение закрепления знаний и способов действий, которые необходимы для самостоятельной работы по новому материалу.	Организация и контроль за процессом выполнения заданий.	Работа в группах с карточками (приложение 2) -ученики читают ситуацию и применяют правила	4 мин	Уметь оформлять свои мысли в устной форме; слушать и понимать речь других. умение строить речевое высказывание в устной и письменной форме. выбор наиболее эффективных способов задач в зависимости от конкретных условий.
7.Первичное осмысление и	Дать качественную	Выявляет качество и	Учащиеся работают в	5 мин	Формирова-ние

закрепление знаний	оценку работы класса и отдельных обучаемых.	уровень усвоения знаний, а также устанавливает причины выявленных ошибок.	парах с последующей взаимопроверкой, анализируют свою работу, выражают вслух свои затруднения и обсуждают правильность решения заданий (тест, приложение 3)		позитивной самооценки умение самостоятельно адекватно анализировать правильность выполнения действий и вносить необходимые коррективы.
8. Рефлексия учебной деятельности на уроке.	Дать количественную оценку работы учащихся	Подводит итоги класса. Ребята оцените свою работу на уроке и продолжите фразу. Было интересно…. Какое открытие мы сегодня сделали…. Как нам удалось открыть правила… Что понравилось на уроке… В чём затруднение…	*-ученики отвечают на вопросы учителя*	4 мин.	Оценивание собственной деятельности на уроке, проверка усвоенных на уроке знаний.
9. Информация о домашнем задании	Обеспечение понимания детьми содержания и способов выполнения домашнего задания	Дает комментарий к домашнему заданию	Учащиеся записывают в дневники задание, задают вопросы по дом.заданию.	3 мин.	

Разработка урока по теме «Конфиденциальность в сети»

Класс: 7

Цель урока: изучить понятие «конфиденциальность», изучить способы защиты личной информации

Тип урока: Урок открытия новых знаний

Формы работы: Фронтальная, индивидуальная, работа в парах и группах.

Планируемые результаты:

предметные: учиться правилам безопасного общения в интернете

личностные: уметь осуществлять самооценку на основе критерия успешности деятельности;

регулятивные: определять и формулировать тему и цель урока;

коммуникативные: формулировать свои мысли в устной и письменной форме;

организовывать и планировать учебное сотрудничество с одноклассниками;

познавательные: ориентироваться в своей системе знаний (отличать новое от известного).

Технологическая карта урока

Этапы урока	Обучающие и развивающие компоненты, задания и упражнения	Деятельность учителя	Деятельность учащихся	Время (в минутах)	Формируемые умения (универсальные учебные действия)
1	2	3	4	5	6
1. Организац-ионный этап	Создать благоприятный настрой на работу	Приветствие· обучающихся, проверка подготовленности к учебному занятию, проверка присутствующих.	Включаются в учебный процесс	1 мин.	Организация своей учебной деятельности;
2. Актуализация знаний	Актуализация опорных знаний и	Напомнить ученикам	Вспоминают правила	4 мин.	Наблюдение, внимательность, умение

	способов действий.	основные правила безопасности в сети	безопасности в сети		осознанно и произвольно строить речевое высказывание в устной форме.
3. Целеполагание, постановка проблемы	Поиск и анализ причины затруднения	-Ребята, давайте попробуем ответить на вопрос (слайд 1) слушает ответы учеников -*Можете ли вы привести примеры, когда люди хотели бы сохранить в тайне — либо от всех, либо от конкретных людей какую-либо информацию?* *Подводит итог беседы* *-действительно, ребята, все мы разные, кто-то любит рассказывать о себе многое, а кто-то совсем не любит болтать и особенно делиться личной информацией, по разным причинам* А теперь давайте вернемся к вопросу, прозвучавшему в начале урока *(слайд 1),* так ли хороша суперсила	-*Устная работа, ученики анализируют вопрос, предлагают свои варианты ответов* *предлагают свои варианты ответов* *ученики рассуждают, отвечают на вопрос*	8 мин.	Умение осознанно и произвольно строить речевое высказывание в устной форме Анализирование информации, внимательность. Выдвижение гипотезы.

		«чтения мыслей»? подводит итог: *-хотя кому-то чтение мыслей может показаться действительно суперсилой, на самом деле, это может быть совсем иначе для всех остальных. У всех нас есть мысли, о которых мы не хотим или не хотим, чтобы другие знали. Это наши личные мысли, и мы, вероятно, почувствовали бы смущение и уязвимость, если бы о них узнал кто-то другой.*			
4. **Постановка цели и задач урока**	Обеспечение мотивации обучения детьми, формулирование ими темы и целей урока.	*Когда вы находитесь в сети, соблюдать конфиденциальность становится сложнее. Вы можете выбирать веб-сайты, которые вы посещаете и информацию, которой вы хотите поделиться с другими, например, в социальных сетях. Но в зависимости от устройства,*	*слушают учителя, записывают тему урока*	2 мин.	Умение осознанно и произвольно строить речевое высказывание в устной форме. самоопределение. умение вступать в диалог, участвовать в коллективном обсуждении вопроса

		приложения или веб-сайта, которые вы используете, ваши слова и действия могут отслеживать. Сегодня мы поговорим о том, как лучше понять, какая информация о вас собирается и используется в интернете, особенно другими сайтами или мошенниками тема урока «конфиденциальность в сети» (слайд 2)			
5. **Изучение нового материала и усвоение новых знаний**	Обеспечение восприятия, осмысления и первичного запоминания детьми изучаемой темы	-что такое «конфиденциальность», как вы понимаете это слово? Слушает ответы, подводит итог с помощью слайда 3 -итак, мы разобрались с понятием «конфиденциальность», а теперь давайте рассмотрим, как этот термин работает в сети. Учитель раздает обучающимся листы для работы в парах (приложение 1).	*Ученики отвечают на вопрос, предлагают свои варианты* *получают рабочие*	10 мин.	Развитие самостоятельности, умения слушать и слышать. Развитие навыка участия в коллективном обсуждении тем. Познавательная активность. Формирование умения выделять и сравнивать стратегии решения задач.

		-давайте прочитаем текст задания и ответим на вопрос №1 -итак, начнем с вопроса 1 *-действительно, когда Маша зашла в интернет-магазин, это, скорее всего, отслеживалось поисковой системой и её устройством. И когда она разместила ссылку в социальных сетях, ее отследило приложение для социальных сетей.* работа со слайдом №4 -посмотрите внимательно на слайд, кто сталкивался с подобными оповещениями в интернете? слайд 5: *-компании получают информацию о вас, отслеживая ваши действия. Один из способов*	*листы, читают текст задания* *отвечают письменно, затем предлагают свои варианты ответов, принимают участие в беседе* *- отвечают на вопрос устно*		

		сделать это — использование ***файлов cookie****. Файл cookie — это небольшой текстовый файл, размещаемый на вашем устройстве сайтами, которые вы посещаете. Это позволяет компаниям собирать информацию о вас и о том, что вы делаете, пока находитесь на их сайте. Компании используют эту информацию, чтобы узнать ваши предпочтения, чтобы они могли порекомендовать вам то, что вам понравится, и облегчить вам использование их сайта.* -возвращаясь к истории Маши, что послужило причиной появления рекламы? -е*сли вас не устраивает такое отслеживание, вы можете отключить файлы cookie в настройках браузера. Обычно эту настройку*	*- файлы cookie*		

		можно найти в настройках конфиденциальности. *Слайд 6:* *- у большинства приложений и браузеров есть настройки, которые можно изменить. В настройках обычно есть раздел* **конфиденциальности,** *который представляет собой выбор, который веб-сайт или приложение предоставляет вам в отношении того, какая информация видна другим пользователям и третьим лицам. Обычно вы можете использовать эти настройки, чтобы отказаться от некоторых способов, которыми приложение отображает и передает ваши данные.* -попробуйте теперь ответить на вопрос №2 в своем рабочем листе Слушает ответы учащихся,	*-отвечают на вопрос №2*		

		подводит к выводу, что файлы cookie можно было отключить Слайд 7 Еще один способ, защитить свою конфиденциальность это прочитать условия, прежде чем нажать кнопку «принять соглашение»			
6. Применение знаний и умений в новой ситуации	Выявление пробелов первичного осмысления изученного материала, обеспечение закрепления знаний и способов действий, которые необходимы для самостоятельной работы по новому материалу.	организация и контроль за процессом выполнения заданий. итак, теперь попробуйте ответить на вопрос №3 в рабочем листе, опираясь на рассмотренную нами информацию	*-отвечают на вопрос №3 в рабочем листе, читают свои ответы, участвуют в беседе*	5 мин	уметь оформлять свои мысли в устной форме; слушать и понимать речь других. умение строить речевое высказывание в устной и письменной форме. выбор наиболее эффективных способов задач в зависимости от конкретных условий.
7. Первичное осмысление и закрепление знаний	Дать качественную оценку работы класса и отдельных обучаемых.	Выявляет качество и уровень усвоения знаний, а также устанавливает причины выявленных ошибок.	Учащиеся работают в парах с последующей взаимопроверкой, анализируют	5 мин	формирование позитивной самооценки умение самостоятельно адекватно анализировать

		Собирает рабочие листы для анализа ответов учащихся.	свою работу, выражают вслух свои затруднения и обсуждают правильность решения заданий (тест, приложение 3)		правильность выполнения действий и вносить необходимые коррективы.
8. Рефлексия учебной деятельности на уроке.	Дать количественную оценку работы учащихся	Раздает ученикам итоговый тест собирает результаты на проверку	*-ученики отвечают на вопросы теста*	7 мин.	оценивание собственной деятельности на уроке, проверка усвоенных на уроке знаний.
9. Информация о домашнем задании	Обеспечение понимания детьми содержания и способов выполнения домашнего задания	Дает комментарий к домашнему заданию	Учащиеся записывают в дневники задание, задают вопросы по дом.заданию.	3 мин.	