# **Должность: Учитель**

**Наименование профессионального стандарта**: Педагог (педагогическая деятельность в сфере основного общего, среднего общего образования) (учитель) [Приказ Министерства труда и социальной защиты РФ от 18 октября 2013 г. N 544н](https://www.ca-kk.ru/wp-content/uploads/2021/07/544%D0%BD-%D0%9F%D0%A1-%D0%9F%D0%B5%D0%B4%D0%B0%D0%B3%D0%BE%D0%B3.pdf)

**Технологическая карта урока**\*

**ФИО учителя**: Хакимов Дамир Рашитович

**Класс**: 9 класс

**УМК/ Образовательная технология**: Босова Л.Л., Босова А.Ю. Информатика. 9 класс. ФГОС, «Просвещение» 2024 г

**Предмет**: Информатика

**Тема**: Информационная безопасность

**Тип урока**: изучение нового материала

**Место и роль урока в изучаемой теме**: Урок изучения нового материала

**Цель и задачи урока**: Образовательные цели: Ознакомить учащихся с основными понятиями и угрозами информационной безопасности.

Научить распознавать потенциальные угрозы и способы защиты личной информации в интернете. Развивающие цели: Развить критическое мышление и навыки анализа информации. Стимулировать активное обсуждение и обмен мнениями по вопросам безопасности в сети.

Воспитательные цели: Воспитать ответственное отношение к личной информации. Формировать у учащихся навыки безопасного поведения в интернете.

Планируемые образовательные результаты\*\*\*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Предметные знания, предметные действия | Универсальные учебные действия | | | Личностные |
| регулятивные | познавательные | коммуникативные |
| Предметные знания  Определение информационной безопасности:  Знания о том, что информационная безопасность — это защита информации от несанкционированного доступа, искажений, уничтожения, а также защита средств, которые используется для обработки и хранения информации.  Типы угроз:  Вредоносное ПО (вирусы, черви, трояны): Понимание, как они функционируют и какие угрозы представляют.  Фишинг: Знание методов, с помощью которых злоумышленники пытаются получить личные данные пользователей через поддельные сайты и письма.  Социальная инженерия: Овладение информацией о методах манипуляции людьми для получения конфиденциальной информации.  Атаки типа DDoS: Понимание, как осуществляются распределённые атаки на серверы с целью их блокировки.  Методы защиты информации:  Шифрование: Знания о принципах шифрования данных и о том, зачем это необходимо.  Антивирусные программы: Понимание роли антивирусов в защите информации и актуальные методы их использования.  Файрволы: Знание принципов работы и назначения межсетевых экранов.  Создание надёжных паролей: Понимание основных принципов, например, длина пароля, использование специальных символов и цифр.  Правовая основа и этика:  Знания о законах, касающихся защиты данных и авторских прав.  Этические аспекты поведения в интернете и ответственности за свои действия.  2. Предметные действия  Анализ угроз:  Способность анализировать и идентифицировать потенциальные угрозы для своей информации (например, проводить аудит безопасности своих учетных записей).  Применение антивирусных решений:  Умение устанавливать и настраивать антивирусные программы для защиты персонального компьютера.  Создание безопасных паролей:  Способность разрабатывать и хранить надёжные пароли, а также использовать менеджеры паролей.  Шифрование данных:  Навыки использования программного обеспечения для шифрования файлов и понимание процесса дешифрования.  Разработка рекомендаций:  Умение составлять рекомендации по безопасности для пользователей (например, как избежать фишинга, какие меры предосторожности соблюдать при работе в интернете).  Работа с политиками безопасности:  Понимание и обсуждение политик безопасности в учреждении или организации, в которой они учатся.  Этические решения:  Способность оценивать и принимать решения в сложных ситуациях, связанных с нарушением информационной безопасности, например, в случае получения информации о кибератаках. | Целеполагание:  Умение ставить цели и задачи при изучении темы информационной безопасности, включая определение критериев успеха (например, знание основных типов угроз).  Контроль и коррекция:  Способность осуществлять самоконтроль в процессе выполнения заданий, связанных с темой безопасности, например, осмыслять свои действия при входе в различные интернет-ресурсы. | Анализ информации:  Умение выделять существенные признаки угроз информационной безопасности (например, типы вредоносного ПО, способы фишинга).  Способность классифицировать виды угроз и методы защиты информации в сети.  Рефлексия:  Оценка собственной компетенции в области безопасности в интернете и место своей информации в глобальной сети.  Умение анализировать причины собственных ошибок в цифровом поведении.  Планирование:  Формирование плана действий для повышения уровня безопасности своих данных в сети, включая выбор антивирусного ПО и стратегий создания паролей. | Групповая работа:  Умение работать в группе, обсуждая проблемы информационной безопасности и разрабатывая рекомендации по ее улучшению.  Формирование навыков ведения диалога и аргументированного обмена мнениями по вопросам защиты личной информации.  Презентация результатов:  Способность представлять результаты работы, касающиеся информационной безопасности, например, в виде доклада или презентации для одноклассников.. | Ответственность:  Формирование умений применить знания по информационной безопасности в повседневной жизни, включая ответственное поведение в интернете (например, не раскрывать личные данные).  Мотивация к обучению:  Формирование интереса и мотивации к изучению информационной безопасности как важной составляющей цифровой грамотности и защиты личной информации.  Этика в цифровом пространстве:  Развитие понимания этических норм поведения в Интернете и осознание важности соблюдения правил безопасности других пользователей. |

Ход урока

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № | Этап урока\*\*\*\* | Задача, которая должна быть решена (в рамках достижения планируемых результатов урока) | Формы организации деятельности учащихся | Действия учителя по организации деятельности учащихся | Действия учащихся (предметные, личностные, познавательные, регулятивные, коммуникативные) | Результат взаимодействия учителя и учащихся по достижению планируемых результатов урока | Диагностика достижения планируемых результатов урока |
| 1 | Организационный момент | Овладеть внимание аудитории и зантересовать о предстоящей теме урока  Формирование дисциплинированности  Отвечать на поставленные вопросы  Формирование мотивации изучения информатики | Фронтальная работа | Приветствует учащихся, проверяет готовность обучающихся к уроку.  Создает эмоциональный настрой на учебную деятельность. | Здороваются с учителем. Настраиваются на учебную деятельность.  Отвечают на вопросы учителя | Настрой к деятельности  Стремление к совершенствованию собственных умений работы за компьютером | Умение активировать внимание к предстоящей работе |
| 2 | Актуализация знаний. | Выявление уровня знаний учащихся.  Отвечать на поставленные вопросы | Фронтальная  Групповая | Задает вопросы ученикам. Показ презентации | Умения организовывать собственную деятельность.  Ответить на поставленные вопросы учителя. | Включение обучающихся в деятельность. | Взаимоконтроль |
| 3 | Определение темы и задач урока | В совместной деятельности сформулировать цели и задачи урока | Фронтальная  Групповая | Учитель рассказывает о понятиях информационной безопасности, основных угрозах (вирусы, хакеры, социальная инженерия), методах защиты (пароли, антивирусы, шифрование и др.).  Приводит примеры из реальной жизни. | Дети ставят перед собой цель на урок. | Выражают свою точку зрения. Формулируют тему урока | Активируют внимание на предстоящей работе |
| 4 | Основная часть | Формирование у учащихся новых понятий по изучаемой теме и методы реализации получегонного материала | Фронтальная | Пояснение как возможно защититься от всевозможных вариантов киберпреступности в иформационном общесте и оградить себя от различного рода проблем  Разобрать определенную жизненную ситуацию исходя из примера по заданному варианту задания | Выполняют задачи поставленные учителем. Участвуют и организовыввают собственную деятельность.  Приводят свои примеры по решению проблем защиты информации | Осуществлять взаимоконтроль  принимать и сохранять учебную цель и задачу |  |
| 5 | Рефлексия | Контроль процесса и результата учебной деятельности | Фронтальная работа | Организует беседу о материале, пройденном на уроке. Побуждает обучающихся к оценке собственной деятельности на уроке с помощью листа самооценки.  Подведение общего итога оценивания.  Осуществляет работу по оцениванию | Анализируют работу класса в целом.  Высказывают оценочные суждения.  Отвечают на вопросы учителя, обобщают работу на уроке, подводят итог (что делали, что узнали).  Оценивают по критериям себя, работу в группе, достижение целей | Развитие адекватной самооценки.  Осуществлять рефлексию в отношении действий по решению учебных и познавательных задач.  Слушать учителя, собеседника. Формулировать собственное мнение.  Осуществлять актуализацию полученных знаний по предмету | Самоконтроль |
| 6 | Домашнее задание | Развитие целеустремлённости, трудолюбия | Фронтальная работа | Объясняет домашнее задание.  Организовывает индивидуальную работу обучающихся  Завершает урок | Самоопределяются к деятельности.  Прощаются с учителем. | Принимают учебную задачу. | Выполнение работы |
|  | Итоги и самоанализ урока \*\*\*\*\* | Самоанализ урока по теме «Информационная безопасность»  Цель урока: формирование у учащихся представления об информационной безопасности и её составляющих, а также о мерах обеспечения информационной безопасности.  Задачи урока:  дать определение понятия «информационная безопасность»;  рассмотреть составляющие информационной безопасности;  изучить меры обеспечения информационной безопасности;  способствовать развитию критического мышления и умения анализировать информацию;  воспитывать ответственное отношение к информации и соблюдению правил информационной безопасности.  Для достижения поставленных целей были использованы следующие методы и приёмы:  Методы: словесный (объяснение, беседа), наглядный (презентация), практический (решение ситуационных задач).  Приёмы: работа в группах, фронтальная работа, самостоятельная работа.  В ходе урока были реализованы все поставленные задачи. Учащиеся усвоили основные понятия и правила информационной безопасности, научились применять полученные знания на практике. Урок способствовал развитию критического мышления, формированию ответственного отношения к информации.  Тем не менее, можно выделить некоторые моменты, которые требуют доработки:  1. Необходимо уделить больше внимания практическому применению полученных знаний, например, предложить учащимся разработать памятку по информационной безопасности для своих сверстников.  2. Следует разнообразить формы работы на уроке, чтобы поддерживать интерес учащихся и стимулировать их активность.  3. Важно учитывать индивидуальные особенности учащихся при выборе заданий и форм работы.  4. Рекомендуется использовать дополнительные источники информации, такие как видеоматериалы, статьи или книги, для более глубокого изучения темы.  5. Стоит обратить внимание на развитие навыков самостоятельной работы учащихся, предоставляя им больше возможностей для самостоятельного поиска информации и решения задач.  6. Можно включить в урок элементы дискуссии или дебатов, чтобы учащиеся могли выразить свою точку зрения и аргументировать свои ответы.  7. Для закрепления материала рекомендуется провести тестирование или опрос, чтобы оценить уровень усвоения темы учащимися.  8. В конце урока необходимо подвести итоги, обобщить основные выводы и подчеркнуть важность соблюдения правил информационной безопасности в повседневной жизни.  Таким образом, проведённый урок по теме «Информационная безопасность» достиг поставленных целей и задач, но требует некоторых доработок для повышения эффективности обучения и развития учащихся. | | | | | |

\* Технологическая карта урока является документом, подтверждающим деятельность, оформленную учителем в «Описании педагогической деятельности».

\*\* Цель и задачи урока формулируются в соответствии с педагогическими функциями: обучение, воспитание, развитие.

\*\*\* Таблица заполняется с учетом этапов формирования, планируемых образовательных результатов и применения контроля предметных знаний, предметных действий, метапредметных умений и личностных образовательных результатов, по конкретной теме (заполнение всех граф таблицы обязательно), в соответствии с возрастными психологическими особенностями обучающихся.

\*\*\*\* Этапы указываются в соответствии с типом урока, реализуемой педагогом технологии, методики, предметной области.

\*\*\*\*\* Осуществлен анализ проведенного урока, дана оценка его эффективности.

.