Преподавание основ кибербезопасности в школе

Учитель высшей категории

Воронина Елена Вальдемаровна

г Елизово

Содержание

Введение

Актуальность данной темы обусловлена ростом количества киберугроз и увеличением использования цифровых технологий в образовательном процессе. Современные учащиеся сталкиваются с различными видами киберрисков, такими как фишинг, вредоносное ПО, кража личных данных и кибербуллинг.

Недостаточно информированности в области кибербезопасности увеличивает риск негативных последствий. Поэтому развитие эффективных методик обучения основам кибербезопасности является важной задачей для повышения информационной грамотности учащихся, формирования навыков безопасного поведения в сети и защиты личных данных.

Значимость изучения темы «Методика преподавания основ кибербезопасности в школе» обусловлена современным уровнем развития информационных технологий и широким распространением цифровых устройств в повседневной жизни учащихся. Этот аспект образования играет ключевую роль в формировании у школьников компетенций, необходимых для безопасного и осознанного поведения в цифровом пространстве.

Во-первых, цифровая грамотность становится неотъемлемой частью общего образования, а кибербезопасность — одной из его важных составляющих. Ученики постоянно сталкиваются с разнообразными киберугрозами, такими как вирусы, фишинг, мошенничество, социальная инженерия и другие виды атак. Без специальных знаний и навыков они становятся уязвимыми для этих угроз, что может привести к потере личных данных, финансовым убыткам, психологическим травмам и другим негативным последствиям.

Во-вторых, методика преподавания кибербезопасности в школе направлена на системное и последовательное усвоение знаний, развитие критического мышления и практических умений, позволяющих эффективно противостоять рискам в интернете. Это способствует формированию ответственного отношения к использованию цифровых технологий, развитию

навыков самозащиты, а также пониманию этических и правовых аспектов цифрового поведения.

В-третьих, внедрение методики обучения кибербезопасности помогает педагогам структурировать учебный процесс, используя современные образовательные технологии и интерактивные методы — игровые формы, ролевые игры, практические кейсы. Это повышает мотивацию учащихся, способствует более глубокому усвоению материала и развитию навыков командной работы.

Кроме того, изучение методики преподавания кибербезопасности обеспечивает подготовку учителей к эффективной работе в условиях постоянного изменения цифровой среды и новых видов угроз. Это позволяет оперативно обновлять содержание учебных программ и адаптировать методы обучения к актуальным вызовам.

Наконец, тема «Методика преподавания основ кибербезопасности в школе» имеет важное социальное значение, поскольку способствует формированию у подрастающего поколения культуры цифровой безопасности, что в перспективе влияет на общую информационную безопасность общества.

Таким образом, изучение данной темы является необходимым и актуальным направлением в современной педагогике, отвечающим требованиям цифровой эпохи и способствующим подготовке учащихся к безопасной и эффективной жизни в информационном обществе.

Объектом исследования является процесс формирования у школьников знаний, умений и навыков, необходимых для обеспечения собственной информационной безопасности в онлайн-среде.

Предметом исследования является методика преподавания основ кибербезопасности в школе, включая подходы, методы, содержание учебных программ и средства обучения, используемые для формирования у учащихся компетенций в области информационной безопасности.

Цель исследования: ознакомить учащихся с основными понятиями и принципами кибербезопасности.

Задачи исследования:

- Формирование понимания важности защиты персональных данных.
- Развитие навыков безопасной работы в интернете.
- Воспитание культуры безопасного поведения в цифровой среде.

Часть 1. Теоретический материал по основам кибербезопасности

1.1. Связь информационной безопасности и кибербезопасности

Защита информации и кибернетическая безопасность представляют собой два отдельных направления в сфере информационных технологий, тесно взаимосвязанных между собой.

Хотя эти две области все чаще взаимодействуют по мере технологического прогресса, важно рассматривать каждую из них как самостоятельную дисциплину, учитывая ее специфические цели и задачи.

Проанализируем различия между ними, сравнивая защиту информации и кибербезопасность: кибербезопасность обеспечивает защиту цифровой среды от вторжений, в то время как информационная безопасность направлена на предохранение данных в целом от всевозможных угроз [8].

Первоочередная задача кибербезопасности – защита сетей, устройств и систем от кибератак. Она также предполагает обеспечение безопасности пользователей от кражи персональных данных, мошенничества и других видов онлайн-преступности. Кибербезопасность охватывает защиту личной информации пользователей путем шифрования их переписки и данных. Важно понимать, что кибербезопасность не занимается охраной интеллектуальной собственности компаний и не гарантирует конфиденциальность информации о сотрудниках [6].

Информационная безопасность концентрируется на защите корпоративных данных от неавторизованного доступа как со стороны сотрудников, так и извне. Обеспечение надежного хранения конфиденциальной информации, предотвращение ее попадания в нежелательные руки – ключевая задача. Информационная безопасность включает в себя три составляющие: физическую (например, ограничение доступа к документам), логическую (например, шифрование важных данных) и административную (например, регулярная смена паролей).

Основная задача информационной безопасности заключается в оказании помощи организациям в защите их интеллектуальной собственности,

клиентской информации, коммерческих секретов, служебной документации и других ценных ресурсов от несанкционированного доступа, использования или разглашения злоумышленниками [3].

Информационная безопасность и кибербезопасность, хотя и являются отдельными сферами, тесно связаны, что приводит к смешению в понимании их специфики. В данной статье мы подробно разберем обе концепции, чтобы помочь вам сформировать четкое представление и принять взвешенные решения о защите данных как в частном, так и в государственном секторе [2].

Информационная безопасность ориентирована на защиту данных от неправомерного доступа, обеспечивая их конфиденциальность, целостность и доступность. Кибербезопасность нацелена на защиту сетей, систем и данных от киберугроз и атак. Обе области критически важны для защиты конфиденциальной информации и предотвращения утечек. Несмотря на взаимосвязь, они преследуют разные цели: кибербезопасность в основном занимается внешними угрозами, в то время как информационная безопасность охватывает как внутренние, так и внешние риски [7].

Цель информационной безопасности – защитить интеллектуальную собственность, клиентские данные, коммерческие тайны, информацию в CRM и другие ценные ресурсы организации от несанкционированного доступа или использования.

Меры информационной безопасности включают шифрование, политики контроля доступа и аутентификацию электронной почты. Например, интернет-магазин должен защищать данные клиентов и заказов, применяя шифрование, разрабатывая политики использования паролей и мониторинга сетевого доступа.

Кибербезопасность – это защита сетей, систем и данных от несанкционированного доступа, модификации и уничтожения. Это общий термин для технологий и дисциплин, предотвращающих несанкционированный доступ к сетям и данным.

Кибербезопасность включает анализ рисков, обнаружение и реагирование, а также защиту [14].

В отличие от этого, информационная безопасность представляет собой более широкое и всеобъемлющее понятие, охватывающее все способы и методы, используемые для защиты информации от несанкционированного доступа, использования, раскрытия, изменения или уничтожения, вне зависимости от ее формы представления. Она обеспечивает защиту данных и информации независимо от их физического местоположения – будь то жесткий диск компьютера в офисе или удаленный сервер за границей.

Основное различие заключается в том, что кибербезопасность обеспечивает механизмы защиты исключительно в рамках киберпространства, тогда как информационная безопасность ставит своей целью охрану данных независимо от их местонахождения или способа использования, будь то в домашней или коммерческой среде.

Кибербезопасность ориентирована на охрану компьютерных систем и сетей от атак в цифровой среде, включая кибертерроризм и другие угрозы, использующие вычислительные устройства или сети как инструменты. В свою очередь, информационная безопасность нацелена на защиту данных независимо от формата их хранения [23].

Например, защита электронных сообщений от взлома – это задача кибербезопасности. Обеспечение конфиденциальности медицинских карт семьи – это вопрос информационной безопасности.

Таким образом, кибербезопасность противостоит опасностям в киберпространстве, возникающим при использовании компьютеров, мобильных устройств или подключении к интернету. Информационная безопасность занимается защитой любых видов данных, будь то физические документы (финансовые отчеты) или цифровая информация (учетные записи электронной почты) [5].

1.2. Основные понятия кибербезопасности

Кибербезопасность – это комплекс мер, включающий технологии и алгоритмы, направленные на охрану IT-инфраструктуры, компьютерных сетей и цифровой информации от киберугроз, хакерских атак и вредоносного программного обеспечения [1].

Ежеминутно в мире фиксируются тысячи попыток несанкционированного доступа к различным системам. По данным статистики, в 2023 году Россия вошла в число лидеров по количеству скомпрометированных учетных записей. За противоправными действиями в сети могут стоять как отдельные киберпреступники, так и организованные хакерские группы, а иногда и структуры, финансируемые правительствами различных стран.

Многочисленные случаи утечки секретной информации и сбоев в работе сетей наглядно демонстрируют, что цифровые данные стали важнейшим элементом функционирования современного бизнеса, органов государственной власти и повседневной жизни обычных пользователей. Обеспечение сохранности этих данных напрямую влияет на безопасность общества в целом. В качестве примера можно привести атаку вируса Stuxnet в 2010 году, которая показала, что вредоносные программы могут быть использованы для нанесения ущерба критически важной инфраструктуре целых государств, в частности, ядерным объектам.

Востребованность кибербезопасности возрастает также в связи с активным развитием Интернета вещей (IoT) и ростом числа подключенных устройств. Ожидается существенный рост рынка IoT, что делает важным защиту каждого устройства, будь то умный телевизор или медицинский прибор, от потенциальных киберугроз.

Взломанные устройства могут быть использованы злоумышленниками для создания ботнетов или для получения доступа к конфиденциальной информации [6].

Не стоит забывать и о человеческом факторе. Значительное число инцидентов происходит из-за ошибок пользователей, таких как выбор слабых паролей, переход по небезопасным гиперссылкам или загрузка подозрительных файлов [5].

Обеспечение кибербезопасности предполагает комплекс мер, направленных на поддержание конфиденциальности, целостности и доступности цифровой информации. Для реализации этой ключевой цели необходимо решение следующих задач:

1. Предотвращение несанкционированных проникновений в сетевую инфраструктуру и серверное оборудование.
2. Выявление и ликвидация слабых мест в прикладном программном обеспечении.
3. Обеспечение защиты от атак, направленных на устройства, подключенные к сети Интернет вещей.
4. Оперативное реагирование на инциденты, связанные с компрометацией и утечкой цифровых данных.

Для достижения основной цели, задачи кибербезопасности реализуются посредством следующих мероприятий:

1. Охрана систем: недопущение несанкционированного доступа к информационным системам и сетевым ресурсам.
2. Контроль и аналитика: непрерывный мониторинг состояния безопасности систем и сетей, а также анализ возникающих инцидентов с целью совершенствования механизмов защиты.
3. Проактивный подход: обнаружение уязвимостей в системе и прогнозирование потенциальных угроз для своевременного усиления защитных мер.
4. Повышение квалификации персонала: просвещение сотрудников относительно существующих киберугроз и методов их нейтрализации [16].

1.3. Основные угрозы кибербезопасности

Основные угрозы кибербезопасности – это различные тактики и способы, применяемые киберпреступниками для несанкционированного проникновения в информационные ресурсы, дестабилизации информационных систем и нанесения вреда пользователям или компаниям.

Далее рассмотрим подробнее три главных типа угроз: фишинговые атаки и рассылки нежелательной почты, вредоносные программы и вирусы, а также методы социальной инженерии [6].

1. Фишинг и спам.

Фишинг представляет собой кибернападение, когда злоумышленник старается обманным путем вынудить пользователя предоставить секретные данные: пароли, реквизиты кредитных карт, сведения о банковских счетах и другие персональные данные. Для этого применяются фальшивые электронные письма, сообщения или веб-сайты, которые имитируют подлинные и надежные источники (банки, популярные сервисы, государственные органы).

Механизм фишинга: юзер получает письмо с просьбой пройти по ссылке для "обновления" учетной записи, "подтверждения" сведений или "получения приза". Кликнув по ссылке, он попадает на поддельный сайт, очень похожий на настоящий, где он вводит свои данные, которые тут же оказываются в руках мошенника.

Угрозы: хищение денег, взлом учетных записей, распространение вредоносных программ, мошенничество.

Спам – это массовая отправка нежелательных сообщений, чаще всего рекламного содержания, но также используемая для распространения фишинговых ссылок или вредоносных вложений.

Спамеры применяют поддельные адреса отправителей, чтобы увеличить доверие и подтолкнуть к открытию письма [13].

Риски спама: переполнение почтовых ящиков, снижение производительности, переход на опасные сайты, заражение вредоносными программами из вложений.

2. Вредоносное ПО и вирусы.

Вирусы – это программы или код, имеющие способность самостоятельно распространяться и интегрироваться в другие программы или файлы, вызывая поломки, потерю информации или изменение функционирования системы.

Вредоносное ПО (malware) – более широкое понятие, включающее всевозможные типы вредоносных программ: вирусы, "трояны", "червей", шпионские программы, программы-вымогатели, кейлоггеры и прочее.

"Трояны" маскируются под законное ПО. После запуска совершают тайные вредоносные действия: кража данных, удаленный контроль компьютера.

"Черви" самопроизвольно распространяются по сети, заражая много компьютеров и перегружая сеть.

Шпионские программы незаметно собирают персональную информацию, историю просмотров, пароли.

Программы-вымогатели шифруют данные пользователя и требуют оплату за их восстановление [18].

Распространение: через вложения в письмах, скачивание из подозрительных источников, уязвимости в ПО.

Последствия: утрата информации, финансовые расходы, сбои в работе коммерческих процессов, утечка конфиденциальных данных.

3. Социальная инженерия.

Социальная инженерия – это комплекс методов психологического воздействия и манипуляции, применяемых злоумышленниками для обмана людей с целью заполучения доступа к информации или системам.

В отличие от технических атак, социальная инженерия эксплуатирует человеческий фактор [25].

Примеры методов:

1. Фишинг по телефону (вишинг): звонки, когда преступник представляется сотрудником банка или технической поддержки и пытается выведать секретные данные.

2. Претекстинг: создание ложной предыстории, дабы вызвать доверие и получить требуемую информацию.

3. Злоупотребление доверием: использование знаний о человеке (например, из соцсетей) для убеждения его раскрыть секреты.

4. Физический доступ: злоумышленники могут попытаться попасть в офис или использовать поддельные документы.

5. Риски: Утечка паролей и взлом систем.

6. Внедрение вредоносных программ через доверие сотрудников.

7. Финансовые потери и компрометация информации [19].

Для результативной защиты от отмеченных угроз нужен комплексный подход: антивирусы, системы фильтрации, шифрование, обучение пользователей правилам безопасности, систематический аудит и обновление систем.

Необходимо расширять информированность юзеров о методах атак и создавать культуру информационной безопасности в компании.

1.4. Методы защиты кибербезопасности

Методы защиты кибербезопасности являются основой для обеспечения безопасности информации и предотвращения несанкционированного доступа, потери данных или других вредоносных воздействий на компьютерные системы и сети.

Рассмотрим три ключевых аспекта защиты: создание сложных паролей в сочетании с двухфакторной верификацией, регулярное обновление программного обеспечения и использование антивирусных программ [27].

1. Сложные пароли и двухфакторная аутентификация – это основа защиты учетных записей и систем. Пароль должен обладать высокой степенью сложности, чтобы его было трудно подобрать.

– Рекомендуется использовать пароли длиной от 12 символов.

– Пароль должен содержать как прописные, так и строчные буквы, цифры и символы.

– Не используйте личную информацию или распространенные слова.

– Регулярно меняйте пароли и не используйте старые комбинации.

– Для каждого сервиса используйте уникальный пароль. 2FA – это дополнительный уровень защиты, требующий подтверждения личности двумя способами, например, пароль и код из SMS или приложения.

– 2FA существенно снижает риск взлома.

– Защищает от фишинга и кражи паролей.

– Рекомендуется использовать 2FA везде, где это возможно.

2. Обновление программного обеспечения – это важный метод защиты, так как многие атаки используют известные уязвимости.

– Обновления устраняют уязвимости, повышают стабильность и добавляют новые функции.

– Включайте автоматическое обновление системы и приложений.

– Следите за обновлениями антивирусов и браузеров. Игнорирование обновлений увеличивает риск заражения вредоносным ПО и утечки данных.

3. Антивирусные программы обнаруживают, блокируют и удаляют вредоносное ПО.

– Антивирусы сканируют файлы и систему, проводят мониторинг в реальном времени и обновляют базы сигнатур.

– Устанавливайте антивирусы от проверенных производителей и регулярно обновляйте их.

– Проводите полные сканирования системы.

Совместное применение надежных паролей с 2FA, своевременное обновление ПО и использование антивирусов формирует прочную защиту кибербезопасности.

Часть 2. Практические задания по теме «Кибербезопасность в школе»

Для эффективного усвоения основ кибербезопасности в школе важно сочетать теоретические знания с практическими упражнениями и игровыми формами обучения.

Ниже представлены подробные описания упражнений и игровых методов, которые помогут учащимся лучше понять и применять принципы безопасности в цифровом пространстве.

Упражнения по теме «Методика преподавания основ кибербезопасности в школе»:

1. Создание надежных паролей.

Цель: научить учащихся генерировать сложные и надежные пароли, предотвращающие несанкционированный доступ к аккаунтам.

Описание: педагог объясняет, что такое надежный пароль, какие требования к нему предъявляются (длина, комбинация символов, отсутствие личной информации). Затем учащиеся самостоятельно или в группе создают примеры надежных паролей и проверяют их «силу» через специальные онлайн-сервисы или вручную.

Результат: Формирование у учащихся навыка создания и использования надежных паролей.

Примеры заданий:

Задание 1:

Составьте 3 сложных пароля, которые вы могли бы использовать для своих учетных записей. Убедитесь, что пароли:

1. Содержат не менее 12 символов.
2. Включают заглавные и строчные буквы, цифры и специальные символы.
3. Не содержат вашего имени, даты рождения или простых слов.

Задание 2:

Приведите примеры слабых паролей (например, «123456», «password», «qwerty») и преобразуйте их в надежные, используя правила из урока.

Задание 3:

Проверьте силу своих паролей с помощью онлайн-сервиса (например, https://password.kaspersky.com/ или https://howsecureismypassword.net/) и проанализируйте, что можно улучшить.

2. Анализ фишинговых писем.

Цель: развить у учеников умение распознавать фишинговые сообщения и избегать угроз.

Описание: представляются примеры реальных и поддельных писем, учащиеся выявляют признаки фишинга: подозрительные ссылки, орфографические ошибки, просьбы о предоставлении личной информации. Проводится обсуждение, как правильно реагировать на такие письма.

Результат: Повышение осведомленности и навыков защиты от мошеннических сообщений.

Примеры заданий:

Задание 1:

Представьте несколько примеров писем (распечатанные или показанные на экране), среди которых есть настоящие и фишинговые. Определите признаки, по которым можно отличить фишинговое письмо (например, подозрительные ссылки, ошибки в тексте, просьбы о личных данных).

Задание 2:

Ответьте на вопросы:

1. Что вы будете делать, если получите подозрительное письмо?
2. К кому обратиться за помощью?
3. Какие действия нельзя предпринимать при получении фишингового письма?

Задание 3:

Составьте список правил безопасного обращения с электронной почтой, чтобы избежать попадания в ловушки мошенников.

3. Установка антивирусных программ.

Цель: ознакомить учащихся с процессом установки и первоначальной настройкой антивирусного ПО.

Описание: демонстрация или практическое занятие, где учащиеся устанавливают антивирусные программы на школьные компьютеры или симулируют процесс, изучают основные функции и важность регулярных обновлений.

Результат: понимание роли антивирусов в защите и умение базовой работы с ними.

Примеры заданий:

Задание 1:

На школьных компьютерах или в демонстрационном режиме покажите, как скачать и установить бесплатный антивирус (например, Avast, Kaspersky Free, AVG).

Задание 2:

Настройте автоматическое обновление антивирусных баз и проведите полное сканирование системы.

Задание 3:

Обсудите, почему важно регулярно обновлять антивирус и что может произойти при отсутствии защиты.

Эти задания помогут учащимся на практике усвоить основные принципы кибербезопасности, развить навыки безопасного поведения в интернете и повысить личную ответственность за защиту своих данных.

Игровые формы по теме «Методика преподавания основ кибербезопасности в школе»:

1. Квесты по кибербезопасности:

Цель: активизировать интерес к теме через интерактивное обучение и командную работу.

Описание: организуются тематические квесты, где команды выполняют задания по распознаванию угроз, созданию паролей, анализу ситуации и выбору безопасных действий. Задания могут быть представлены в виде головоломок, викторин, практических сценариев.

Результат: Укрепление знаний и навыков через игровой опыт, развитие командного взаимодействия.

2. Ролевые игры на тему социальной инженерии:

Цель: показать методы психологического воздействия злоумышленников и научить противодействовать им.

Описание: учащиеся делятся на группы и разыгрывают роли: одни – «мошенники», пытающиеся получить конфиденциальную информацию, другие – «жертвы», которые должны распознать и отвергнуть попытки манипуляции. После игры проводится разбор действий и обсуждение эффективных приёмов защиты.

Результат: развитие критического мышления и навыков защиты от социальных атак.

Комбинация практических упражнений и игровых методов способствует более глубокому и осознанному усвоению материала по кибербезопасности.

Такой подход помогает формировать у школьников необходимые навыки для безопасного поведения в цифровом мире и создает положительный эмоциональный настрой на изучение важной темы.

Приведем несколько примеров квестов и игровых форм по кибербезопасности, которые соответствуют описанным целям и формату:

1. Квест «Взлом системы».

Цель: научиться распознавать фишинговые письма и злонамеренные ссылки.

Задание: команда получает набор писем и сообщений – часть из них настоящие, часть – фишинговые. Нужно за ограниченное время определить, какие из них опасны, и объяснить почему.

Формат: головоломка + обсуждение.

Результат: умение быстро выявлять подозрительные сообщения и не попадаться на уловки злоумышленников.

2. Квест «Создай надежный пароль».

Цель: показать важность сложных паролей и методов их создания.

Задание: участникам предлагается сгенерировать безопасный пароль, соблюдая правила (длина, разнообразие символов), и проверить его «на прочность» с помощью онлайн-сервисов или сценариев.

Формат: практическое упражнение + викторина.

Результат: понимание, как создавать и хранить надежные пароли.

3. Ролевая игра «Социальная инженерия в действии».

Цель: научиться распознавать попытки манипуляций и социального давления.

Задание: одна группа играет роль «мошенников», пытающихся получить пароль у другой группы – «сотрудников». «Мошенники» используют разные приемы: давление, лестные слова, инсценировки. «Сотрудники» должны либо отказаться, либо правильно проверить личность.

Формат: ролевая игра с последующим обсуждением.

Результат: развитие навыков противодействия социальному давлению и манипуляциям.

4. Квест «Безопасный серфинг»

Цель: научить распознавать опасные сайты и угрозы в интернете.

Задание: группе предлагаются скриншоты и описания разных сайтов и приложений – нужно определить, какие из них небезопасны, и обосновать выбор.

Формат: викторина + анализ случаев.

Результат: повышение осведомленности о сомнительных ресурсах и способах защиты.

5. Интерактивный сценарий «Потеря устройства».

Цель: отработать последовательность действий при потере смартфона или ноутбука.

Задание: участникам предлагается описать, какие шаги нужно предпринять, чтобы минимизировать ущерб (блокировка, смена паролей, уведомление IT-поддержки).

Формат: командное обсуждение и практические рекомендации.

Результат: формирование алгоритма действий в экстренных ситуациях.

Эти игровые формы помогут сделать обучение кибербезопасности увлекательным, практичным и эффективным.

Приведем пример лабораторных заданий по кибербезопасности для школьников. Эти задания помогут учащимся узнать основы кибербезопасности, развить навыки анализа и защиты информации, а также понять важность безопасности в цифровом пространстве.

Лабораторное задание 1: основы паролей.

Цель: понять важность сильных паролей и методы их создания.

Задания:

1. Исследуйте, что делает пароль сильным. Напишите краткий отчет (до 1 страницы).

2. Создайте 3 разных пароля: слабый, средний и сильный. Объясните, почему каждый из них имеет такой уровень безопасности.

3. Используйте онлайн-генератор паролей, чтобы создать 5 сильных паролей и сохраните их в безопасном месте (например, в менеджере паролей).

Лабораторное задание 2: фишинг и социальная инженерия.

Цель: выявить угрозы фишинга и социального инжиниринга.

Задания:

1. Прочитайте о техниках фишинга и социального инжиниринга. Напишите краткий отчет (до 1 страницы).

2. Создайте фальшивое электронное письмо, имитирующее фишинговую атаку (без использования реальных адресов). Включите элементы, которые могут выдать его как фальшивое.

3. Обсудите с классом, как можно защититься от фишинга.

Лабораторное задание 3: Защита Wi-Fi сети.

Цель: изучить методы обеспечения безопасности беспроводных сетей.

Задания:

1. Исследуйте основные протоколы безопасности Wi-Fi (WEP, WPA, WPA2, WPA3). Напишите краткий отчет о каждом.

2. Если у вас есть доступ к маршрутизатору, измените настройки безопасности, чтобы использовать WPA3 (если доступно).

3. Проведите тест на безопасность своей сети (например, с помощью приложения для анализа Wi-Fi, как Wireshark).

Лабораторное задание 4: Основы шифрования.

Цель: понять, как работает шифрование.

Задания:

1. Прочитайте о различных методах шифрования (симметричное и асимметричное). Напишите краткий отчет (до 1 страницы).

2. Используйте онлайн-генератор для шифрования простого текста (например, “Привет, мир!”) помощью метода Цезаря.

3. Попробуйте расшифровать текст самим или с помощью онлайн-инструмента.

Лабораторное задание 5: Анализ вредоносного ПО.

Цель: изучить, как работает вредоносное ПО и как его выявлять.

Задания:

1. Посмотрите видео или прочитайте материал о различных типах вредоносного ПО (вирусы, трояны, шпионские программы и др.).

2. Создайте презентацию о том, как распознать вредоносное ПО и что делать, если оно было обнаружено.

3. На своем компьютере выполните сканирование с помощью бесплатного антивирусного ПО и проанализируйте результаты.

Лабораторное задание 6: Защита личной информации.

Цель: понять важность защиты личной информации в интернете.

Задания:

1. Исследуйте, какие данные о вас могут быть доступны в интернете (например, через социальные сети).

2. Проведите аудит своих аккаунтов в социальных сетях, проверьте настройки конфиденциальности и сделайте необходимые изменения.

3. Подготовьте рекомендации для своих сверстников о том, как защитить свою личную информацию в сети.

Лабораторное задание 7: Создание безопасного веб-сайта

Цель: изучить основы веб-безопасности.

Задания:

1. Создайте простой веб-сайт с использованием HTML и CSS.

2. Исследуйте, как можно защитить веб-сайт от угроз (например, SQL-инъекций, XSS).

3. Примените методы защиты на своем веб-сайте и напишите отчет о том, что вы сделали.

Эти лабораторные задания помогут учащимся развить понимание кибербезопасности и развить навыки, которые будут полезны в будущем.

Часть 3. Оценочные материалы по теме «Кибербезопасность в школе»

Оценочные материалы по теме «Методика преподавания основ кибербезопасности в школе» представляют собой инструменты для проверки знаний, умений и навыков учащихся, а также для развития их практических компетенций в области безопасного поведения в цифровом пространстве.

Ниже приведено подробное описание двух основных типов таких материалов с примерами.

1. Тесты.

Цель: проверить уровень усвоения учащимися основных понятий кибербезопасности, методов защиты информации и навыков распознавания угроз.

Структура тестов:

1. Вопросы с выбором одного правильного ответа.
2. Вопросы с множественным выбором.
3. Вопросы на сопоставление (например, термины и их определения).
4. Ситуационные задачи для оценки умения применять знания на практике.

Примеры заданий:

Вопрос 1 (множественный выбор): Какие из перечисленных действий помогут защитить ваши личные данные в интернете?

а) Использование сложных паролей

б) Открытие вложений от незнакомцев

в) Регулярное обновление программного обеспечения

г) Сообщение пароля друзьям

Правильные ответы: а), в)

Вопрос 2 (одинарный выбор):

Что такое фишинг?

а) Вирус, который удаляет файлы

б) Мошенническая попытка получить конфиденциальную информацию, выдаваясь за доверенное лицо

в) Тип антивирусной программы

г) Способ создания надежных паролей

Правильный ответ: б)

Вопрос 3 (ситуационная задача):

Вы получили электронное письмо с просьбой срочно обновить пароль через ссылку. Какие ваши действия?

а) Перейти по ссылке и обновить пароль

б) Удалить письмо и не переходить по ссылке

в) Связаться с официальной службой поддержки сайта для подтверждения

г) Отправить письмо друзьям

Правильные ответы: б), в)

Вопрос 4 (сопоставление):

Сопоставьте термины с их определениями:

Термин	Определение
Антивирус	Программа для защиты от вредоносных программ
Социальная инженерия	Метод психологического воздействия для получения конфиденциальной информации
VPN	Сервис для создания защищённого интернет-соединения
Фишинг	Попытка обмана с целью получения личных данных

Критерии оценки:

1. Полнота и правильность ответов.
2. Понимание принципов защиты.
3. Способность применять знания в практических ситуациях.

2. Практические проекты.

Цель: развить у учащихся умения создавать информационные материалы по кибербезопасности, ориентированные на различную аудиторию, и применять знания на практике.

Формат: индивидуальная или групповая работа, результатом которой становится оформленная инструкция, памятка, буклет или презентация.

Примеры проектов:

Проект 1. Создание инструкции «Правила безопасной работы в интернете для школьников»

Содержание инструкции может включать:

1. Как создавать и хранить надежные пароли (примеры хороших и плохих паролей).
2. Основные признаки фишинговых писем и как на них реагировать.
3. Правила безопасного общения в социальных сетях (например, не раскрывать личную информацию).
4. Как правильно скачивать приложения и обновлять программы.
5. Алгоритм действий при подозрении на взлом аккаунта.

Пример фрагмента инструкции:

«Никогда не сообщайте свои пароли никому, даже друзьям. Используйте пароли, содержащие заглавные и строчные буквы, цифры и специальные символы.

Например, вместо “123456” лучше создать пароль “S3cur3P@ssw0rd!”. Если вы получили подозрительное письмо – не переходите по ссылкам и не открывайте вложения.»

Проект 2. Разработка памятки для родителей «Как обеспечить безопасность детей в интернете»

Основные разделы:

1. Настройка родительского контроля на устройствах.
2. Советы по ограничению времени пребывания в интернете.
3. Рекомендации по обучению детей правилам безопасности.
4. Программы и приложения для мониторинга активности.

Проект 3. Презентация «Основные угрозы в интернете и методы защиты»

Задачи презентации:

1. Описать распространенные угрозы: вирусы, фишинг, социальная инженерия.
2. Показать способы защиты: антивирусы, обновления, проверка источников информации.
3. Рассказать о важности критического мышления и осмотрительности.

Критерии оценки проектов:

1. Полнота и точность представленной информации.
2. Ясность, доступность и логичность изложения.
3. Оформление и визуальная привлекательность (для презентаций и памяток).
4. Практическая польза и применимость рекомендаций.

Использование тестов и практических проектов как оценочных материалов позволяет всесторонне проверить знания и навыки учащихся в области кибербезопасности.

Такой подход способствует не только теоретическому усвоению материала, но и формированию практических умений, необходимых для безопасного поведения в цифровом мире.

По окончании тестирования и выполнения заданий организуйте обсуждение, в котором учащиеся смогут поделиться своими находками и выводами из проведенных исследований. Это поможет углубить понимание

темы и позволит учащимся обсудить важные аспекты кибербезопасности в более широком контексте.

Эти оценочные материалы помогут учителям эффективно оценить знания учащихся в области кибербезопасности и развивать их навыки защиты информации.

Часть 4. Технологические карты по теме «Кибербезопасность»

Технологические карты по теме «Кибербезопасность» являются неотъемлемой частью образовательного процесса. Они помогают учителям эффективно планировать и проводить занятия, обеспечивая системный подход к обучению учащихся основам безопасности в цифровом мире.

Ниже представлены подробные технологические карты уроков по теме «Кибербезопасность» для 7–11 классов. Каждая карта включает цель урока, планируемые результаты, структуру занятия, методы и формы работы, а также примерное время на каждый этап.

Технологическая карта урока 1.

Тема: Введение в кибербезопасность.

Класс: 7–8.

Продолжительность: 45 минут.

Цели урока:

1. Ознакомить учащихся с понятием кибербезопасности.
2. Показать значимость защиты информации в цифровом мире.
3. Рассмотреть основные угрозы в интернете.

Планируемые результаты:

1. Учащиеся смогут дать определение кибербезопасности.
2. Назовут основные виды угроз в интернете.
3. Поймут важность безопасного поведения в сети.

Оборудование и материалы:

1. Презентация с иллюстрациями.
2. Компьютер и проектор.
3. Раздаточные материалы с ключевыми понятиями.

Ход урока:

Этап	Содержание	Время	Методы и формы работы
Организационный момент	Приветствие, постановка целей урока	5 мин	Фронтальная беседа
Актуализация знаний	Обсуждение: «Какие угрозы в интернете вы знаете?»	5 мин	Мозговой штурм, обсуждение в группе
Изучение нового материала	Понятие кибербезопасности, основные угрозы (вирусы, фишинг, мошенничество)	15 мин	Лекция с презентацией, объяснение
Практическое задание	Разбор простого кейса: «Что делать, если пришло подозрительное письмо?»	10 мин	Работа в парах, обсуждение
Итог урока	Рефлексия: вопросы и ответы, краткое повторение	5 мин	Обсуждение, устный опрос
Домашнее задание	Подготовить список правил безопасного поведения в интернете	–	Индивидуальная работа

Технологическая карта урока 2.

Тема: Создание надежных паролей и основы защиты личных данных

Класс: 8–9.

Продолжительность: 45 минут

Цели урока:

1. Научить создавать надежные пароли.
2. Рассмотреть методы защиты личной информации.
3. Формировать навыки ответственного использования цифровых сервисов.

Планируемые результаты:

1. Учащиеся смогут создать сложный и надежный пароль.
2. Поймут, как защитить личные данные в интернете.
3. Осознают риски использования слабых паролей.

Оборудование и материалы:

1. Компьютеры или планшеты с доступом в интернет.
2. Презентация.
3. Таблицы с критериями надежности паролей.

Ход урока:

Этап	Содержание	Время	Методы и формы работы
Организационный момент	Приветствие, постановка целей урока	5 мин	Фронтальная беседа
Актуализация знаний	Обсуждение: «Какие пароли вы используете? Почему?»	5 мин	Обсуждение в классе

Изучение нового материала	Правила создания надежных паролей, примеры и ошибки	15 мин	Лекция с презентацией, демонстрация
Практическое задание	Создание собственных паролей, проверка их надежности с помощью онлайн-сервисов	15 мин	Индивидуальная работа на компьютерах
Итог урока	Обсуждение результатов, выводы	5 мин	Рефлексия, устный опрос
Домашнее задание	Подготовить памятку с советами по защите личных данных	–	Индивидуальная работа

Технологическая карта урока 3.

Тема: Социальная инженерия и методы защиты от нее

Класс: 9–11.

Продолжительность: 45–60 минут.

Цели урока:

1. Показать методы социальной инженерии.
2. Научить распознавать попытки манипуляций.
3. Развить навыки защиты от психологического воздействия злоумышленников.

Планируемые результаты:

1. Учащиеся смогут объяснить, что такое социальная инженерия
2. Определять признаки попыток манипуляций.
3. Применять методы противодействия.

Оборудование и материалы:

1. Ролевые карточки с ситуациями.
2. Презентация.
3. Раздаточные материалы с рекомендациями.

Ход урока:

Этап	Содержание	Время	Методы и формы работы
Организационный момент	Приветствие, постановка задач урока	5 мин	Фронтальная беседа
Изучение нового материала	Объяснение понятия социальной инженерии, примеры атак	10 мин	Лекция с презентацией

Ролевая игра	Разделение на группы «мошенники» и «жертвы», разыгрывание сценариев	20 мин	Ролевая игра, работа в группах
Анализ и обсуждение	Разбор действий, выявление эффективных способов защиты	10 мин	Обсуждение, рефлексия
Итог урока	Выводы, рекомендации по защите	5 мин	Фронтальное обсуждение
Домашнее задание	Подготовить памятку с советами по противодействию социальной инженерии	–	Индивидуальная работа

Технологическая карта урока 4.

Тема: Практические навыки безопасного пользования интернетом

Класс: 10–11.

Продолжительность: 45 минут.

Цели урока:

1. Отработать навыки безопасного поведения в интернете.
2. Научить распознавать подозрительные сайты и сообщения.
3. Формировать критическое мышление при работе с информацией.

Планируемые результаты:

1. Учащиеся смогут оценивать безопасность сайтов.
2. Будут знать, как действовать при подозрительной активности.
3. Осознают важность критического отношения к информации.

Оборудование и материалы:

1. Компьютеры с доступом в интернет.
2. Примеры сайтов и писем (скриншоты).
3. Презентация.

Ход урока:

Этап	Содержание	Время	Методы и формы работы
Организационный момент	Приветствие, цель урока	5 мин	Фронтальная беседа
Изучение нового материала	Критерии оценки безопасности сайтов и сообщений	10 мин	Лекция с презентацией
Практическое задание	Анализ примеров сайтов и писем, выявление угроз	20 мин	Работа в группах, обсуждение

Итог урока	Обсуждение результатов, правила безопасного поведения	5 мин	Общий разбор, рефлексия
Домашнее задание	Подготовить рекомендации по безопасному использованию интернета	–	Индивидуальная работа

Эти технологические карты можно адаптировать и расширять в зависимости от уровня подготовки учащихся и целей учебного курса.

Включение интерактивных заданий и практических упражнений способствует лучшему усвоению материала и развитию критического мышления.

Ниже приведены тесты для проверки знаний по каждому из четырех уроков, основанных на технологических картах.

Тесты включают вопросы с выбором ответа, множественным выбором и ситуационные задачи.

Тест по уроку 1: Введение в кибербезопасность (7–8 классы)

1. Что такое кибербезопасность?

a) Защита от вирусов только на домашнем компьютере

b) Защита информации и систем в цифровом мире

c) Установка игр на компьютер

d) Использование интернета для общения

2. Какие из перечисленных угроз относятся к кибербезопасности? (Выберите все правильные варианты)

a) Вирусы

b) Фишинг

c) Погодные условия

d) Мошенничество в интернете

3. Что нужно делать, если вы получили подозрительное письмо с просьбой перейти по ссылке?

a) Перейти по ссылке и ввести свои данные

b) Удалить письмо и не переходить по ссылке

c) Переслать письмо всем друзьям

d) Сохранить письмо на компьютере

4. Почему важно соблюдать правила безопасного поведения в интернете?

a) Чтобы не потерять друзей

b) Для защиты личных данных и предотвращения мошенничества

c) Чтобы быстрее скачать фильмы

d) Чтобы играть в онлайн-игры

Тест по уроку 2: Создание надежных паролей и защита личных данных (8–9 классы)

1. Какой из паролей является наиболее надежным?

a) 123456

b) пароль

c) P@ssw0rd!2024

d) qwerty

2. Какие правила помогут создать надежный пароль? (Выберите все правильные варианты)

a) Использовать буквы разного регистра (большие и маленькие)

b) Использовать дату рождения

c) Сочетать буквы, цифры и специальные символы

d) Использовать простые слова из словар

3. Зачем нужно защищать личные данные в интернете?

a) Чтобы избежать кражи личной информации

b) Чтобы получить больше подписчиков

c) Чтобы не потерять телефон

d) Чтобы быстрее загрузить сайты

4. Что из перечисленного НЕ следует размещать в открытом доступе в интернете?

a) Фамилию и имя

b) Любимые фильмы

c) Пароли и номера банковских карт

d) Хобби и интересы

Тест по уроку 3: Социальная инженерия и методы защиты (9–11 классы)

1. Что такое социальная инженерия?

a) Метод программирования

b) Психологические методы получения конфиденциальной информации путем обмана или манипуляции

c) Вирус, который разрушает файлы

d) Антивирусная программа

2. Какие из действий могут быть признаками социальной инженерии? (Выберите все правильные варианты)

a) Незнакомец просит сообщить пароль

b) Коллега просит помощь с документом

c) Звонок от “службы безопасности” с просьбой подтвердить личные данные

d) Получение письма с предложением выиграть приз

3. Как следует реагировать на подозрительные попытки получить вашу информацию?

a) Сразу передать информацию

b) Игнорировать и проверить информацию через официальные каналы

c) Поделиться с друзьями

d) Позвонить мошеннику обратно

4. Какой способ поможет защититься от социальной инженерии?

a) Постоянно менять пароли и не сообщать их никому

b) Открывать все входящие письма

c) Использовать простой пароль

d) Принимать все звонки и сообщения без вопросов

Тест по уроку 4: Практические навыки безопасного пользования интернетом (10–11 классы)

1. Что из перечисленного является признаком небезопасного сайта?

a) Наличие защищённого протокола HTTPS

b) Появление всплывающих окон с просьбой скачать неизвестный файл

c) Чистый и понятный дизайн

d) Официальный адрес сайта

2. Какие действия нужно предпринять, если вы получили подозрительное письмо с незнакомой ссылкой?

a) Сразу перейти по ссылке

b) Удалить письмо и не открывать ссылки

c) Переслать письмо друзьям

d) Сохранить письмо для просмотра позже

3. Как оценить безопасность сайта? (Выберите все правильные варианты)

a) Проверить наличие HTTPS в адресной строке

b) Обратить внимание на дизайн сайта

c) Проверить отзывы о сайте в интернете

d) Вводить личные данные, не проверяя сайт

4. Почему важно критически относиться к информации в интернете?

a) Чтобы верить всему подряд

b) Чтобы не стать жертвой мошенников и не распространять ложные данные

c) Чтобы быстро загружать страницы

d) Чтобы играть в игры онлайн

Ключи для ответов:

Урок 1: 1b, 2a,b,d, 3b, 4b

Урок 2: 1c, 2a,c, 3a, 4c

Урок 3: 1b, 2a,c,d, 3b, 4a

Урок 4: 1b, 2b, 3a,c, 4b

Эти тесты помогут объективно оценить уровень знаний учащихся по ключевым аспектам кибербезопасности, соответствующим целям уроков.

Часть 5. Методика преподавания основ кибербезопасности в школе

Методика преподавания основ кибербезопасности в школе, основанная на представленных технологических картах уроков, предполагает поэтапное и системное освоение учащимися ключевых знаний и практических навыков, необходимых для безопасного поведения в цифровом пространстве.

Рассмотрим основные особенности и подходы к организации учебного процесса по каждой из карт.

1. Введение в кибербезопасность (7–8 классы).

Методика:

Урок строится на активном вовлечении учащихся через обсуждения и практические кейсы.

На этапе актуализации знаний педагог стимулирует учеников поделиться своими представлениями об угрозах в интернете, что помогает выявить исходный уровень понимания и повысить мотивацию к изучению темы.

Лекция с презентацией подаёт теоретический материал доступно и наглядно, используя иллюстрации и примеры, что способствует лучшему усвоению.

Практическое задание – разбор кейса с подозрительным письмом – позволяет учащимся применить полученные знания, отрабатывая навыки распознавания угроз. Рефлексия в конце урока закрепляет материал и выявляет пробелы.

2. Создание надежных паролей и защита личных данных (8–9 классы)

Методика:

Задача урока – не только дать теорию, но и развить практические умения. После обсуждения опыта учащихся с паролями преподаватель демонстрирует правила создания надёжных паролей и типичные ошибки.

Использование компьютеров или планшетов для самостоятельной работы с онлайн-сервисами проверки паролей обеспечивает интерактивность и практическую направленность урока.

Обсуждение результатов помогает закрепить правильные подходы и понять риски.

Домашнее задание – подготовка памятки – способствует систематизации знаний и развитию коммуникативных навыков.

3. Социальная инженерия и методы защиты (9–11 классы)

Методика:

Урок ориентирован на развитие критического мышления и навыков самозащиты от психологических воздействий. Теоретическая часть вводит понятие социальной инженерии на примерах. Основная часть – ролевая игра, где учащиеся делятся на группы и разыгрывают сценарии «мошенников» и «жертв». Такой активный метод способствует глубокому пониманию механизмов манипуляции и отработке навыков противодействия в реальных ситуациях. Анализ и рефлексия после игры позволяют осмыслить опыт и сформулировать эффективные рекомендации. Домашнее задание направлено на закрепление навыков и создание собственного памятного материала.

4. Практические навыки безопасного пользования интернетом (10–11 классы)

Методика:

Данный урок развивает умения анализа и критической оценки информации и ресурсов интернета. Лекция знакомит с критериями оценки безопасности сайтов и сообщений, формируя теоретическую базу. Практическое задание в группах по анализу реальных примеров способствует развитию навыков распознавания угроз и совместного принятия решений. Итоговая рефлексия позволяет обобщить опыт и сформулировать правила безопасности. Домашнее задание помогает закрепить знания и развить навыки самостоятельной работы с информацией.

Общие методические принципы:

1. Интерактивность и активное участие учащихся – обсуждения, мозговые штурмы, ролевая игра и практические задания способствуют вовлечению и мотивации.

2. Наглядность и доступность подачи материала – использование презентаций, иллюстраций и реальных примеров облегчает понимание сложных понятий.

3. Практическая направленность – за счет кейсов, самостоятельного создания паролей, ролевых игр и анализа реальных ситуаций ученики учатся применять знания на практике.

4. Рефлексия и обратная связь – обсуждения итогов урока и устные опросы помогают закрепить материал и выявить зоны для доработки

5. Дифференцированный подход – материал и задания адаптированы под возрастные особенности и уровень подготовки учащихся.

Домашние задания направлены на систематизацию знаний и развитие навыков самостоятельной работы.

Таким образом, методика преподавания основывается на сочетании теоретического материала с разнообразными интерактивными и практическими формами обучения, что обеспечивает всестороннее формирование у школьников компетенций в области кибербезопасности и готовит их к безопасному и ответственному поведению в цифровом мире.

Часть 6. Ресурсы и рекомендации по теме «Преподавание основ кибербезопасности в школе»

1. Баланов А. Н. Комплексная информационная безопасность. Полный справочник специалиста. Практическое пособие. М.: Инфра-Инженерия. 2024. 156 с.

2. Барков А.В., Киселев А.С. Влияние цифровизации на правовое обеспечение информационной безопасности государства и бизнеса в условиях современных геополитических вызовов // Безопасность бизнеса. 2022. N 3. С. 3 — 7.

3. Барков А.В., Киселев А.С. О правовом обеспечении безопасности информационно-телекоммуникационной инфраструктуры банков и государственных структур // Банковское право. 2022. N 4. С. 20 — 27.

4. Безкоровайный М. М., Татузов А. Л. Кибербезопасность подходы к определению понятия // Вопросы кибербезопасности. – 2014. – №. 1 (2). – С. 22-27. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-podhody-k-opredeleniyu-ponyatiya

5. Безопасность: теория, парадигма, концепция, культура. Словарь-справочник / Автор-сост. профессор В.Ф. Пилипенко. 2 е изд., доп. и перераб. – М.: ПЕР СЭ-Пресс, 2008.

6. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учебное пособие – М.: Горячая линия – Телеком, 2006

7. Белоус, А. И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения : практическое пособие / А. И. Белоус. - Москва ; Вологда : Инфра-Инженерия, 2020. - 644 с. - ISBN 978-5-9729-0512-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1167734 (дата обращения: 13.11.2025). – Режим доступа: по подписке.

8. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : научно-популярное издание / А. И. Белоус, В. А.

Солодуха. - 2-е изд. - Москва ; Вологда : Инфра-Инженерия, 2025. - 692 с. - ISBN 978-5-9729-2520-9. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2226293 (дата обращения: 13.11.2025). – Режим доступа: по подписке.

9. Бондарев В. В. Введение в информационную безопасность автоматизированных систем. М.: МГТУ им. Н. Э. Баумана. 2024. 252 с.

10. Бородакий Ю. В., Добродеев А. Ю., Бутусов И. В. Кибербезопасность как основной фактор национальной и международной безопасности XX! века (часть 1) // Вопросы кибербезопасности. – 2013. – №. 1. – С. 2-9. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-kak-osnovnoy-faktor-natsionalnoy-i-mezhdunarodnoy-bezopasnosti-hh-veka-chast-1

11. Ванина, А. Г. Персональная кибербезопасность : учебное пособие (курс лекций) / А. Г. Ванина, Д. В. Орел, С. В. Аникуев. - Ставрополь : Изд-во СКФУ, 2022. - 137 с. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2133410 (дата обращения: 13.11.2025). – Режим доступа: по подписке.

12. Васильева Т. Ю., Куприянов А. И., Мельников В. П. Информационная безопасность. Учебник. М.: КноРус. 2023. 372 с.

13. Галыгина Л. В., Галыгина И. В. Социальные аспекты информационной безопасности. Лабораторный практикум. М.: Лань. 2021. 64

14. Гришина Н. В. Основы информационной безопасности предприятия. Учебное пособие. М.: Инфра-М. 2021. 216 с.

15. Гродзенский Я. С. Информационная безопасность. Учебное пособие. М.: РГ-Пресс. 2024. 144 с.

16. Диогенес, Ю. Кибербезопасность: стратегии атак и обороны : практическое руководство / Ю. Диогенес, Э. Озкайя ; пер. с анг. Д. А. Беликова. - Москва : ДМК Пресс, 2020. - 326 с. - ISBN 978-5-97060-709-1. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1908427 (дата обращения: 13.11.2025). – Режим доступа: по подписке.

17. Добродеев А. Ю. Кибербезопасность в Российской Федерации. Модный термин или приоритетное технологическое направление обеспечения национальной и международной безопасности XXI века // Вопросы кибербезопасности. – 2021. – №. 4 (44). – С. 61-72. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-v-rossiyskoy-federatsii-modnyy-termin-ili-prioritetnoe-tehnologicheskoe-napravlenie-obespecheniya-natsionalnoy-i

18. Дубень А.К. Международное сотрудничество в сфере информационной безопасности: общая характеристика и российский подход к изучению // Международное право и международные организации. 2022. N 1. С. 24 — 30.

19. Дубень А.К. Опыт международного сотрудничества в сфере информационной безопасности: проблемы и перспективы // Международное право и международные организации. 2023. N 3. С. 13 — 19.

20. Дугенец А.С., Павлова Л.В. Государственное регулирование обеспечения информационной безопасности несовершеннолетних как составляющая национальной безопасности России // Административное право и процесс. 2023. N 5. С. 22 — 25.

21. Еремин А. Л. Информационная и цифровая гигиена. М.: Лань. 2023. 92 с.

22. Жарова А.К. Защита информации ограниченного доступа, получаемой по цифровым каналам передачи информации о совершаемых коррупционных правонарушениях // Государственная власть и местное самоуправление. 2023. N 9. С. 37 — 41.

23. Зенков А. В. Информационная безопасность и защита информации. М.: Юрайт. 2023. 108 с.

24. Зенков А. В. Основы информационной безопасности. Учебное пособие. М.: Инфра-Инженерия. 2022. 104 с.

25. Иванова С.В. Защита информации // СПС КонсультантПлюс. 2024.

26. Информационная безопасность (2 я книга социально-политического проекта «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009.

27. Кабанов А. С. Основы информационной безопасности. М.: Academia. 2021. 320 с.

28. Казарин О. В., Шубинский И. Б. Основы информационной безопасности: надежность и безопасность программного обеспечения. М.: Юрайт. 2023. 343 с.

29. Как организации защитить конфиденциальную информацию // СПС КонсультантПлюс. 2024.

30. Ковалев А. А., Балашов А. И. Международно-правовые аспекты политики кибербезопасности некоторых европейских стран бывшего советского блока // Вестник Поволжского института управления. – 2018. – Т. 18. – №. 5. – С. 105-114. URL: https://cyberleninka.ru/article/n/mezhdunarodno-pravovye-aspekty-politiki-kiberbezopasnosti-nekotoryh-evropeyskih-stran-byvshego-sovetskogo-bloka

Заключение

Таким образом, методика преподавания основ кибербезопасности в школе требует комплексного подхода, включающего теоретические знания, практические навыки и активное взаимодействие между всеми участниками образовательного процесса.

Обучение кибербезопасности не только защищает детей от угроз, но и подготавливает их к осознанному и безопасному поведению в цифровом мире.

В данной работе подробно рассмотрены ключевые аспекты, связанные с преподаванием основ кибербезопасности в школе, что обеспечивает комплексный подход к формированию у учащихся необходимых знаний, умений и навыков для безопасного поведения в цифровом пространстве.

В Части 1 представлен теоретический материал, который включает несколько важных подразделов.

В разделе 1.1 раскрывается взаимосвязь между информационной безопасностью и кибербезопасностью, что позволяет понять общие цели и специфику каждой из областей.

В разделе 1.2 даны основные понятия кибербезопасности, что формирует базовую терминологическую основу для дальнейшего изучения темы.

Раздел 1.3 посвящён описанию основных угроз кибербезопасности, таких как вирусы, фишинг, социальная инженерия и другие, что помогает осознать масштабы и виды рисков в цифровом мире.

В разделе 1.4 рассмотрены методы защиты, включая технические и организационные меры, направленные на предотвращение и минимизацию негативных последствий атак.

Часть 2 содержит практические задания, которые направлены на закрепление теоретических знаний через активное участие учащихся. Эти задания способствуют развитию навыков распознавания угроз, создания надежных паролей, а также выработке правильного поведения в различных ситуациях, связанных с безопасностью в интернете.

В Части 3 представлены оценочные материалы, включающие тесты и проекты, предназначенные для объективной проверки знаний и умений учащихся. Такие материалы позволяют систематически оценивать уровень усвоения материала и эффективность преподавания.

Часть 4 содержит технологические карты уроков по теме «Кибербезопасность», которые подробно описывают структуру занятий, цели, планируемые результаты, используемые методы и формы работы. Это облегчает подготовку и проведение уроков, обеспечивая последовательное и логичное изложение материала, а также включение интерактивных методов обучения.

В Части 5 раскрывается методика преподавания основ кибербезопасности в школе, основанная на сочетании теоретических знаний и практических навыков.

Особое внимание уделяется активным формам работы, таким как:

– ролевые игры,

– обсуждения,

– анализ кейсов и практические упражнения.

Это способствует формированию критического мышления и ответственного отношения к безопасному использованию цифровых технологий.

Наконец, в Части 6 приведены ресурсы и рекомендации для преподавателей, которые включают полезные материалы, онлайн-платформы и методические пособия.

Данные рекомендации помогают организовать учебный процесс более эффективно, а также поддерживать интерес учащихся к теме кибербезопасности.

Таким образом, работа охватывает все необходимые компоненты для успешного внедрения и преподавания основ кибербезопасности в школьной программе, сочетая:

– теоретическую базу,

- практические навыки,
- оценочные инструменты,
- методическую поддержку педагогов.