11 КЛАСС ОБЗР

Опасности, связанные с ПО — конспект урока

Автор Глеб Беломедведев

ЯНВ 17, 2025 #безопасность, #видео, #вирус, #данные, #защита, #интеллект-карта, #интересные факты, #карта памяти, #компьютер, #кроссворд, #ментальная карта, #облако слов, #опасность, #полезные советы, #презентация, #рабочий лист, #таблица, #тесты, #технологическая карта, #чек-лист 19 фото Время прочтения: 36 минут(ы)

Содержание [Скрыть]

Опасности, связанные с использованием программного обеспечения — конспект урока ОБЗР (Основы безопасности и защиты Родины)

Вступление

> ***В современном мире каждый школьник проводит в цифровом пространстве больше времени, чем в реальном. Но знаете ли вы, что по статистике каждый третий подросток становится жертвой киберпреступников? В этом конспекте вы найдете не только актуальный материал по информационной безопасности, но и комплект методических материалов: технологическую и интеллект-карту, бесплатную презентацию, тестовые задания, рабочие листы и кроссворд для закрепления знаний.***

История

Классный руководитель

5 класс

6 класс

7 класс

8 класс

9 класс

10 класс

11 класс

Профориентационные уроки

Математика

Музыка

Начальная школа

ОБЗР

8 класс

9 класс

10 класс

11 класс

Обществознание

Право

Психология

Русская литература

Русский язык

Технология (Труды)

Физика

Физкультура

Химия

Экология

Экономика

Копилка учителя

Сценарии школьных праздников

ИНТЕРЕСНОЕ

Выберите похожие названия

- Методическая разработка: «Кибербезопасность и защита персональных данных»
- Открытый урок: «Информационные угрозы современного мира»
- Интегрированное занятие: «Цифровая гигиена и информационная безопасность»
- Практикум: «Защита от вредоносных программ и социальной инженерии»

Возраст учеников

16-17 лет

Класс

11 класс

Календарно-тематическое планирование

КТП по ОБЗР 11 класс

Модуль

Модуль № 10 «Безопасность в информационном пространстве» (7 часов)

УМК (Учебно-методический комплекс)

[укажите название своего УМК по которому Вы работаете]

Учебник

[укажите название своего учебника]

Дата проведения

[укажите дату проведения]

Длительность

45 минут (1 академический час)

Вид

Комбинированный

Тип

Изучение нового материала с элементами практической работы

Форма проведения

Занятие-практикум с элементами дискуссии

Цель

- Сформировать у обучающихся комплексное представление об опасностях, связанных с использованием программного обеспечения, и способах защиты от них.

Задачи

- **Обучающая:** Сформировать знания о видах вредоносного ПО и методах защиты от него
- **Развивающая:** Развить навыки критического мышления при работе в цифровом пространстве
- **Воспитательная:** Воспитать ответственное отношение к информационной безопасности

Универсальные учебные действия (УУД)

- **Личностные УУД:** Формирование ответственного отношения к собственной информационной безопасности
- **Регулятивные УУД:** Умение оценивать риски и принимать решения в нестандартных ситуациях
- **Познавательные УУД:** Развитие навыков анализа информационных угроз
- **Коммуникативные УУД:** Развитие умения работать в команде при решении практических задач
- **Метапредметные УУД:** Формирование целостного представления о безопасности в цифровом мире

Методические приёмы, педагогические методы, технологии обучения

- Кейс-метод
- Интерактивный опрос
- Мозговой штурм
- Критический анализ
- Метод проблемного изложения
- Работа в малых группах

Ожидаемые результаты

- **Личностные:** Осознание значимости информационной безопасности
- **Метапредметные:** Умение анализировать и оценивать информационные угрозы
- **Предметные:** Владение основными методами защиты от вредоносного ПО

Предварительная работа педагога

- Подготовка презентации
- Разработка практических заданий и кейсов
- Создание раздаточного материала
- Составление тестов, кроссворда, облака слов
- Разработка технологической и интеллект-карты
- Создание рабочих листов для учащихся
- Поиск видеоуроков и видеороликов

Оборудование и оформление кабинета

- Компьютер с проектором
- Интерактивная доска
- Раздаточный материал
- Плакаты
- Рабочие места с компьютерами для практической работы

Ход занятия / Ход мероприятия

Организационный момент

Здравствуйте, ребята! Рада всех вас видеть. Давайте проверим, кто сегодня присутствует на занятии. Староста, пожалуйста, отметьте отсутствующих в журнале.

После переклички.

Отлично, теперь проверим вашу готовность. На партах должны быть: учебник, рабочая тетрадь, ручка и карандаш. Проверьте, пожалуйста, всё ли у вас есть… Вижу, что все подготовились к занятию ответственно.

Обратите внимание на свой внешний вид — форма должна быть в порядке, а длинные волосы — аккуратно убраны. Это важно не только для дисциплины, но и для вашей собственной безопасности во время практических занятий.

Дежурные, будьте добры, подготовьте проекционный экран к работе. Убедитесь, что он хорошо виден со всех парт.

Напоминаю правила поведения: мы внимательно слушаем друг друга, не перебиваем, поднимаем руку, если хотим что-то сказать или спросить. Во время практической работы соблюдаем технику безопасности. И ещё одна важная просьба — пожалуйста, переведите ваши телефоны в беззвучный режим и уберите их в сумки. Они нам сегодня не понадобятся, а вот отвлекать могут существенно.

С улыбкой.

Я вижу, что сегодня у всех хорошее настроение, и это замечательно! Уверена, что наше занятие будет интересным и продуктивным. Вы — замечательный класс, и я знаю, что вместе мы сможем разобраться даже в самых сложных вопросах. Готовы начать? Тогда не будем терять ни минуты!

Актуализация усвоенных знаний

Прежде чем мы перейдем к новой теме, давайте вспомним, о чём мы говорили на прошлом занятии. Мы изучали тему «Безопасность в цифровой среде» и сегодня эти знания станут для нас важным фундаментом.

Анна, расскажите, пожалуйста, что такое цифровая среда и какую роль она играет в современном мире?

После ответа.

Отлично! Действительно, электронная среда стала неотъемлемой частью нашей жизни, и очень важно понимать, как в ней правильно существовать.

Михаил, а что такое цифровой след? Какие данные о нас остаются в интернете?

Ученик отвечает.

Верно! И каждый раз, когда мы пользуемся интернетом, наш цифровой след становится всё более заметным.
Давайте подумаем вместе: почему цифровую зависимость считают современной угрозой? Кто готов поделиться своими мыслями?

Выслушивает ответы.

Очень глубокие рассуждения! Особенно важно, что вы отметили влияние интернет-зависимости на психическое здоровье.

Елена, назовите, пожалуйста, основные угрозы, которые могут подстерегать нас в электронном мире?

После ответа.

Прекрасно! Вы очень хорошо запомнили эти важные моменты.

А теперь давайте вместе подумаем над таким вопросом: как связаны между собой информационная безопасность личности и культура поведения в цифровой среде?

Педагог организует короткое обсуждение.

Замечательно! Ваши ответы показывают, что вы действительно понимаете важность осознанного и ответственного поведения в сети.

И последний вопрос: какие основные правила безопасного поведения в цифровой среде мы с вами обсуждали? Давайте вспомним вместе.

Выслушивает ответы, дополняет при необходимости.

Отлично! Я вижу, что материал прошлого занятия вы усвоили очень хорошо. Эти знания пригодятся нам сегодня, потому что мы будем углубляться в один из важнейших аспектов цифровой безопасности.

Вступительное слово учителя

Ребята, каждый из вас наверняка уже установил не один десяток программ на свой смартфон или компьютер. Игры, мессенджеры, приложения для учёбы и развлечений – всё это делает нашу жизнь удобнее и интереснее. Но задумывались ли вы когда-нибудь, что программное обеспечение может быть не только полезным, но и опасным?

Демонстрирует на экране новостную статистику.

Взгляните на эти цифры: только за прошлый год было зарегистрировано более миллиона случаев заражения устройств вредоносными программами. Причём среди пострадавших немало ваших ровесников. Как вы думаете, почему именно подростки часто становятся жертвами киберпреступников?

Выслушивает несколько ответов.

Действительно, молодые люди чаще скачивают новые приложения, активнее используют социальные сети, но при этом не всегда задумываются о безопасности. И сегодня мы с вами будем говорить об очень важной теме.

Записывает на доске.

Тема нашего урока: «Опасности, связанные с использованием программного обеспечения»

Эти знания помогут вам защитить не только свои устройства, но и личные данные, а возможно, даже финансы вашей семьи. Потому что современные вредоносные программы становятся всё изощрённее, а их создатели – всё хитрее в попытках обмануть пользователей.

На этом занятии мы разберём основные виды вредоносного программного обеспечения, узнаем, как оно попадает на наши устройства, и самое главное – научимся эффективно защищаться от этих угроз. Готовы погрузиться в мир кибербезопасности?

> ***Цитата:***
> ***«Как только вы теряете бдительность в сети, появляются скрытые угрозы, которые могут повлиять на вашу жизнь.»***
> ***— М.В. Костина, 1992–н.в., специалист по угрозам в сети, преподаватель цифровых дисциплин***

Оглядывает класс с воодушевляющей улыбкой.

Тогда начнём наше путешествие в мир цифровой безопасности!

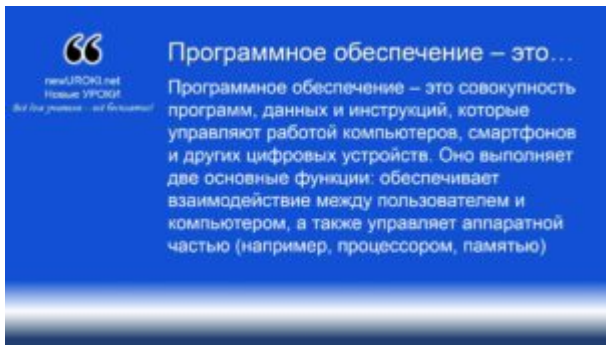
Основная часть

Иллюстративное фото / newUROKI.net

Вредоносное программное обеспечение: основные понятия и определения

Определение

> ***Программное обеспечение – это*** *совокупность программ, данных и инструкций, которые управляют работой компьютеров, смартфонов и других цифровых устройств. Оно выполняет две основные функции: обеспечивает взаимодействие между пользователем и компьютером, а также управляет аппаратной частью (например, процессором, памятью).*

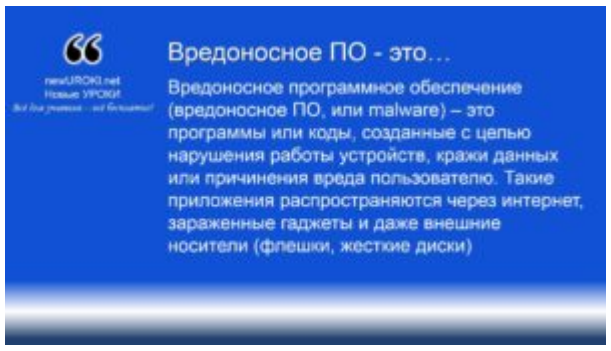


Определение

Без программного обеспечения современные гаджеты не могут выполнять даже самые простые задачи – от работы калькулятора до сложных научных расчетов.

Понятие вредоносного программного обеспечения

> ***Вредоносное программное обеспечение (вредоносное ПО, или malware*) – это программы или коды, созданные с целью нарушения работы устройств, кражи данных или причинения вреда пользователю. Такие приложения распространяются через интернет, зараженные гаджеты и даже внешние носители (флешки, жесткие диски).***



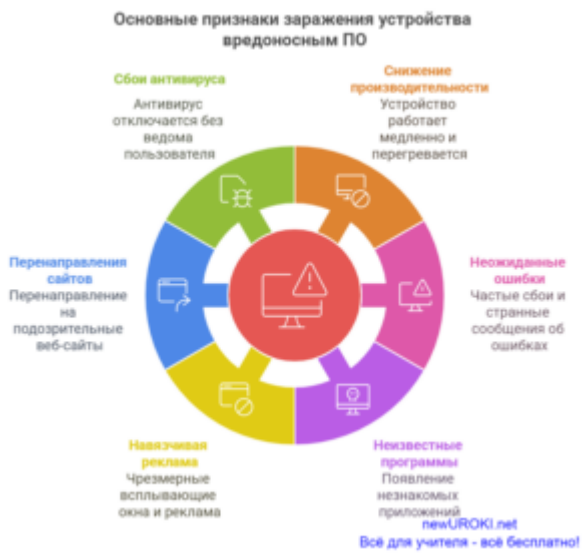
Определение

Цель такого ПО – нанести ущерб пользователю или его устройству, похитить данные или получить несанкционированный доступ к системе.

> ***Вредоносная программа (другие термины: зловредная программа, вредонос, зловред; англ. malware — словослияние слов malicious и software (рус. малварь)) — любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путём копирования, искажения, удаления или подмены информации. Рувики***

Основные признаки заражения устройства вредоносным ПО

- **Снижение производительности.** Компьютер или телефон начинают работать медленнее, приложения долго открываются, устройство перегревается.
- **Неожиданные ошибки или сбои.** На экране могут появляться странные сообщения, приложения неожиданно закрываются, система «зависает».
- **Появление неизвестных программ.** Пользователь замечает, что на устройстве установлены утилиты, которые он не скачивал.
- **Навязчивая реклама.** Часто открываются всплывающие окна или реклама, даже если пользователь не находится в браузере.
- **Перенаправление на подозрительные сайты.** При попытке открыть один сайт, пользователь оказывается на другом, часто мошенническом.
- **Сбои в работе антивируса.** Антивирус может быть отключен или вообще удален, что сигнализирует о попытке маскировки вирусного ПО.



Инфографика / newUROKI.net

История появления и развития вредоносных программ

Первое вредное программное обеспечение появилось в 1970-х годах, когда компьютерные сети только начали развиваться. Одной из первых известных программ был «червь Морриса», созданный в 1988 году студентом Робертом Моррисом. Этот червь распространился через сеть ARPANET (предшественник интернета) и вывел из строя тысячи компьютеров.

В 1990-е годы с развитием интернета опасное ПО стало более распространенным. Вирусы распространялись через электронную почту, зараженные файлы и веб-сайты. Примером может быть вирус Melissa (1999 год), который рассылал зараженные письма через адресные книги пользователей.

В 2000-х годах вирусные утилиты стали более сложными. Появились программы-вымогатели, такие как WannaCry, которые блокировали доступ к данным и требовали выкуп. В этот же период возникли трояны – программы, маскирующиеся под полезные приложения, но выполняющие разрушительные действия.

Сегодня такое ПО может использоваться не только хакерами, но и целыми кибергруппировками для проведения кибератак, шпионажа и вымогательства. Благодаря развитию технологий, такие зловредные утилиты могут атаковать не только компьютеры, но и умные приборы, включая бытовую технику.

Стоит прочесть также: [Профилактика и первая помощь при отравлениях - конспект урока]

Вирусное ПО остается серьезной угрозой, поскольку с каждым годом оно становится более сложным, а методы его распространения – более изощренными. Именно поэтому важно уметь распознавать угрозы и защищать свои устройства.

Классификация вредоносного программного обеспечения

Иллюстративное фото / newUROKI.net

Компьютерные вирусы и их разновидности

Компьютерные вирусы – это специальные коды или файлы, способные самостоятельно внедряться в другие приложения или системные компоненты и распространяться по устройству или сети. Их цель – нарушить нормальную работу системы, уничтожить информацию или использовать ресурсы устройства для выполнения несанкционированных действий.

Основные виды вирусов:

- **Файловые вирусы.** Инфицируют исполняемые файлы (например, с расширением .exe) и активируются при их запуске.

- **Загрузочные вирусы.** Проникают в загрузочные сектора дисков и активируются при запуске устройства.
- **Макровирусы.** Поражают документы офисных приложений (например, Word или Excel) через встроенные макросы.
- **Полиморфные вирусы.** Эти зловредные элементы могут изменять свой код, чтобы обходить антивирусные программы.
- **Резидентные вирусы.** Оседают в памяти и остаются активными даже после завершения зараженного приложения.

Инфографика / newUROKI.net

Троянские программы и их особенности

Трояны – это вредоносные элементы, которые маскируются под безвредные приложения. Пользователь сам устанавливает такие утилиты, думая, что они полезны, например, текстовые редакторы, игры или утилиты. Однако после установки они выполняют действия, угрожающие безопасности системы.

Особенности троянов:

- Они «не размножаются» самостоятельно.
- Часто используются для кражи данных (логины, пароли, банковские реквизиты).
- Могут предоставлять удаленный доступ к системе злоумышленникам.

Примеры: Трояны-банкиры, которые крадут данные банковских карт, и трояны-шпионы, следящие за действиями пользователя.

Программы-шпионы (спайвер)

Шпионское ПО – это инструменты, предназначенные для сбора информации о человеке без его ведома. Обычно такие утилиты собирают данные о привычках пользователя в интернете, посещаемых сайтах, вводимых паролях и логинах.

Основные признаки наличия шпионского кода:

- Увеличение числа рекламы или всплывающих окон.
- Перенаправление поисковых запросов на неизвестные сайты.
- Замедление работы системы из-за постоянной передачи данных злоумышленнику.

Примеры шпионов: кейлоггеры, фиксирующие нажатия клавиш, или скрытые сканеры, следящие за использованием веб-камеры.

Программы-вымогатели (рансомвар*)

Вымогательское ПО – это один из самых опасных типов вредоносного кода, который блокирует доступ к файлам человека или шифрует их. Чтобы вернуть доступ, злоумышленники требуют выкуп.

> ***Программа-вымогатель, программа-шантажист** (англ. ransomware — контаминация слов ransom — выкуп и software — программное обеспечение, винлокер (англ. winlocker — блокировщик Windows) — тип зловредного программного обеспечения, предназначен для вымогательства, блокирует доступ к компьютерной системе или предотвращает считывание записанных в нём данных (часто с помощью методов шифрования), а затем требует от жертвы выкуп для восстановления исходного состояния. Википедия*

Принцип работы рансомвара:

- Опасный код попадает на устройство (чаще всего через электронную почту или зараженные сайты).
- После активации он шифрует важные файлы, такие как документы, фотографии, видео.
- Пользователь получает сообщение с требованием выкупа, обычно в криптовалюте.

Последствия: даже после оплаты злоумышленники не всегда возвращают доступ к файлам и информации. Именно поэтому важно регулярно создавать резервные копии.

Рекламное ПО (адвер)

Рекламные приложения – это вредоносные модули, которые навязчиво демонстрируют рекламу, перенаправляют пользователя на рекламные сайты или устанавливают дополнительные нежелательные утилиты.

Признаки адвера:

- Частое появление баннеров и всплывающих окон.
- Установка приложений, которые пользователь не скачивал.
- Замедление работы браузера и других приложений.

Хотя такое ПО может показаться менее опасным, оно часто служит «входной точкой» для более серьезных угроз, таких как трояны или шпионы.

Все вредоносные инструменты имеют разные цели и механизмы работы, но общий принцип их действия – навредить человеку или извлечь выгоду для злоумышленников. Чтобы минимизировать риски заражения, важно понимать основные характеристики каждого типа угроз и соблюдать правила цифровой безопасности.

Таблица: Типы угроз и их примеры

Угроза	Пример
Вирусы	Самораспространяющиеся файлы
Трояны	Приложения с двойным назначением
Шпионские приложения	Мониторинг клавиатуры
Рекламные приложения	Постоянные всплывающие окна
Фишинговые атаки	Ложные банковские страницы

Принципы работы вредоносного ПО

Иллюстративное фото / newUROKI.net

Механизмы заражения устройств

Для проникновения в устройство злоумышленники используют различные методы, которые помогают обмануть систему безопасности или человека.

Основные механизмы включают:

- Использование уязвимостей. Некорректно написанные программы или устаревшие версии операционных систем содержат ошибки, позволяющие опасному коду проникнуть внутрь без ведома владельца.
- Встраивание в файлы. Злонамеренные компоненты часто прячутся в документах, изображениях или мультимедийных файлах. При их открытии запускается скрытый процесс внедрения.
- Автоматический запуск. Некоторые угрозы активируются при подключении инфицированных флеш-накопителей или внешних дисков.

Способы распространения вредоносных программ

Способы распространения опасных инструментов разнообразны и постоянно развиваются.

Основные из них:

- **Электронная почта.** Одна из самых распространенных схем – отправка зараженных вложений или ссылок на опасные сайты. Чаще всего сообщения маскируются под официальные письма от банков, магазинов или государственных учреждений.
- **Сайты и загрузки.** Такие элементы могут быть интегрированы в файлы, доступные для скачивания на сомнительных веб-ресурсах. Иногда даже на первый взгляд безопасный сайт становится опасным из-за встроенных скриптов.
- **Социальные сети.** Злоумышленники используют поддельные аккаунты, чтобы рассылать ссылки на заражённый контент, заманивая людей, например, обещанием бесплатных подарков.
- **Подключение внешних носителей.** Инфицированные флешки и другие устройства часто становятся источником угрозы.
- **Маскировка под обновления.** Некоторые опасности представляются как обновления операционной системы или популярных приложений, что вводит пользователей в заблуждение.

Инфографика / newUROKI.net

Цели создателей вредоносного ПО

Мотивы, побуждающие злоумышленников создавать и распространять вредоносные коды, можно разделить на несколько групп:

- **Финансовая выгода.** Большинство атак нацелено на кражу средств, данных банковских карт или вымогательство денег у пользователей.
- **Сбор информации.** Программы часто используются для шпионажа, сбора личных данных, логинов и паролей.
- **Саботаж.** Некоторые атаки направлены на подрыв работы компаний или учреждений, например, путем шифрования их данных.
- **Демонстрация возможностей.** Некоторые хакеры создают угрозы для саморекламы, демонстрируя свои технические навыки.
- **Идеологические мотивы.** Вирусный код может быть частью кибервойны, нацеленной на дискредитацию определенных стран или организаций.

Последствия заражения для пользователя и устройства

Последствия атак вредоносного ПО могут быть как мелкими неудобствами, так и серьезными проблемами.

- **Утрата данных.** Вирусы могут удалять, шифровать или повреждать файлы, делая их недоступными для пользователя.
- **Кража личной информации.** Логины, пароли, данные банковских карт и личные переписки – все это становится доступным злоумышленникам.
- **Финансовые потери.** Мошеннические схемы могут привести к списанию денег с банковских карт или необходимости оплачивать восстановление данных.
- **Замедление работы гаджета.** Зараженные компьютеры начинают работать медленнее, перегреваться или внезапно перезагружаться.
- **Использование аппарата в бот-сетях.** Некоторые вирусы превращают устройства в часть глобальной сети для отправки спама или проведения кибератак.

Понимание принципов работы вредоносных программ помогает пользователям осознавать угрозы и защищать свои гаджеты. Соблюдение элементарных правил безопасности, таких как установка обновлений, использование надежных паролей и антивирусного софта, позволяет значительно снизить риск внедрения.

Кража персональных данных и методы социальной инженерии

Иллюстративное фото / newUROKI.net

Виды персональных данных и их ценность

Персональные данные – это информация, позволяющая идентифицировать человека. В современном цифровом мире такие сведения становятся одним из самых ценных ресурсов.

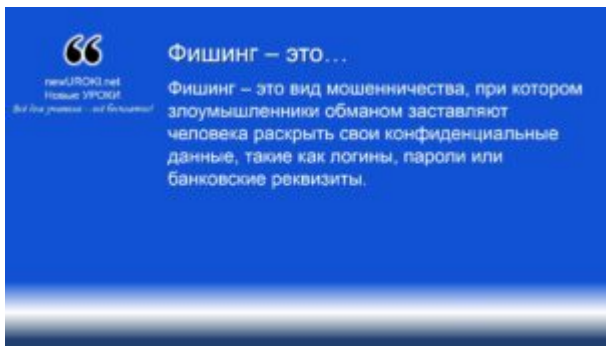
Они включают:

- **ФИО и контактные данные.** Телефонные номера, адреса электронной почты и домашние адреса часто используются злоумышленниками для рассылки спама или мошеннических сообщений.
- **Финансовые сведения.** Номера банковских карт, пароли, логины от интернет-банков и другая информация, связанная с денежными операциями, являются основной целью хакеров.
- **Идентификационные номера.** Паспортные сведения, номер СНИЛС, ИНН или медицинские полисы могут быть использованы для оформления кредитов или поддельных документов.
- **Личная информация.** Это сведения о хобби, предпочтениях, образе жизни, которые злоумышленники собирают для создания психологического портрета.

Ценность персональной информации обусловлена её применением в мошеннических схемах, продаже на теневых интернет-рынках или использовании для шантажа.

Фишинг: признаки и методы

> ***Фишинг – это** вид мошенничества, при котором злоумышленники обманом заставляют человека раскрыть свои конфиденциальные данные, такие как логины, пароли или банковские реквизиты.*



Определение

Методы фишинга:

- **Фальшивые письма.** Мошенники отправляют электронные сообщения, замаскированные под уведомления от банков, онлайн-магазинов или государственных служб.

- **Поддельные сайты.** Злоумышленники создают копии известных ресурсов, чтобы пользователь ввел свои сведения, не подозревая подвоха.
- **Ссылки в соцсетях.** Обманные ссылки могут быть замаскированы под акции или конкурсы.

Признаки фишинга:

- Ошибки в текстах сообщений (грамматические или стилистические).
- Ссылки, ведущие на подозрительные или неофициальные ресурсы.
- Требование срочно ввести личные сведения или пароль.

Социальная инженерия в сети

Социальная инженерия – это совокупность методов психологического воздействия, применяемых злоумышленниками для получения доступа к конфиденциальной информации. Основной акцент делается на слабостях человека, а не на технических уязвимостях системы.

Примеры методов социальной инженерии:

- **Притворство.** Мошенники выдают себя за сотрудников банка, технической поддержки или друзей жертвы, чтобы получить доступ к информации.
- **Создание чувства срочности.** Злоумышленники подталкивают жертву к поспешным действиям, например, к переходу по ссылке или вводу кода подтверждения.
- **Манипуляции доверием.** Использование фальшивых отзывов, фотографий или документов для завоевания доверия.

Эти методы широко применяются для получения доступа к социальным сетям, электронным почтам и даже корпоративным системам.

Распространенные схемы мошенничества

Современные киберпреступники используют разнообразные уловки.

Основные схемы включают:

- **Выманивание паролей.** Жертве предлагают ввести данные на поддельном сайте, обещая бонус или подарок.
- **Мошеннические звонки.** Сценарии могут варьироваться от «сотрудника банка», предупреждающего о подозрительных операциях, до «правоохранителей», требующих подтвердить личность.
- **Лотереи и розыгрыши.** Участникам сообщают о мнимом выигрыше, но для его получения нужно оплатить «комиссию».
- **Вирусы в виде обновлений.** Злоумышленники предлагают загрузить обновление или приложение, которое на самом деле является вредоносным кодом.
- **Мошенничество через объявления.** Ложные объявления на платформах продаж товаров или услуг, цель которых – получить аванс или предоплату.

Защита персональных данных требует внимательного отношения к каждому действию в цифровой среде. Пользователям важно проверять адреса сайтов, избегать ввода личных сведений на подозрительных ресурсах и не поддаваться на провокации мошенников. Знание основных схем социальной инженерии и фишинга помогает минимизировать риски и избежать неприятных последствий.

Комплексная защита от вредоносного ПО

Иллюстративное фото / newUROKI.net

В условиях цифровой эпохи пользователи регулярно сталкиваются с угрозами со стороны вредоносных приложений. Для минимизации рисков важно обеспечить комплексную защиту своих устройств, что включает использование специализированных инструментов и соблюдение правил безопасного поведения.

Антивирусные решения

Антивирусы – это специальные приложения, предназначенные для обнаружения, блокировки и удаления вредоносного кода.

Функции антивирусов:

- Мониторинг системы в реальном времени. Антивирус сканирует все действия на устройстве, включая запуск приложений, загрузку файлов и взаимодействие с сетью.
- Обнаружение угроз. Современные антивирусные решения используют базы сигнатур, а также технологии машинного обучения для выявления известных и новых угроз.
- Удаление вредоносного кода. Если угроза обнаружена, антивирус либо удаляет её автоматически, либо предлагает пользователю возможные действия.

Для максимальной эффективности антивирусного решения необходимо регулярно обновлять его базу, что позволяет защититься от самых последних угроз.

Файерволы и их настройка

Файерволы, или межсетевые экраны, являются существенным компонентом защиты гаджета. Они контролируют сетевой трафик, фильтруя входящие и исходящие соединения.

Роль файерволов в безопасности:

- **Фильтрация сетевых пакетов.** Файервол проверяет каждое подключение, определяя, безопасно ли оно.
- **Блокировка подозрительных соединений.** В случае обнаружения подозрительного трафика он немедленно блокируется.
- **Создание безопасной сети.** Файерволы защищают не только компьютеры, но и целые локальные сети.

При настройке файервола нужно указать разрешенные соединения, чтобы избежать блокировки необходимых программ.

Регулярное обновление систем и приложений

Одним из основных способов предохранения от заражения, является своевременное обновление операционных систем и установленного софта.

Почему они важны:

- **Закрытие уязвимостей.** Разработчики регулярно выпускают патчи, устраняющие обнаруженные бреши в безопасности.
- **Повышение стабильности.** Не только защищают устройства, но и исправляют ошибки в их работе.
- **Новые функции.** Иногда обновления включают дополнительные инструменты безопасности.

Стоит прочесть также: Психологические механизмы - конспект урока

Игнорирование обновлений делает аппарат уязвимым перед киберугрозами, так как злоумышленники активно используют известные уязвимости.

Резервное копирование информации

Создание резервных копий – это обязательная мера защиты, которая позволяет избежать потери важных материалов в случае атаки или поломки устройства.

Способы создания резервных копий:

- **Облачные хранилища.** Такие платформы, как Google Drive, Яндекс.Диск или Dropbox, предоставляют возможность сохранять информацию на удалённых серверах.
- **Внешние накопители.** Это могут быть USB-диски или внешние жёсткие диски, на которых хранятся копии данных.
- **Автоматическое резервирование.** Многие гаджеты позволяют настроить автоматическое копирование информации по расписанию.

Создание резервных копий важно не только для защиты от вирусов-вымогателей, но и для предотвращения потерь из-за аппаратных сбоев.

Комплексная защита – это не только установка специализированного софта, но и регулярное выполнение профилактических действий. Использование антивирусов, настройка файерволов, своевременное обновление системы и создание резервных копий являются основными шагами для обеспечения безопасности в цифровом мире. Соблюдая эти меры, пользователь минимизирует риск потери важной информации и защищает своё устройство от киберугроз.

Правила безопасного использования устройств и программ

Иллюстративное фото / newUROKI.net

Чтобы минимизировать риск кибератак и защитить личные сведения, важно следовать базовым правилам защищённого поведения в цифровой среде. Эти рекомендации охватывают различные аспекты использования гаджетов, интернет-сервисов и приложений.

Создание надежных паролей

Пароль – это ключ к защите личной информации. Использование слабых или однотипных комбинаций делает учётные записи лёгкой целью для злоумышленников.

Рекомендации по созданию надёжного пароля:

- **Длина и сложность.** Надежный пароль должен состоять минимум из 12 символов и включать буквы разного регистра, цифры и специальные знаки.
- **Избегайте предсказуемости.** Не используйте дату рождения, имя или простые комбинации, такие как «123456» или «password».
- **Уникальность для каждого сервиса.** Один и тот же код доступа не следует применять для нескольких учётных записей.
- **Используйте менеджеры паролей.** Эти приложения помогут создавать и хранить сложные комбинации.

Безопасная работа с электронной почтой

Электронная почта – один из основных каналов для рассылки фишинговых писем и вредоносных вложений.

Как избежать угроз при работе с почтой:

- **Проверяйте отправителя.** Убедитесь, что адрес отправителя принадлежит надёжному источнику.
- **Не переходите по подозрительным ссылкам.** Даже если письмо выглядит официальным, избегайте перехода по ссылкам, вызывающим сомнения.
- **Сканируйте вложения.** Используйте антивирусы для проверки прикреплённых файлов перед их открытием.
- **Настройте двухфакторную аутентификацию.** Это создаст дополнительный уровень защиты для вашей электронной почты.

Правила загрузки и установки приложений

Загрузка и установка программ – процесс, в котором важно соблюдать осторожность, чтобы избежать заражения вредоносным кодом.

Основные рекомендации:

- Загружайте только из проверенных источников. Используйте официальные магазины, такие как Google Play или App Store.
- Проверяйте отзывы и рейтинги. Изучите комментарии других пользователей, чтобы убедиться в безопасности продукта.
- Обратите внимание на разрешения. Перед установкой приложения ознакомьтесь с тем, к каким функциям устройства оно запрашивает доступ.
- Обновляйте программы своевременно. Разработчики регулярно исправляют уязвимости в своих продуктах.

Безопасное поведение в социальных сетях

Социальные сети часто становятся местом, где злоумышленники собирают личную информацию или распространяют вредоносные ссылки.

Правила безопасности в социальных сетях:

- Ограничивайте видимость профиля. Настройте конфиденциальность так, чтобы посторонние не имели доступа к личной информации.
- Не делитесь избыточной информацией. Избегайте публикации данных о месте жительства, номерах телефонов или банковских картах.
- Будьте осторожны с незнакомцами. Не принимайте запросы на добавление в друзья от неизвестных людей.

- Не переходите по подозрительным ссылкам. Даже если ссылка получена от друга, убедитесь в её безопасности.

Действия при обнаружении заражения

Если вы подозреваете, что устройство подверглось атаке, важно немедленно принять меры.

Алгоритм действий:

- **Отключите устройство от сети.** Это предотвратит дальнейшее распространение вредоносного кода.
- **Запустите сканирование с помощью антивируса.** Используйте проверенные инструменты для обнаружения угроз.
- **Удалите подозрительные файлы или утилиты.** Если они не удаляются стандартным способом, воспользуйтесь безопасным режимом гаджета.
- **Поменяйте коды доступов.** Если были обнаружены утечки, немедленно обновите данные для входа на всех аккаунтах.
- **Обратитесь за помощью.** Если проблема сохраняется, проконсультируйтесь со специалистом или службой поддержки.

Соблюдение этих правил позволяет минимизировать риски, связанные с использованием цифровых устройств и онлайн-сервисов. Комплексный подход к безопасности включает защиту учётных записей, осторожность при работе с почтой и социальными сетями, а также своевременное реагирование на подозрительные активности. Важно помнить, что каждый пользователь несёт ответственность за свою безопасность в интернете.

Рефлексия

Давайте сейчас остановимся на минуту, проведём рефлексию и подумаем о том, как вы себя чувствуете после этого урока. Я хочу, чтобы каждый из вас оценил свои эмоции, своё состояние и то, насколько полезной оказалась информация, которую мы сегодня разобрали.

Для начала, подумайте: что из изученного сегодня было для вас наиболее важным? Возможно, это новые знания о защите устройств, правила создания надёжных паролей или информация о видах угроз?

Теперь вспомните, что вызвало у вас наибольший интерес или, может быть, удивление. Поднимите руку или просто поделитесь мыслями. Например, кто-то мог открыть для себя неожиданные методы социальной инженерии или узнать, как распознать фишинг.

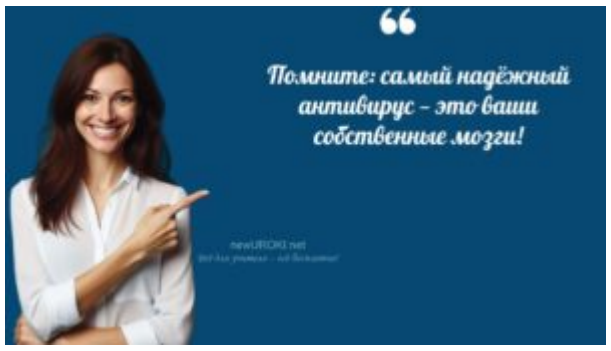
Далее задайте себе вопрос: что было для вас сложным? Если есть темы, которые остались непонятными, это нормально. Запишите их для себя или скажите мне, чтобы мы могли вместе ещё раз их разобрать.

Давайте задумаемся, как вы сможете применить полученные знания на практике. Что из того, что вы услышали, вы планируете использовать в ближайшее время? Например, кто собирается проверить свои пароли или изменить настройки безопасности на устройствах?

Если вы оцените себя по шкале от 1 до 5, где 1 — «мне было совсем неинтересно и трудно», а 5 — «я чувствую себя уверенно и узнал много нового», какую оценку вы бы себе поставили за участие и понимание материала?

Наконец, подумайте, что бы вы хотели узнать больше в этой теме. Возможно, вы хотели бы изучить конкретные виды угроз более подробно или поговорить о новых технологиях защиты?

Заключение



Учителя шутят

Друзья, сегодня мы сделали ещё один важный шаг к тому, чтобы чувствовать себя уверенно в современном мире технологий. Вы доказали, что можете мыслить критически, анализировать риски и находить решения даже в сложных ситуациях. Это действительно ценно!

Помните, что ваше цифровое пространство — это отражение вашей реальной жизни. Чем больше внимания вы уделяете его защите, тем спокойнее и безопаснее вам будет работать и отдыхать в сети.

Вы уже обладаете ключами, которые помогут вам избежать многих неприятностей. Эти знания и навыки — ваш щит и опора в цифровую эпоху. Главное — не забывать их применять!

Каждый из вас может стать примером для других: друзей, семьи, близких. Расскажите им о том, что вы узнали, помогите разобраться в сложных вопросах. Вместе мы можем сделать окружающее цифровое пространство более безопасным для всех.

И пусть каждый ваш шаг в этом направлении будет не только полезным, но и вдохновляющим! Верьте в себя, будьте внимательны и настойчивы, ведь знания — это сила, которая всегда с вами.

Спасибо за ваш интерес, внимание и активность сегодня. Вы большие молодцы!

Домашнее задание

Ученики шутят

- Изучить материал параграфа § учебника.
- Составить памятку «Правила безопасного поведения в сети Интернет».
- Проанализировать защищенность своего домашнего компьютера.
- Выполнить практическое задание в рабочем листе.

Технологическая карта

Скачать бесплатно технологическую карту урока по теме: «Опасности, связанные с использованием программного обеспечения»

Технологическая карта — это документ, который содержит структуру и планирование учебного занятия, включая цели, задачи, этапы, методы и формы организации деятельности учащихся, а также используемые ресурсы и оборудование.

Смотреть видео

Полезные советы учителю

Скачать бесплатно 5 полезных советов для проведения урока основ безопасности и защиты Родины по теме: «Опасности, связанные с ПО» в формате Ворд

Чек-лист педагога

Скачать бесплатно чек-лист для проведения урока ОБЗР по теме: «Опасности, связанные с ПО» в формате Word

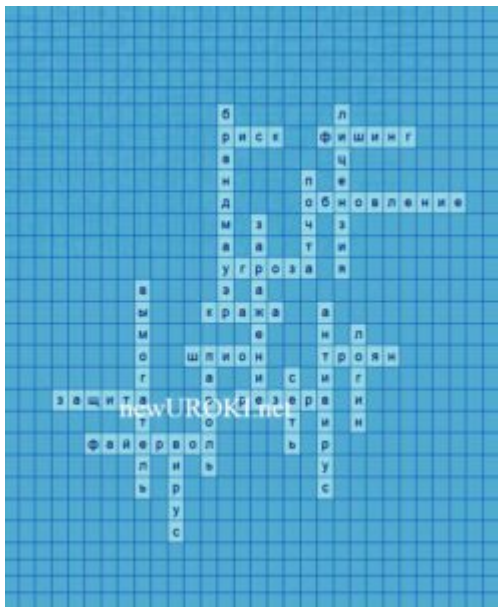
Чек-лист для педагога — это инструмент педагогической поддержки, представляющий собой структурированный перечень задач, шагов и критериев, необходимых для успешного планирования, подготовки и проведения урока или мероприятия.

Карта памяти для учеников

Скачать бесплатно карту памяти для учеников 11 класса по ОБЗР по теме: «Опасности, связанные с ПО» в формате Ворд

Карта памяти школьника — это методический инструмент, который помогает учащимся структурировать и запоминать ключевую информацию по определенной теме.

Кроссворд



Кроссворд

Скачать бесплатно кроссворд на урок ОБЗР в 11 классе по теме: «Опасности, связанные с использованием программного обеспечения» в формате WORD

Тесты

Какой значок в письме может указывать на попытку обмана?

a) Восклицательный знак в красном треугольнике

b) Синяя стрелка для пересылки

c) Зеленая галочка подтверждения

Правильный ответ: a

Что нужно делать при получении сообщения о выигрыше в лотерею?

a) Перейти по ссылке для получения приза

b) Проигнорировать такое сообщение

c) Отправить свои банковские реквизиты

Правильный ответ: b

Как часто рекомендуется менять пароли от важных аккаунтов?

a) Раз в 2-3 месяца

b) Раз в 2-3 года

c) Только при взломе

Правильный ответ: a

Какой пароль считается наиболее надежным?

a) Дата рождения

b) KjP9$mN2#qL5

c) Qwerty123

Правильный ответ: b

Что делать при получении странного файла от друга?

a) Сразу открыть

b) Уточнить у друга, отправлял ли он его

c) Переслать другим друзьям

Правильный ответ: b

Как проверить надежность интернет-магазина?

a) По красивому дизайну

b) По очень низким ценам

c) По отзывам и наличию контактов

Правильный ответ: c

Что делать при появлении всплывающего окна о заблокированном компьютере?

a) Позвонить по указанному номеру

b) Перевести деньги для разблокировки

c) Обратиться к специалисту

Правильный ответ: c

Какой признак может указывать на поддельное письмо от банка?

a) Логотип банка

b) Ошибки в тексте письма

c) Время получения письма

Правильный ответ: b

Где лучше хранить резервные копии важных файлов?

a) Только на компьютере

b) На разных носителях

c) В социальных сетях

Правильный ответ: b

Как защитить свой wi-fi роутер?

a) Оставить настройки по умолчанию

b) Установить сложный пароль

c) Отключить пароль совсем

Правильный ответ: b

Интересные факты для занятия

1. **Интересный факт 1:**
   В 1988 году студент Корнеллского университета Роберт Моррис создал первый сетевой червь, который за 24 часа заразил более 6000 компьютеров и парализовал работу большей части интернета. Интересно, что Моррис сделал это не со злым умыслом, а в исследовательских целях, но просчитался в коде, из-за чего червь начал неконтролируемо размножаться.
2. **Интересный факт 2:**
   Самым первым компьютерным взломщиком в истории стал… попугай! В 1903 году попугай Джона Невила Маскелайна научился издавать звуки, имитирующие сигналы азбуки Морзе, и срывал работу первого беспроводного телеграфа Маркони, передавая неприличные сообщения. Это был первый зафиксированный случай взлома системы связи.
3. **Интересный факт 3:**
   В современном мире хакеры часто используют «социальную инженерию» вместо технических методов взлома. Например, в 2020 году подростки взломали Twitter-аккаунты знаменитостей, просто позвонив сотрудникам компании и представившись системными администраторами. Этот случай показал, что человеческий фактор может быть уязвимее любой технической защиты.

Интеллект-карта

Ментальная карта (интеллект-карта, mind map)

Ментальная карта (интеллект-карта, mind map) — это графический способ структурирования информации, где основная тема находится в центре, а связанные идеи и концепции отходят от неё в виде ветвей. Это помогает лучше понять и запомнить материал.

Облако слов

Облако слов

Облако слов — удобный инструмент на занятии: помогает активизировать знания, подсказывает, служит наглядным материалом и опорой для учащихся разных возрастов и предметов.

Презентация

Презентация

Скачать бесплатно презентацию на урок ОБЗР в 11 классе по теме: «Опасности, связанные с использованием программного обеспечения» в формате PowerPoint

БОНУС: Рабочий лист

Скачать бесплатно рабочий лист по ОБЗР по теме: «Опасности, связанные с использованием программного обеспечения» в формате ВОРД

Рабочий лист – это образовательный инструмент, представляющий собой специально подготовленный комплект заданий, упражнений или вопросов, который используется на занятии для активизации познавательной деятельности учащихся.

Список источников и использованной литературы

1. Ярковский В.П., «Цифровые угрозы и методы защиты». Издательство «Сириус», Санкт-Петербург, 2001. 220 страниц.
2. Гулькевич М.К., «Информационные риски в сети». Издательство «Электронные решения», Москва, 2000. 150 страниц.
3. Лунина О.А., «Основы защиты в мире новых технологий». Издательство «Прогресс плюс», Новосибирск, 2005. 180 страниц.
4. Зуров С.И., «Современные методы защиты от угроз в цифровом мире». Издательство «Техно-Бизнес», Екатеринбург, 2002. 210 страниц.
5. Борисов И.Г., «Цифровые угрозы: защита и профилактика». Издательство «Информационные технологии 2000», Казань, 2004. 160 страниц.

Слова ассоциации (тезаурус) к уроку: риск, защита, угроза, кража, пароль, фишинг, логин, сеть, вирус, троян, шпион, брандмауэр, обновление, почта.

Безопасность в цифровой среде — конспект урока »

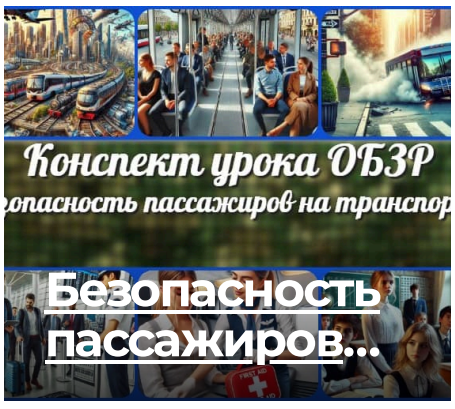
Автор Глеб Беломедведев

Глеб Беломедведев - постоянный автор и эксперт newUROKI.net, чья биография олицетворяет трудолюбие, настойчивость в достижении целей и экспертность. Он обладает высшим образованием и имеет более 5 лет опыта преподавания в школе. В течение последних 18 лет он также успешно работает в ИТ-секторе. Глеб владеет уникальными навыками написания авторских конспектов уроков, составления сценариев школьных праздников, разработки мероприятий и создания классных часов в школе. Его талант и энтузиазм делают его неотъемлемой частью команды и надежным источником вдохновения для других.

ПОХОЖИЕ УРОКИ

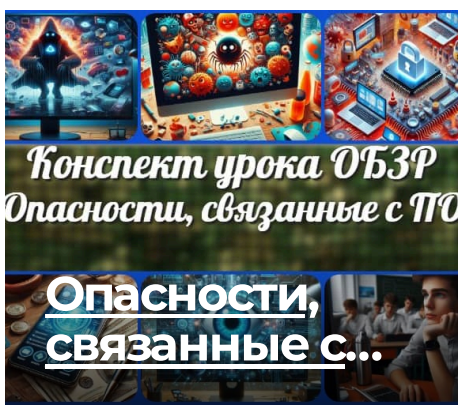
Безопасность в цифровой...

Помощь при ЧС на...



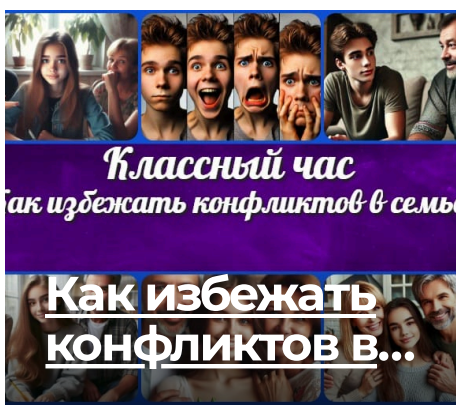
Безопасность пассажиров...

ИНТЕРЕСНЫЕ КОНСПЕКТЫ УРОКОВ

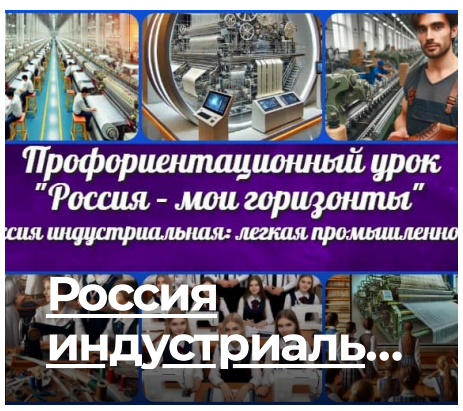


Опасности, связанные с...

Безопасность в цифровой...



Как избежать конфликтов в...



Россия индустриаль...

Новые УРОКИ

Новый сайт от проекта UROKI.NET. Конспекты уроков, классные часы, сценарии школьных праздников. Всё для учителя - всё бесплатно!

Добро пожаловать на сайт "Новые уроки" - newUROKI.net, специально созданный для вас, уважаемые учителя, преподаватели, классные руководители, завучи и директора школ! Наш лозунг "Всё для учителя - всё бесплатно!" остается неизменным почти 20 лет! Добавляйте в закладки наш сайт и получите доступ к методической библиотеке конспектов уроков, классных часов, сценариев школьных праздников, разработок, планирования по ФГОС, технологических карт и презентаций. Вместе мы сделаем вашу работу еще более интересной и успешной! Дата открытия: 13.06.2023