Методические материалы для учителя.

Урок «Типы информационных угроз»

kaspersky

Урок «Типы информационных угроз»

Цель обучения:

Сформировать понимание основных типов информационных угроз.

Задачи:

- определить основные типы угроз, с которыми можно столкнуться в Интернете;
- научить выявлять угрозы в Интернете и классифицировать их;
- сформировать правила защиты своих данных и устройств при работе в Интернете.

Планируемые результаты:

Личностные: мотивация к обучению в области информационной безопасности и формирование устойчивого интереса к раскрытию связей между информационными технологиями и информационной безопасностью;

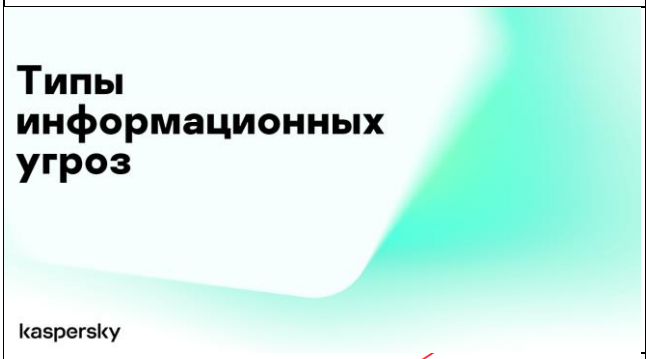
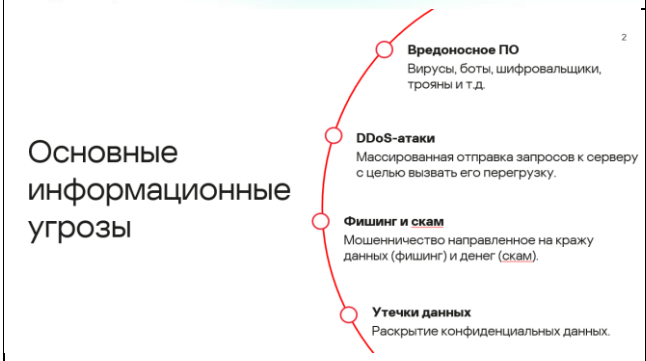
Предметные: раскрытие прикладного использования методов защиты от основных типов информационных угроз, с которыми могут столкнуться пользователи при работе в информационном пространстве;

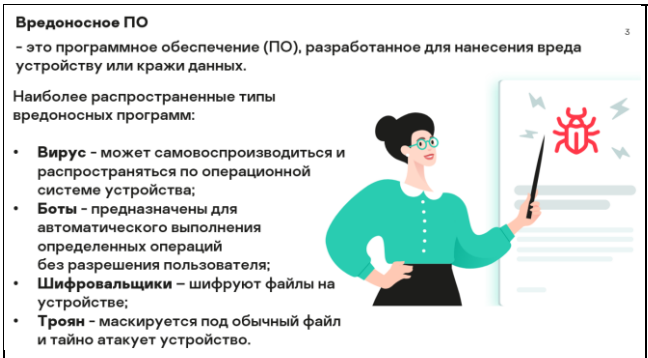
Метапредметные: формирование самостоятельности выполнения конкретной поставленной задачи, формирование навыков анализа, сравнения и обобщения.

Методическое обеспечение и средства обучения:

1. Методические материалы для учителя
2. Презентация к уроку
3. Рабочие листы учащихся

Методический материал носит рекомендательный характер и учитель, принимая во внимание особенности класса, может изменять вопросы и дополнять задания.

Слайд	Пояснения для учителя
	На этом уроке необходимо сформировать ключевые понятия о типах информационных угроз и о том, как защитить себя и свои данные в информационном пространстве.
	В список информационных угроз, которые мы будем рассматривать на этом уроке входят: **вредоносное программное обеспечение** (вредоносное ПО) - вирусы, боты, шифровальщики, трояны и т.д.; **DDoS-атаки** - ммассированная отправка запросов к серверу с целью вызвать его перегрузку. **фишинг и скам** - мошенничество, направленное на кражу данных (фишинг) и денег (скам); **утечки данных** - рраскрытие конфиденциальных данных. В ходе урока мы подробно раскроем каждую из представленных угроз и дадим рекомендации о том, как себя защитить.



Начните объяснение того, что такое вредоносное ПО с определения. Вредоносное ПО — это программное обеспечение (ПО), разработанное для нанесения вреда устройству или кражи данных.
По типам вредоносного ПО, которое могут использовать злоумышленники выделяют следующие:
Вирус - может самовоспроизводиться и распространяться по операционной системе устройства;
Действие такого ПО можно сравнить с тем, как распространяется биологический вирус. Носителями в данном случае будут выступать файлы пользователя, после взаимодействия с вредоносным кодом, они становятся зараженными.
Боты - предназначены для автоматического выполнения определенных операций без разрешения пользователя.
Обычно это незаметные программы, которые могут никак себя не проявлять до определенной команды от злоумышленника.
Шифровальщики – шифруют файлы на устройстве. Обычно, после этого на экране пользователя появляется уведомление с требованием выкупа в обмен на код разблокировки. Не стоит верить таким обещаниям, так как никто не даст гарантии того, что после оплаты вам такой код сообщат.
Троян - маскируется под обычный файл и тайно атакует устройство.

На этом слайде перечислены основные советы для того, чтобы защитить себя от вредоносного ПО.
- Антивирусные программы необходимы на всех устройствах пользователей, как на стационарных компьютерах, так и на мобильных устройствах (смартфонах и планшетах).

	- Загружайте приложения только с надежных сайтов и магазинов приложений. Это снижает риск загрузки вредоносного программного обеспечения. Мы рекомендуем так же сказать учащимся о том, что это не гарантирует 100% защиты от того, что вы не встретите вредоносное ПО в официальных онлайн-магазинах. Нужно обращать внимание на рейтинг приложения, отзывы пользователей, а также на предупреждения антивирусных решений, которые срабатывают при попытке скачивания и установки зловредного кода. Злоумышленники могут «прятать» зловредный код в самых обычных приложениях. - Регулярно обновляйте операционные системы и приложения на всех своих устройствах. Разработчики регулярно выпускают обновления систем безопасности. - Проверяйте запрошенные разрешения для приложений. Обратите внимание на то, к каким функциям вашего устройства приложения запрашивают доступ и оставляйте только те, которые необходимы им для работы. Например, приложению «фонарик», совсем не нужен доступ к вашей геопозиции или доступ к книге ваших «контактов». - Бесплатные точки доступа Wi-Fi могут создавать злоумышленники для того, чтобы ввести в заблуждение пользователей и получить контроль над их трафиком. Поэтому критически важно рассказать об этом учащимся, делая акцент на том, чтобы они не совершали онлайн-покупки или не пересылали личную информацию, когда находятся в публичной сети.

Расскажите учащимся о том, что угроза DDoS-атаки является актуальной в настоящее время и может быть использована злоумышленникам для атаки на веб-ресурсы (сайт компаний, социальные сети, компьютерные игры и т.д.).
DDoS-атака - это отправка большого количества запросов на веб-ресурс, в результате чего может произойти прекращение работы ресурса.
Признаками такой атаки являются повышение активности трафика передачи данных, резкий рост входящих запросов. Схема того, как устроена такая атака расположена на слайде и включает в себя:
- множество зараженных устройств, среди которых могут быть как стационарные компьютеры, смартфоны, устройства умного дома, в общем все устройства, которые могут подключаться к интернету.
- веб-ресурс, который подвергается атаке не способен обработать такое большое количество запросов и из-за этого его работа приостанавливается
- обычные пользователи не могут зайти на атакованный веб-ресурс, потому что их запросы «встают» в очередь.
Из-за этого доступ к ресурсу оказывается невозможным.
Чтобы дать представление о том, насколько «мощной» может быть DDoS-атака стоит упомянуть атаку в мае 2025 года, где участниками стали сотни тысяч зараженных IP-адресов из 161 стран, которые создали трафик мощностью 7,3 Гбит/сек.

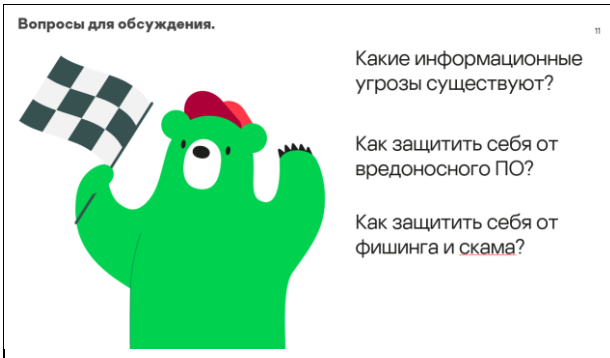
DDoS-атаки. Предотвращение и смягчение последствий. 6 **Сети Anycast.** Перераспределяют трафик для сохранения работоспособности сервера, чтобы его не пришлось отключать полностью. **Межсетевые экраны.** Межсетевые экраны веб-приложений (WAF) для защиты своих серверов. WAF можно настроить с помощью правил фильтрации трафика, блокируя только подозрительный трафик. **Маршрутизация по принципу «черной дыры».** Перенаправление всего трафика с сервера на маршрут специально созданного узла - «черной дыры», исключая его из сети и сохраняя его целостность. **Ограничение скорости.** Ограничение количества запросов, которые сервер может принять в любой момент времени.	Рекомендации о том, как защититься и смягчить последствия таки атак приведены на слайде.
Фишинг и скам. 7 **Фишинг** – действия злоумышленников, направленные на **кражу данных**. **Скам** – действия злоумышленников, направленные на **кражу денег**. С помощью фишинга и скама мошенники обычно пытаются сделать следующее: • заразить ваше устройство вредоносным ПО; • похитить конфиденциальную информацию, чтобы получить доступ к вашим деньгам или персональным данным; • получить доступ к вашим учетным записям; • убедить вас добровольно перевести деньги или другие ценности. 	Несмотря на разные способы онлайн-мошенничества, которые могут использовать злоумышленники, их можно классифицировать по двум типам: **Фишинг** – действия злоумышленников, направленные на **кражу данных**. **Скам** – действия злоумышленников, направленные на **кражу денег**. С помощью фишинга и скама мошенники обычно пытаются сделать следующее: • заразить ваше устройство вредоносным ПО; • похитить конфиденциальную информацию, чтобы получить доступ к вашим деньгам или персональным данным; • получить доступ к вашим учетным записям; • убедить вас добровольно перевести деньги или другие ценности.
Фишинг и скам. Рекомендации по защите. 8 **Подумайте, прежде чем сообщать кому-либо конфиденциальную информацию.** Коды из смс, Push-уведомлений, одноразовые пароли не нужно сообщать никому. **Своевременно обновляйте приложения, операционную систему и защитные решения.** **Не верьте тревожным сообщениям.** Известные компании не будут запрашивать у вас идентификационные или учетные данные по электронной почте или в мессенджерах. **Не открывайте вложения,** содержащиеся в подозрительных письмах или письмах от неизвестного адресата. **Никогда не переходите по ссылкам в письме,** поскольку это может привести к загрузке вредоносного ПО.	Рекомендации о том, как защититься и смягчить последствия таки атак приведены на слайде.

Утечки данных – это получение доступа к конфиденциальной, личной или защищаемой информации лицом, не имеющим соответствующего разрешения.
Основные причины утечки данных:
Случайные или умышленные действия сотрудника.
Получение доступа к информации и/или её распространение для нанесения ущерба компании или физическому лицу;
Потеря или кража устройства.
Пропажа или кража любого устройства, на котором содержится информация пользователя;
Умышленные действия стороннего лица.
Действия хакеров, которые в результате разного рода атак получают доступ к корпоративным или персональным данным.

Мишенями для атаки злоумышленников становятся:
Ненадежные пароли. Чаще всего утечки происходят из-за ненадежных паролей или кражи учетных данных.
Похищенные учетные данные. Утечка данных в результате фишинга – это серьезный инцидент кибербезопасности. Полученные в результате такой утечки персональные данные преступники могут использовать для получения доступа, например, к вашим онлайн- и банковским аккаунтам.
Платежные карты. Злоумышленники устанавливают «скиммеры» на банкоматы и похищают данные во время каждого контакта устройства с картой.

Рекомендации о том, как защититься от возможных утечек данных для пользователей заключаются в том, чтобы они могли выполнять ряд советов:

- **Используйте надежные пароли и многофакторную аутентификацию**, так вы будете уверены в том, что ваши данные надежно защищены от взлома. При этом обязательно напомните учащимся о том, что использованные пароли должны быть не только надежными (от 12 символов, с использованием строчных и прописных букв, цифр и специальных символов), но и уникальными, т.е. должно соблюдаться правило:
1 сервис – 1 пароль.
- **Делайте резервное копирование своих данных**.
Сохраняйте важные данные для возможности их восстановления. Иногда последствия утечек могут быть такими, что данные будут уничтожены. Чтобы избежать этого, нужно периодически создавать резервные копии.
- Проверяйте свои данные, которые могли попасть в открытый доступ.
Вовремя обнаруженная утечка данных позволит изменить пароль и спасти данные пользователя. Есть разные способы это сделать, самым простым способом является использование специальной функции в антивирусном решении, которая позволяет анализировать утечки данных на предмет поиска в них ваших учетных данных и сообщает об этом пользователю.
- Обновляйте ПО для исправления ошибок и повышения безопасности использования приложений. Разработчики приложений всегда улучшают защитные механизмы своих решений и до пользователя они доходят благодаря обновлениям.

	В подведении итогов, попросите учащихся ответить на предложенные вопросы в формате фронтального опроса или дискуссии. Предложенные вопросы являются базовыми, и вы можете добавлять в них свои исходя из степени готовности учащихся. В процессе выполнения заданий учащиеся заполняли рабочие листы, которые они могут использовать в качестве «памятки» или опорного конспекта.