



УРОК ЦИФРЫ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ **по организации и проведению в школах Российской** **Федерации тематического урока «Что прячется в** **смартфоне: исследуем мобильные угрозы» в рамках** **Всероссийской образовательной акции «Урок Цифры»**

Москва

2023

СОДЕРЖАНИЕ

Аннотация	3
Пояснительная записка	4
Информация о теме урока	4
Правила информационной безопасности	8
Цели и задачи урока	11
Подготовка к уроку	12
План урока	12
Набор материалов	16
Приложение 1. Технические требования для проведения урока	16
Приложение 2. Список полезных источников	17
Приложение 3. Описание заданий тренажера	17
Задание 1. «Определи вредоносное приложение»	19
Задание 2. «Выясни, как зловред проник на устройство»	21
Задание 3. «Обнови устройство»	22
Задание 4. «Найди признаки фишинговой страницы»	23
Задание 5. «Измени настройки приватности в социальных сетях и защити учетную запись»	24

Аннотация

Данные методические рекомендации предназначены для руководителей образовательных организаций и педагогов, организующих уроки в рамках всероссийского образовательного мероприятия «Урок Цифры» для своих школ, классов, организаций дополнительного образования школьников.

Мероприятие имеет просветительскую направленность и способствует раннему профессиональному самоопределению школьников в области информационных технологий в условиях перехода к цифровой экономике. Оно ориентировано на учеников 1–11 классов общеобразовательных школ и включает как элементы, универсальные для всех возрастов, так и дифференцированные по возрастам, что отражено далее в тексте настоящих рекомендаций.

Методические материалы находятся в открытом доступе на сайте мероприятия «Урок Цифры» (<https://урокцифры.рф>) и могут быть использованы для проведения тематических уроков информатики, а также педагогами дополнительного образования для проведения занятий и школьными учителями для проведения профориентационных классных часов и организации внеурочной деятельности обучающихся по направлениям, связанным с информационными технологиями.

Пояснительная записка

Обозначение проблемной области

Смартфоны сегодня есть практически у всех. По данным опроса «Лаборатории Касперского», у 88% детей в возрасте 7-10 лет уже есть свой смартфон или планшет. При этом дети, как и взрослые, сталкиваются с различными киберугрозами. Так, по данным того же опроса, за последние два года 15% детей сталкивались с онлайн-мошенничеством, еще столько же — с телефонным, у 13% были взломаны аккаунты в различных сервисах.

Количество персональных, конфиденциальных и платежных данных, которые хранятся на смартфонах, сегодня во многих случаях уже не уступают компьютерам, поэтому интерес злоумышленников к смартфонам и данным на них будет только расти.

При этом злоумышленники умело манипулируют пользователями, в том числе детьми. Детям важно понимать, с какими угрозами они могут столкнуться на смартфонах, и уметь их избежать.

Информация о теме урока

Для мобильных устройств актуальны почти все те же киберугрозы, что и для компьютеров, в том числе — вредоносные программы, а также фишинг и скам. Большинство мобильных угроз нацелены на устройства с операционной системой Android, однако есть и такие киберугрозы, с которыми могут столкнуться пользователи со смартфонами на iOS.

Какие существуют примеры вредоносного ПО?

Троянцы — это вредоносные программы, осуществляющие несанкционированные пользователем действия: они уничтожают,

блокируют, модифицируют или копируют информацию, нарушают работу компьютеров или компьютерных сетей.

Программы-вымогатели — это вредоносное ПО, которое шифрует данные или блокирует доступ к ним и требует заплатить выкуп за снятие блокировки или дешифровку файлов.

В России, в частности, распространены скамерские приложения (скам — вид онлайн-мошенничества, при котором пользователю предлагают щедрое денежное вознаграждение). После скачивания такого приложения пользователя перенаправляют на страницу ввода личных данных. Затем на экране отображается размер якобы положенной человеку компенсации или выигрыша. Далее пользователя просят заплатить «комиссию», например, за вывод средств. Если человек это сделает, то злоумышленники получат свою прибыль — в виде этой «комиссии», а пользователь только потеряет деньги, не получив ничего взамен. Кроме того, если для перевода «комиссии» пользователь вводил данные карты, то рискует и их сохранностью.

В прошлом году активизировались также и троянцы-подписчики. Выглядит эта киберугроза так: пользователям предлагают скачать приложение, например, с онлайн-курсом домашних тренировок (легенды и темы таких приложений могут быть разными). Затем человек покупает доступ к контенту в этом приложении за небольшую сумму, для чего вводит данные банковской карты. Однако на деле он соглашается со скрытыми условиями, написанными мелким шрифтом, которые часто не помещаются на экране. В результате с карты ежемесячно начнут списываться деньги — сотни или даже тысячи рублей. Так пользователь рискует потерять крупную сумму.

Вредоносные и нежелательные программы — не единственная цифровая угроза, с которой могут столкнуться пользователи смартфонов. Например, фишинг и скам в интернете — универсальные угрозы, иными словами, с ними могут столкнуться пользователи смартфонов независимо от операционной системы телефона или его марки.

Давайте разберемся с терминами. Фишинг — процесс выманивания конфиденциальной информации у пользователя (логин и пароль, данные банковской карты и т. п.). Цель злоумышленников, как правило, — кража денег и конфиденциальной информации. Как это выглядит? Например, человек думает, что вводит данные от учетной записи в социальной сети, но на самом деле оставляет логин и пароль от аккаунта на поддельном сайте. Так его данные становятся доступны злоумышленникам.

Фишинговые ресурсы, как правило, живут недолго — от одного до трех дней. Поэтому злоумышленники стараются разослать их как можно большему количеству людей и придумать для этого убедительную легенду.

В конце прошлого года и в начале 2023, например, года значительно вырос объем фишинговых атак на пользователей мессенджеров. Люди столкнулись с различными схемами, в рамках которых злоумышленники пытались украсть аккаунты в мессенджерах с помощью поддельных ресурсов, где побуждали ввести данные для входа в учетную запись. Среди легенд, которые они использовали, в частности, предложение принять участие в голосовании за лучший детский рисунок на тему «Моя любимая зима». Для того, чтобы проголосовать за рисунок, необходимо было перейти по ссылке и ввести свои учетные данные. Полученный доступ к аккаунтам злоумышленники могут использовать для различных целей, в том числе для кражи конфиденциальных данных, шантажа и рассылки мошеннических сообщений. При этом стоит отметить, что злоумышленники постоянно меняют свои легенды.

Зачастую фишинг выступает одним из векторов (ступеней) более сложных кибератак, которые злоумышленники используют для того, чтобы похитить данные пользователей и компаний.

Про скам мы уже упоминали, когда говорили о скам-приложениях. Однако важно помнить, что с таким видом онлайн-мошенничества человек может столкнуться не только в виде приложений, но и в виде ресурсов в интернете, например, когда посещает сайты в мобильном браузере или переходит по ссылкам из мессенджеров и социальных сетей.

Стоит отметить, что сегодня технологии защиты для данных на мобильных устройствах во многом не уступают технологиям защиты для ПК. Однако вместе с тем пользователям также важно повышать свою цифровую грамотность, чтобы еще больше снизить риски попасться на удочку злоумышленников.

Ранее мы привели примеры вредоносного ПО, но как можно понять, что на смартфоне прячется вредоносная программа?

Прежде всего стоит отметить, что современные зловреды в большинстве своем умеют хорошо скрываться — они могут никак себя не выдавать.

Самостоятельно определить, что с устройством что-то не так может быть довольно сложно. Существует ряд косвенных признаков, которые лишь намекают на то, что с устройством что-то случилось. Например, у смартфона (даже нового) начинает быстро садиться батарея, расходуется подозрительно большой объем интернет-трафика, устройство тормозит, внезапно перезагружается. И не только.

Однако крайне важно подчеркнуть, что точно ответить на вопрос — заражено ли устройство — можно только с помощью защитных решений.

Злоумышленники могут распространять вредоносные программы под видом самых разных приложений. Например, однажды программа-шифровальщик распространялась под видом долгожданной популярной игры, а точнее — ее несуществующей «бета-версии для Android». Но на тот момент разработчик никак не анонсировал мобильный вариант игры, и это, конечно, должно было насторожить пользователей.

Что делать, если устройство действительно оказалось заражено вредоносным ПО? Мы не рекомендуем пытаться избавиться от вредоносных программ самостоятельно, для этого детям обязательно нужно обратиться за помощью к взрослым и использовать защитные решения.

Конечно, намного проще изначально следовать правилам безопасного поведения в интернете и защищать свои устройства, чем потом бороться с последствиями.

Правила информационной безопасности

Прежде чем что-то скачать в интернете или принять участие в крайне щедрой акции, обязательно перепроверяйте информацию в официальных источниках. Это могут быть сайт компании, телефон службы поддержки, официальные страницы в социальных сетях.

- **Скачивайте приложения только из официальных источников.**
Это могут быть официальные магазины приложений или сайты компаний. Такие приложения (и их обновления) проходят модерацию на наличие вредоносного кода.
- **Запретите установку приложений из неизвестных источников.**
Исключение можно сделать только для официальных магазинов приложений и официальных сайтов компаний.

- **Регулярно обновляйте программы и операционную систему.** Вместе с обновлениями разработчики исправляют ошибки и уязвимости в ПО.
- **Установите антивирус и регулярно его обновляйте.** Решение защитит ваши данные и устройство от различных вредоносных и нежелательных программ, не даст перейти по фишинговой ссылке.
- **Используйте надежные пароли, которые трудно подобрать и не храните их в открытом доступе.** Можно воспользоваться специальной программой — менеджером паролей, которая облегчит задачу, предложив сгенерированный надежный пароль, и будет этот пароль безопасно хранить.
- **Используйте двухфакторную аутентификацию** — это способ защитить свой аккаунт, даже в том случае, если логин и пароль от него знают злоумышленники. Обычно это выглядит так: первый шаг — это логин и пароль, второй — специальный код, приходящий по SMS, в push-уведомлении или на электронную почту. Варианты могут быть разными.
- **Не переходите по ссылкам из подозрительных сообщений в почте, мессенджерах и социальных сетях.** За такими ссылками может скрываться фишинговый или скам-ресурс.
- **Не сообщайте конфиденциальную информацию незнакомым людям.** Злоумышленники могут маскироваться под знакомых, дальних родственников или сотрудников банка, писать в социальных сетях или даже позвонить.
- **Свяжитесь напрямую с компанией, если вы получили подозрительный запрос.** Если звонящий просит вас предоставить какие-либо данные, положите трубку. Перезвоните в компанию напрямую по номеру телефона на ее официальном сайте и убедитесь, что вам звонили не злоумышленники.

- **Внимательно проверяйте адреса веб-сайтов, прежде чем вводить на них конфиденциальную информацию.** Обращайте внимание на URL-адреса сайтов, совпадают ли они с настоящими. Отличие даже на одну букву должно насторожить.
- **Когда устанавливаете приложения на смартфон, не давайте им доступ к тем разрешениям и функциям, которые им не нужны для корректной работы.** Например, приложению «Фонарик» явно не нужен доступ к фотографиям и контактам.
- **Выходите из ваших аккаунтов после работы за школьными компьютерами или чужими устройствами.** Помните, что только лишь закрыть вкладку недостаточно, нужно нажать кнопку «выход» из своей учетной записи в социальной сети, мессенджере или любом другом сервисе.

Отдельно остановимся на паролях. Пароль — это одна из важнейших составляющих безопасности аккаунтов. Здесь нужно придерживаться следующих правил:

- пароль должен быть надежным: иметь минимум 12 символов, а также содержать прописные и строчные буквы, цифры, специальные символы;
- меняйте пароли регулярно;
- если у вас есть подозрение, что ваш пароль и логин оказались у злоумышленников или в открытом доступе, как можно скорее поменяйте пароль;
- в пароле не должно быть личной информации, например, имени питомца или номера телефона;
- используйте уникальные пароли для разных сайтов;
- не храните пароли на листочках и в текстовых файлах на компьютере, для этого лучше использовать специальные программы — менеджеры паролей.

Если вам интересно узнать больше про информационную безопасность, заходите в блог «Лаборатории Касперского» (kaspersky.ru/blog/ и kids.kaspersky.ru). Там вы найдете много полезных материалов на эту тему, а также интерактивные обучающие материалы. Также в блоге рассказывается про новые виды мошеннических схем и вредоносные приложения.

Цели и задачи урока

Цель урока

В рамках урока мы расскажем школьникам о видах киберугроз для мобильных устройств. На конкретных примерах для двух наиболее распространенных мобильных операционных систем разберем, как злоумышленники могут похитить данные и аккаунты. Объясним, как можно избежать потерю данных и обезопасить свой смартфон.

Важно отметить, что алгоритм настройки разрешений, а также процесс установки защитного решения и обнаружения вредоносного ПО показан в тренажерах в схематичном упрощенном виде. В реальности сценарии могут отличаться, в том числе в зависимости от ОС, марки смартфона и конкретного приложения.

В данном уроке мы предлагаем обратить внимание школьников на общие рекомендации по кибербезопасности.

Задачи урока

- Изучить видеоролик, рассказывающий про разновидности мобильных угроз и рекомендации по защите.
- В упрощенном виде дать общее представление о том, как специалисты по информационной безопасности анализируют такие угрозы.

- Сформировать серьезное отношение к кибератакам.
- Провести профориентацию в сфере информационной безопасности и в сфере разработки мобильных приложений.
- Сформировать теоретические знания и практические навыки безопасного использования смартфона в реальной жизни.
- Обсудить полученный опыт, сформулировать выводы.

Подготовка к уроку

- Изучить данный документ, посмотреть видеолекцию и презентацию к уроку.
- Сохранить заранее два видеоролика и презентацию на компьютере с доступом в Интернет.
- Подготовить листы бумаги и ручки по числу учеников для проведения викторины.
- Подготовить класс в соответствии с информацией, представленной в Приложении 1.
- Сформулировать собственный план занятия на основе предложенного.

План урока

Этап	Содержание этапа	Слайды	Время этапа
1. Анонс урока	– Приветствуем учеников. – Формулируем задачу на урок для учеников.	1–6	5 мин
2. Просмотр видеолекции	– Организуем просмотр видеолекции по теме урока. – Обсуждаем просмотренное видео.	7–11	15 мин

3. Обсуждение темы урока	– Объясняем, правильное поведение в сети интернет. – Рассматриваем, какие данные лучше скрыть со страниц соцсети. – Объясняем, чем занимается эксперт по кибербезопасности.	12–19	5 мин
4. Викторина	– Организуем викторину по информационной безопасности.	20–32	15 мин

Пояснение к этапам урока

1. Анонс урока (5 минут)

Поприветствуйте учеников и сообщите, что сегодня у них будет не обычный урок, а «Урок Цифры», который посвящен теме «Что прячется в смартфоне: исследуем мобильные угрозы».

Сформулируйте цель урока:

«Сегодня вы познакомитесь с понятием „мобильные угрозы“, узнаете, как специалисты по информационной безопасности помогают разрабатывать защитные решения какие бывают киберугрозы для пользователей смартфонов. И самое главное, вы научитесь избегать их в реальной жизни».

2. Просмотр вводного видеоролика и обсуждение темы урока (21 минута)

Покажите ученикам видеолекцию по теме урока. Ответьте на вопросы, которые возникли у ребят после просмотра. Для закрепления материала видеолекции задайте уточняющие вопросы:

- Что такое мобильные угрозы?
- Какие бывают мобильные угрозы?

- Как защитить себя от мобильных угроз?

3. Обсуждение темы урока (5 минут)

Расскажите ученикам, чем занимается специалист по кибербезопасности, Какие существуют цифровые угрозы для смартфонов? Чем они могут быть опасны и как их обнаружить (подробнее в разделе «Информация о теме урока»). Для учеников 1–4 классов, вместо слайдов, можно использовать комикс (этот же комикс представлен в тренажере), как более понятный пример объяснения материала. Слайды комикса сохранены отдельной презентацией.

Обсудите как обезопасить свой смартфон от мобильных угроз:

- *из магазинов или с сайтов разработчиков* чтобы не столкнуться со зловредными или нежелательными программами, скачивайте приложения только из официальных источников такие приложения (и их обновления) проходят модерацию на наличие вредоносного кода.

- *не переходите по ссылкам из подозрительных сообщений* даже если их прислали знакомые, не вводите свои конфиденциальные данные на сомнительных ресурсах.

- *Настройте в сервисах двухфакторную аутентификацию* это метод идентификации пользователя в каком-либо сервисе, на практике это обычно выглядит так: первый этап — вы вводите логин и пароль, второй — специальный код, приходящий по SMS, в push-уведомлениях или на почту. Это значительно повысит защищенность ваших аккаунтов.

- *Важно критически относиться к крайне щедрым или, наоборот, пугающим сообщениям и предложениям в сети.* Если человека торопят и не дают времени подумать, не исключено, что за этим стоят

злоумышленники. Прежде чем вводить платежные или конфиденциальные данные на сайте, стоит проверить адрес ресурса – в нем не должно быть опечаток.

- Используйте надежное защитное решение, которое остановит попытку перейти на фишинговый или скам-сайт, не даст загрузить и установить вредоносную программу.

4. Викторина (15 минут)

Проведите викторину для учеников, она поможет понять ученикам насколько хорошо они защищены в информационном мире. Викторина состоит из 10 вопросов. Вам нужно подготовить/раздать ученикам листы бумаги, куда они будут записывать ответы. Попросите заранее проставить цифры от 1 до 10. Предоставляйте ученикам время для обдумывания каждого вопроса (30–60 секунд). После проведения викторины подведите итоги. Покажите правильные ответы ученикам. Попросите учеников самостоятельно подсчитать количество правильных ответов, отметить их знаком «+». Узнайте, какие результаты получили ученики. Поздравьте учеников, набравших наивысшие баллы.

Если останется время после подведения итогов, пройдите с учениками еще раз по вопросам викторины, чтобы пояснить ответы к каждому вопросу. Можно попросить учеников комментировать, почему они выбрали именно такой вариант ответа.

Обратите внимание, что для школьников 1–4 классов количество вопросов может быть скорректировано. Выберите самостоятельно вопросы, учитывая возраст и уровень знаний детей.

Набор материалов

- **Видеолекция.** Ведущий контент-аналитик и руководитель направления по детской онлайн-безопасности «Лаборатории Касперского» Андрей Сиденко рассказывает о видах киберугроз на мобильных платформах.
- **Презентация** содержит всю необходимую информацию для проведения урока в формате без компьютеров, упрощает подготовку учителя к уроку. Презентация содержит этапы: проблематизацию, обсуждение темы урока, практическую часть в виде викторины и рефлексии.
- **Комикс** поможет наглядно объяснить процесс исследования кибератак на примере захватывающей истории, особенно ученикам начальных классов.

Приложение 1. Технические требования для проведения урока

Для реализации данной версии урока (без интернета) необходим класс, где у учителя есть компьютер, видеопроектор, экран и динамики. Материалы к уроку, необходимо скачать заранее на компьютере, где есть доступ к Интернету. Урок проводится с показом видеолекции и презентации.

Рекомендуем до начала урока запустить презентацию и видеоролики на учительском компьютере для проверки работоспособности.

Приложение 2. Список полезных источников

1. Блог «Лаборатории Касперского»: <https://www.kaspersky.ru/blog/>
2. Портал «Лаборатории Касперского» по детской онлайн-безопасности: <https://kids.kaspersky.ru>
3. YouTube-канал «Лаборатории Касперского»:
<https://www.youtube.com/c/KasperskyLabRussia/>
4. Курс «Лаборатории Касперского» на Stepik для школьников «Математика в кибербезопасности»:
<https://stepik.org/course/62247/promo>
5. Программа стажировок «Лаборатории Касперского» для студентов
<https://safeboard.kaspersky.ru/>

Приложение 3. Описание заданий тренажера

Тренажер предлагает ученикам понять, что необходимо делать в ситуации, когда учетные данные оказались у злоумышленников или на смартфон, проник зловред. Задания тренажера строятся вокруг работы с телефонами двух главных героев истории: Запятайки и Скобца.



Герои комикса:

- Запятайка, Скобец — обычные персонажи-школьники, которые попадают в различные ситуации и вместе с учеником получают новые знания в области информационной безопасности.

- Мидори — эксперт по кибербезопасности в «Лаборатории Касперского».
- Петя — разработчик защитных решений для мобильных устройств в «Лаборатории Касперского».
- Антон работает контент-аналитиком в «Лаборатории Касперского».
- Виктория — спам-аналитик в «Лаборатории Касперского».

Краткое содержание сюжета комикса:

1. Скобец и Запятаия просят помощи у эксперта по кибербезопасности Мидори Кума. У Скобца телефон ведет себя странно: быстро садится заряд батареи и расходуется большой объем интернет-трафика. Запятаия не может зайти в свой аккаунт в социальной сети, похоже его украли. Они созваниваются с экспертом через платформу видеосвязи.
2. Мидори подключает к звонку своего коллегу — Петю. Он разработчик защитных решений для мобильных и носимых устройств. Они помогают разобраться, что случилось со смартфоном и как на телефон проникло вредоносное ПО.
3. После того, как Скобцу удастся найти вредоносное ПО (троянца) и понять, как оно попало на смартфон, Петя говорит, что нужно установить антивирус и поменять настройки безопасности на смартфоне.
4. Теперь нужно разобраться, что случилось у Запятины. Мидори подключает Викторию и Антона. Антон работает контент-аналитиком. Он помогает защищать пользователей от фишинга и скам, анализирует методы, которые применяют онлайн-мошенники. Виктория — спам-аналитик. Она помогает защищать пользователей от спама и других почтовых угроз. Антон предлагает Запятине посмотреть на страницу авторизации в социальной сети, где она ввела

свои учетные данные. Страница выглядит подозрительно. Надо найти признаки, по которым можно определить, что это фишинг.

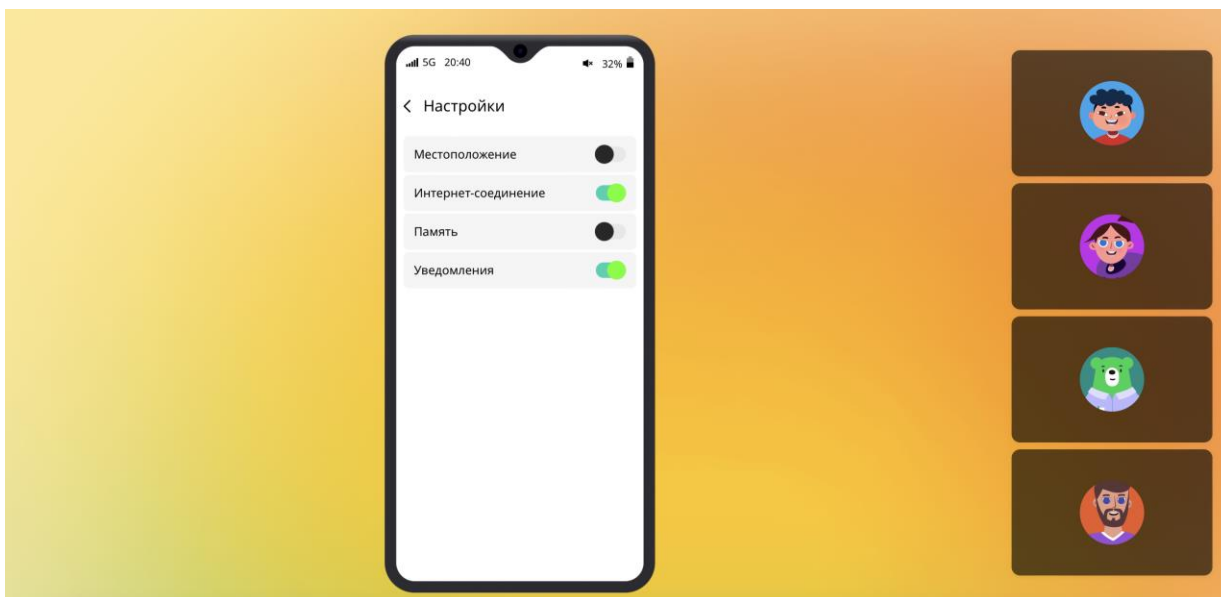
5. После восстановления доступа к странице, герои обращают внимание, что у Запятайки в профиле есть конфиденциальные данные, которых не должно быть в открытом доступе. Нужно это исправить, и Виктория предлагает заняться этим в упражнении.
6. К финалу герои узнают, с какими киберугрозами могут столкнуться владельцы смартфонов, и научатся основным правилам, чтобы обезопасить свои данные на смартфонах.

Задания тренажера построены таким образом, что ученик не сможет выполнить неверное действие. Кроме того, герои «Урока Цифры» указывают на то, в чем состоит ошибка.

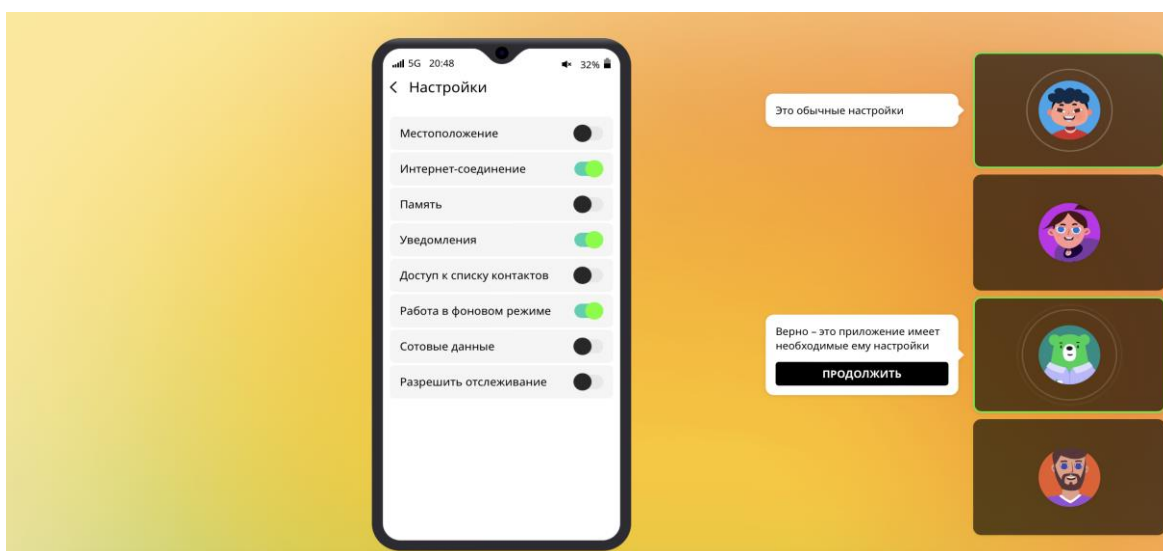
Ниже представлены примеры интерфейса тренажера (снимки экрана). Они могут незначительно отличаться от той версии тренажера, которую предстоит пройти ученикам в рамках «Урока Цифры».

Задание 1. «Определи вредоносное приложение»

Ученикам нужно вместе с Мидори Кума и героями истории найти вредоносное приложение. Оно имеет доступ к большому количеству данных на Android-смартфоне Скобца. Для этого ученику необходимо проверить приложения и найти то, которое имеет подозрительно много разрешений.



Для учеников начальных классов количество приложений и настроек сокращено до минимума: три приложения и четыре разрешения.

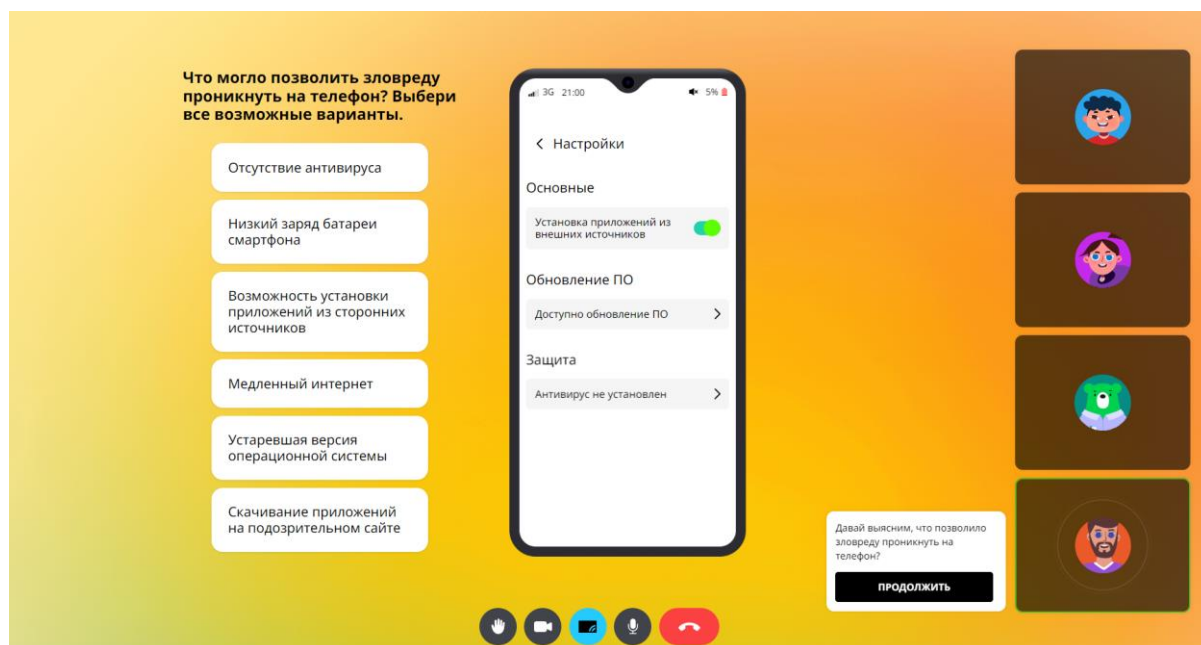


Версия задания для 5–11 классов.

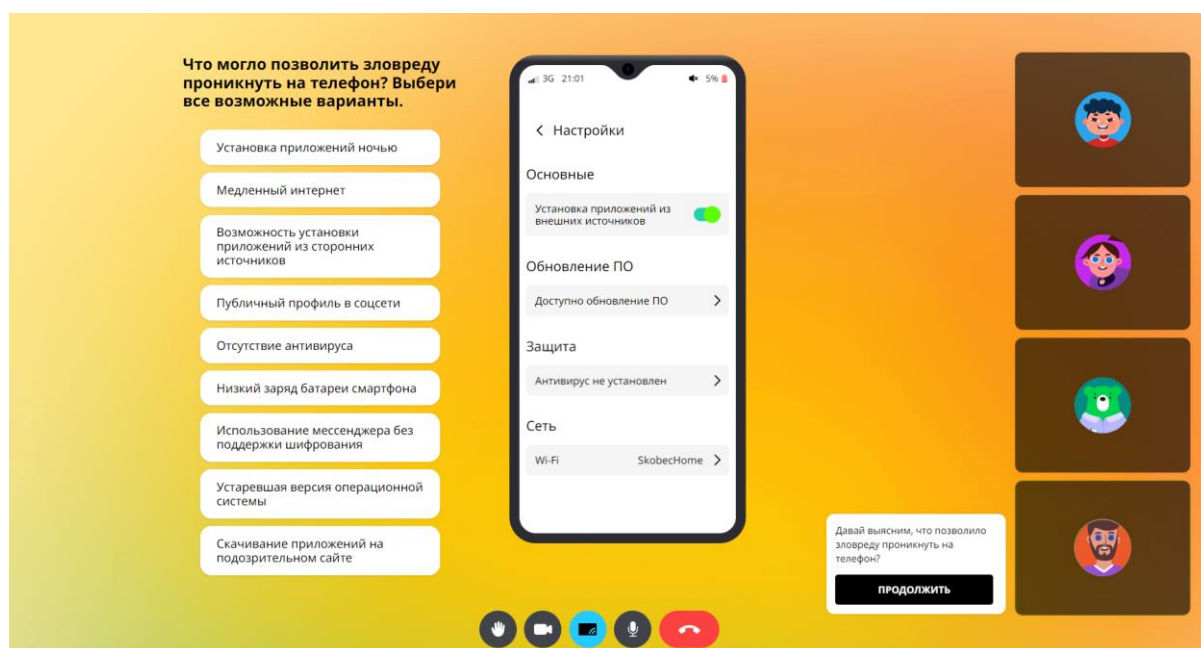
Задание 2. «Выясни, как зловред проник на устройство»

В этом задании ученикам нужно провести анализ — как зловред проник на устройство.

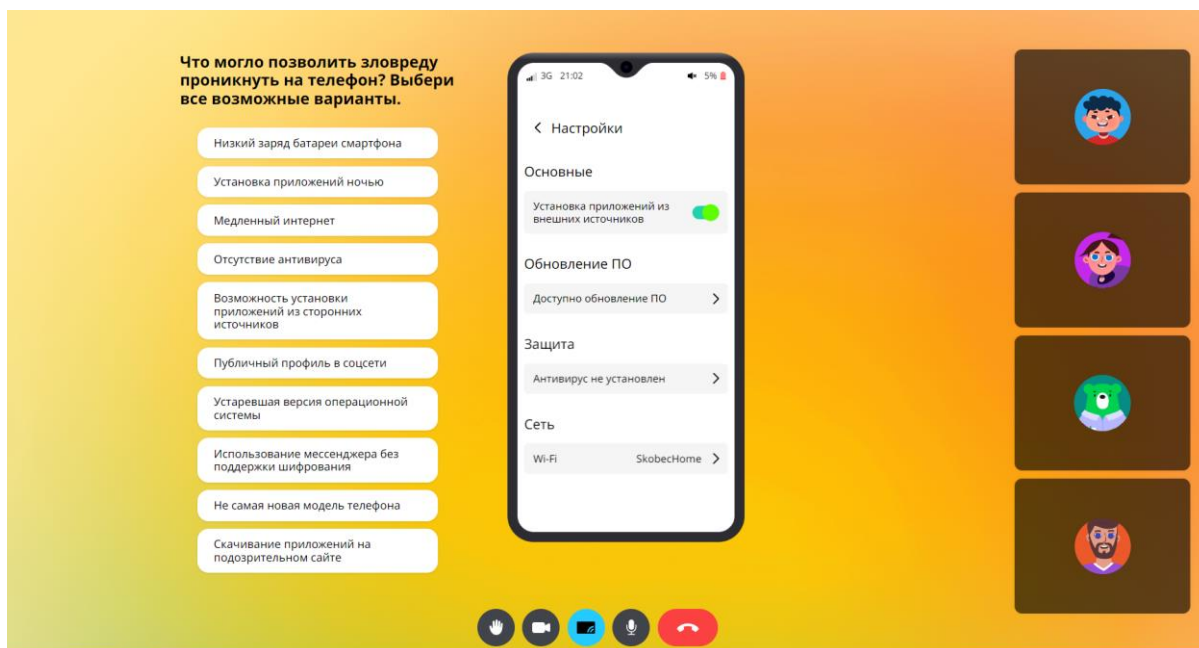
Ученику нужно проверить настройки телефона вместе с героями и определить, что «помогло» зловреду проникнуть на телефон Скобца.



Версия задания для 1–4 классов.



Версия задания для 5–8 классов.



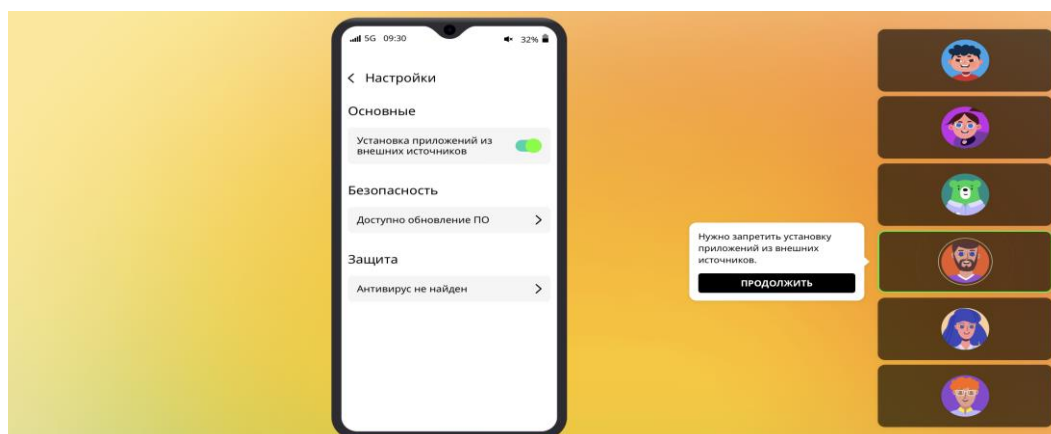
Версия задания для 9–11 классов.

Задание 3. «Обнови устройство»

Нужно обновить операционную систему и установить антивирус (он автоматически удалит зловреда) на смартфон Скобца.

Необходимо зайти в настройки телефона и обновить ОС до последней версии, после этого нужно скачать антивирус и проверить телефон на наличие вредоносного ПО. После обнаружения подозрительного приложения, нужно удалить его с помощью антивируса.

Различия между классами нет.

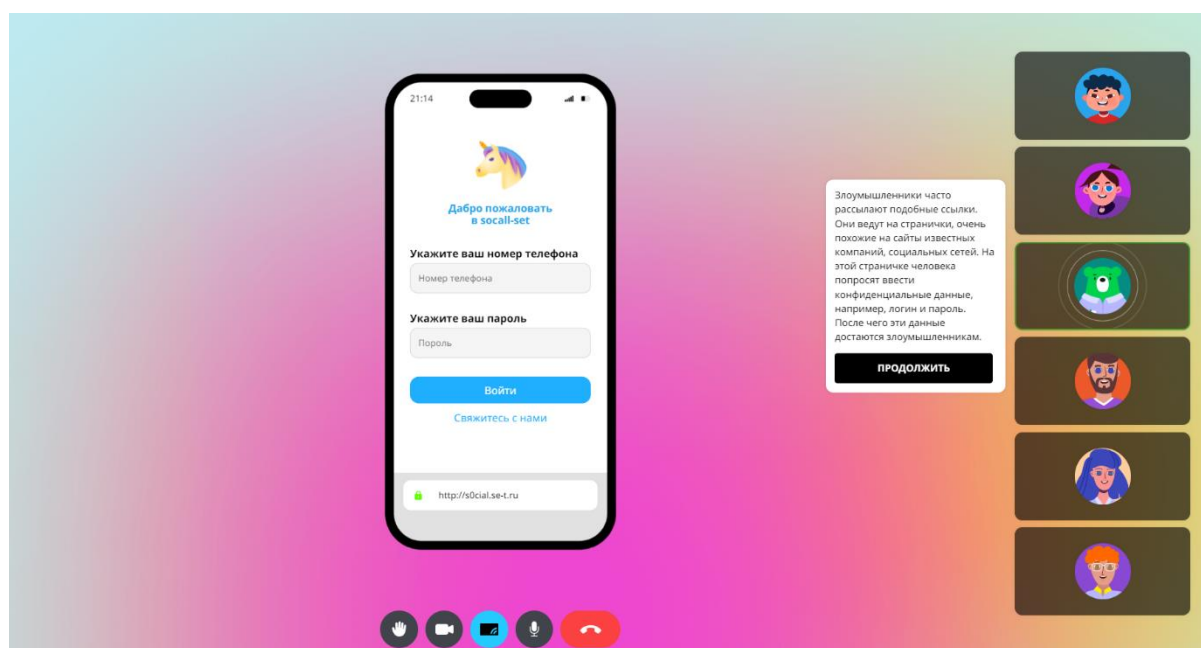


Версия задания для 1–11 классов.

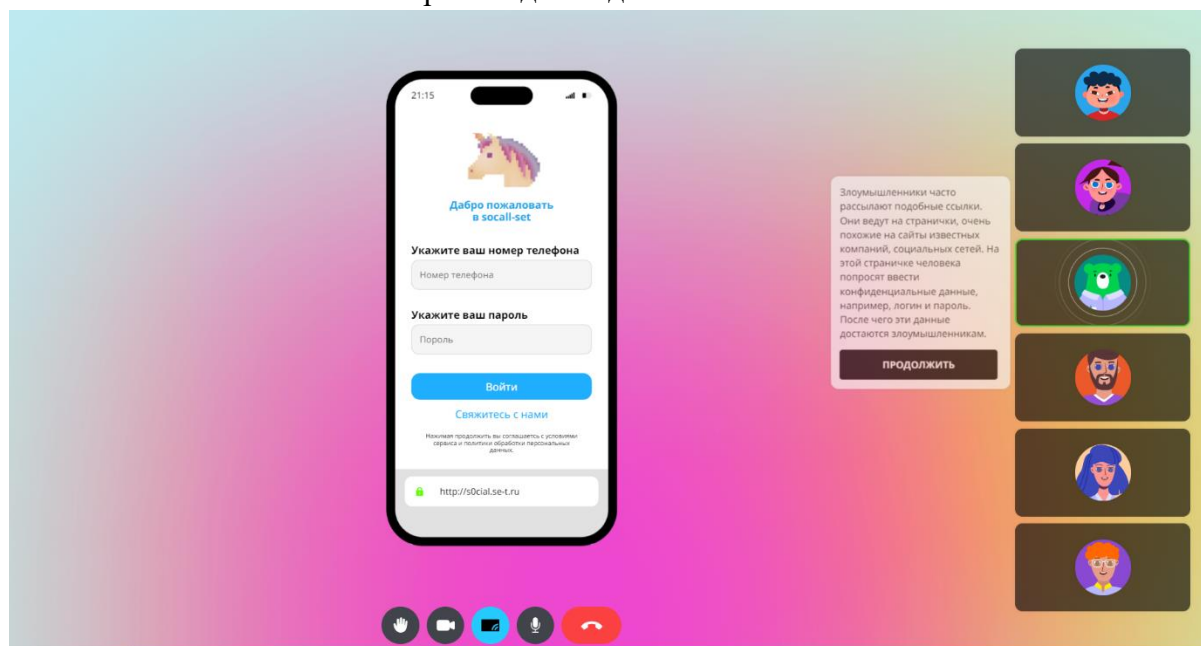
Задание 4. «Найди признаки фишинговой страницы»

В этом задании ученикам необходимо на примере страницы выдуманной социальной сети найти признаки фишинга.

Различие между возрастами заключается в количестве признаков. В 1-4 классах их 5, в 5-11 их по 7.



Версия задания для 1–4 классов.

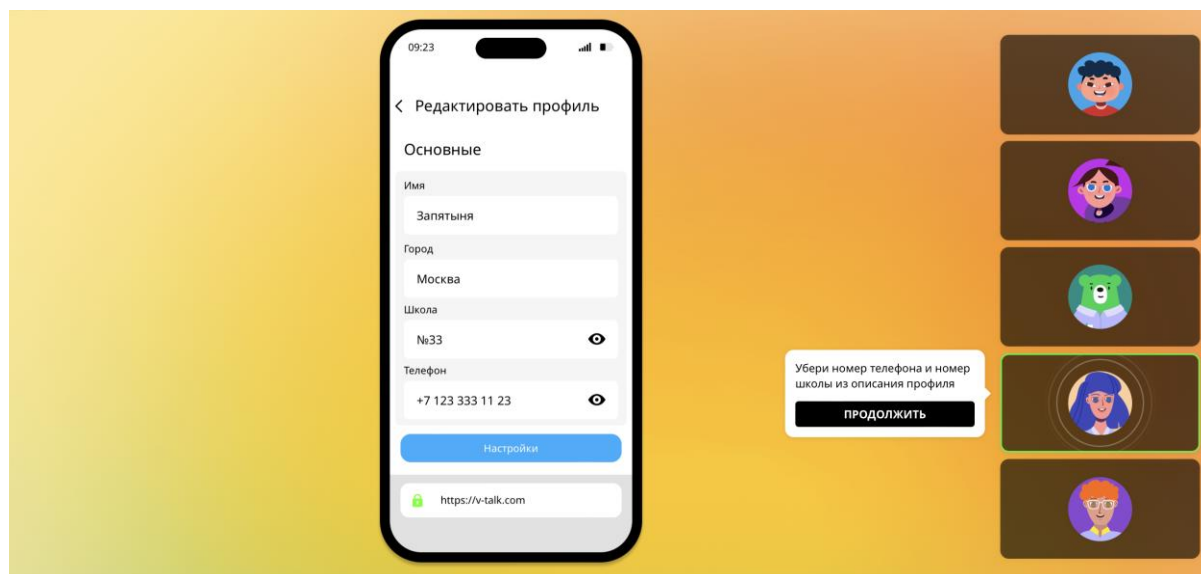


Версия задания для 5–11 классов.

Задание 5. «Измени настройки приватности в социальных сетях и защити учетную запись»

В этом задании ученику необходимо помочь Запятайне убрать конфиденциальную информацию со страницы в социальной сети, включить двухфакторную аутентификацию и придумать сложный пароль.

Различия между классами нет.



Версия задания для 1–11 классов.