УРОК ЦИФРЫ

Февраль, 2021 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по организации и проведению в школах Российской Федерации тематических уроков информатики в рамках Всероссийской образовательной акции «Урок цифры».

Урок: «Приватность в цифровом мире».

Москва

2021

СОДЕРЖАНИЕ

Пояснительная записка

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» (http://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.

Введение. Постановка проблемы и терминология

Распространение смартфонов, появление социальных сетей и других интернет-сервисов открыло для людей новые возможности: общаться с близкими и друзьями на большом расстоянии, делать покупки не выходя из дома, быстро распространять и получать информацию.

В то же время этим пользуются и злоумышленники. Персональная и личная информация, попавшая в Сеть, все чаще используется против её владельцев в форме шантажа, буллинга и мошенничества.

Овладение основами цифровой грамотности и знание правил информационной безопасности является неотъемлемой частью жизни современного человека, а умение защитить свою приватность — важный навык 21 века.

Определения, используемые в уроке

- Информационная безопасность — это процесс обеспечения конфиденциальности, целостности и доступности информации.
- Приватность в Интернете — это право человека на сохранение в секрете своей персональной информации.
- Персональная информация — это та информация, по которой можно определить, кто вы.
- Овершеринг — стремление человека рассказывать окружающим больше, чем стоило бы, заходя слишком далеко с откровенностью и забывая о приватности.
- Цифровой след — вся информация, которая остается о человеке в Интернете.
- Конфиденциальность — доступ к информации имеют только определенные лица.

Приватность данных

Чтобы разобраться, как персональная информация может стать общеступной, нужно понять, как информация попадает в Интернет. Есть несколько вариантов:

- Заполняем анкету при регистрации на ненадежном сайте.
- Участвуем в сомнительных онлайн-опросах, конкурсах, викторинах.
- Оплачиваем покупки в Сети на фишинговом сайте.
- Публикуем посты или сториз в социальных сетях, где рассказываем что-то о себе, отправляем данные в чатах, мессенджерах.
- Выкладываем фотографии, на которые случайно попадает персональная информация, например, табличка с названием улицы и номером дома.

Но это не единственные способы. Перечисленные выше варианты, касаются конкретных действий самого пользователя, но важно понимать, что влиять на приватность может то, что мы не контролируем напрямую, например:

- Публикации других людей о нас. Например, друзья размещают совместную с вами фотографию без разрешения.
- История наших поисковых запросов и посещенных сайтов. Ее обычно собирают поисковые системы, чтобы предложить вам более подходящую рекламу.
- А также установка и использование сомнительных приложений. Например, приложению «Фонарик» нужен доступ только ко вспышке, но если такое приложение просит доступ к контактам и сообщениям, это повод задуматься. Под видом благонадежного приложения, может на самом деле оказаться зловредное программное обеспечение или рекламный софт.

Чтобы уменьшить риски и сохранить приватность в Интернете надо соблюдать ряд простых правил:

- Когда регистрируетесь на сайтах, определите, что можно рассказать о себе, а что нет.
- В социальных сетях используйте «Настройки приватности». Ограничьте доступ незнакомых людей к вашей странице.
- Если хотите поделиться какой-то персональной информацией, ограничивайте ее в зависимости от ситуации.
- Не сообщайте персональную информацию незнакомым людям. Мошенники могут маскироваться под знакомых ваших родителей, дальних родственников или сотрудников банка, писать вам в соцсетях или даже позвонить.
- Пользуйтесь защитными решениями и определителями номеров, а также VPN, когда подключаетесь к неизвестным общественным Wi-Fi сетям.
- Не переходите по подозрительным ссылкам в социальных сетях, почте или мессенджерах, даже если их прислали знакомые.
- Когда устанавливаете приложения на смартфон, не давайте им доступ к тем функциям, которые им не нужны. Например, приложению «Фонарик» явно не нужен доступ к вашим фотографиям или камере.
- Скачивайте приложения и программы только из официальных магазинов приложений.
- Выходите из ваших аккаунтов после работы за школьными компьютерами или чужими устройствами.
- Если хотите разместить фотографию со своим другом, не забудьте уточнить у него, разрешает он вам это сделать или нет. То же самое просите делать и по отношению к вам.

- Используйте двухфакторную авторизацию — это способ защитить свой аккаунт от несанкционированного доступа, даже в том случае, если ваш логин и пароль знают злоумышленники. Обычно это выглядит так: первый рубеж — это логин и пароль, второй — специальный код, приходящий по SMS, в push-уведомлении или электронной почте.

Также давайте вспомним правила, которые касаются паролей. Пароль — это одна из важнейших составляющих вашей приватности. Чтобы пароль был сложным для взлома, нужно придерживаться следующих правил:

- Если связка логин/пароль «утекла», то как можно скорее поменяйте пароль. Как это узнать? Есть специальные сайты для проверки утечек учетных записей. Обращайте внимание на новости о том, в каких сервисах произошли утечки.
- Меняйте пароль регулярно.
- Пароль должен быть надежным: иметь минимум 12 символов, а также содержать прописные и строчные буквы, цифры, специальные символы.
- В пароле не должно быть общедоступной или личной информации, например, имени вашего питомца или номера телефона.
- Используйте разные уникальные пароли для разных сайтов.
- Не храните пароли на листочках, в текстовых файлах на компьютере. Для этого лучше использовать специальные программы — менеджеры паролей.

Если вам интересно узнать больше, про то, как защитить свою приватность в Интернете, заходите в блог «Лаборатории Касперского» (www.kaspersky.ru/blog/ и www.kids.kaspersky.ru), там вы найдете много полезных материалов на эту тему. Также в блоге рассказывается про

новые виды мошеннических схем и приложения для кражи персональных данных.

Цели и задачи урока

Цель урока:

Познакомить учащихся с понятиями «персональные данные», «приватность» и «конфиденциальность», сформировать теоретические знания и практические навыки безопасного поведения в сети Интернет и в реальной жизни.

Задачи урока:

- Сформировать устойчивое понимание вводимых на уроке понятий: «персональные данные», «приватность» и «настройки приватности».
- Изучить видеоролик, рассказывающий об информационной безопасности.
- Познакомить с правилами информационной безопасности, связанными с сохранением приватности.
- Развить навык предотвращения неприятных ситуаций.
- В онлайн-тренажере пройти набор заданий, связанных с информационной безопасностью.
- Обсудить полученный опыт, сформулировать выводы.

Подготовка к уроку:

- Пройти самостоятельно тренажер для соответствующего возраста на одном из компьютеров, которые будут использоваться учениками.
- Сохранить на компьютер видеоролик (на случай проблем с подключением к Интернету).
- Подготовить класс в соответствии с организационной информацией (Приложение 1).

- Изучить данный документ, сформулировать собственный план занятия на основе предложенного.

План урока

Этап	Содержание этапа	Время этапа
1. Анонс занятия	– Рассказать, что будет на уроке. – Сформулировать для учеников задачу на урок. – Обсудить понятия: «персональные данные», «приватность» и «настройки приватности».	5 мин
2. Просмотр вводного видеоролик	– Просмотреть видеоролик по теме урока. – Обсудить видеоролик и ответить на вопросы.	10 мин
3. Обсуждение новой темы	– Обсудить, почему важно сохранять приватность, как это сделать. – Обсудить, какие профессии существуют в сфере информационной безопасности.	5 мин
4. Работа за компьютером	– Продемонстрировать вход в тренажер. – Помогать ученикам при возникновении у них затруднений.	20 мин
5. Рефлексия	– Зафиксировать результат урока. – Задать домашнее задание.	5 мин

1. Анонс занятия (5 мин)

Поприветствуйте детей и анонсируйте урок:

«Добрый день! Сегодняшний урок проводится в рамках акции «Урок цифры» и посвящен теме «Приватность в цифровом мире». Что такое приватность? Как вы думаете?»

Дайте определение следующим понятиям: «приватность», «персональные данные», «конфиденциальность».

Сформулируйте цель урока:

«*Вы познакомитесь с понятием приватность, узнаете, почему важно хранить свои личные данные в секрете, как персональная информация попадает в Интернет, что с этими данными может сделать злоумышленник, и как предотвратить утечку персональной информации».*

2. Просмотр вводного видео ролика (10 мин)

Просмотрите вместе с детьми вводное видео:

«Давайте посмотрим вводное видео к уроку. В видеоролике эксперт «Лаборатории Касперского» по детской безопасности в Интернете расскажет: как персональные и личные данные попадают в Сеть, как злоумышленники могут этим воспользоваться, а также как уберечь персональные данные и настроить конфиденциальность. Попробуйте записать или запомнить правила информационной безопастности, о которых говорится в видео. Если появятся вопросы, запишите их, чтобы задать после просмотра».

Ответьте на вопросы, которые возникли у ребят после просмотра.

3. Обсуждение новой темы (5 мин)

Далее предложите ребятам вспомнить правила информационной безопасности, которые помогут сохранить приватность. Можно вызывать желающих к доске, чтобы они записывали свои варианты (если дети назвали меньше 4 правил, посмотрите видео еще раз):

- При регистрации на сайте, рассказывайте меньше о себе.
- В социальных сетях изучите «Настройки приватности».
- Ограничивайте информацию, которой хотите поделиться.
- Не сообщайте персональную информацию незнакомым людям.
- Не используйте открытые, неизвестные общественные Wi-Fi сети.
- Не переходите по подозрительным ссылкам, даже если их прислали знакомые.

- Обращайте внимание на разрешения, которые запрашивает устанавливаемое приложение.
- Скачивайте приложения и программы только из официальных магазинов приложений.
- Выходите из ваших аккаунтов после работы за школьными компьютерами или чужими устройствами.
- Если хотите разместить фотографию со своим другом, не забудьте получить у него разрешение.
- Используйте двухфакторную авторизацию там, где это возможно.
- Проверяйте связку логин/пароль на «утечку».
- Меняйте пароль регулярно.
- Пароль должен быть надежным: иметь минимум 12 символов, содержать прописные и строчные буквы, цифры, специальные символы.
- В пароле не должно быть общедоступной или личной информации.
- Используйте разные уникальные пароли для разных сайтов.
- Не храните пароли на листочках, в текстовых файлах на компьютере.

При проведении урока у учеников 5 класса и старше, предложите рассказать, сталкивался ли кто-то из ребят или их знакомых с тем или иным видом мошенничества, и что нужно делать в этом случае.

С учениками начальной школы обсудите, почему, например, опасно иметь одинаковый пароль от всех сервисов или выкладывать фотографии своих билетов. Комментируйте высказывания детей только после того, как они попробуют сформулировать мысль самостоятельно.

Если останется время, обсудите с ребятами, какие профессии существуют в сфере информационной безопасности (Приложение № 2).

4. Работа за компьютером (20 мин)

Продемонстрируйте интерфейс входа в тренажер, отправьте учеников за компьютеры. После выполнения своих заданий ребята могут выполнить задания для других возрастов.

Обращайте внимание на задания, которые вызывают наибольшие затруднения.

5. Рефлексия (5 мин)

«Что вам больше всего запомнилось? Кто прошёл все задания? Какое задание показалось вам самым интересным?»

Можно также разобрать задания, которые вызвали наибольшие затруднения.

Оценка активности ученика

Обратите внимание, что за прохождение тренажеров можно поставить оценку. Для этого предупредите учеников, что будете оценивать их активность. Чтобы заработать оценку, нужно пройти задание тренажера и поделиться результатом на странице соцсети (в конце каждого тренажера есть соответствующая кнопка). Если у вас есть ссылка на страницу школьника, тогда достаточно проверить, разместил ли ученик на странице публикацию с результатом прохождения задания.

Если у вас и вашего ученика нет возможности что-то размещать на странице соцсети, тогда вы можете попросить ученика отправить вам на почту принтскрин последнего уровня тренажера с итоговым результатом (набранными баллами).

Описание заданий, которые выполняются на платформе

Тренажер рассказывает правила и тренирует навыки информационной безопасности в увлекательной для школьников форме (приключенческая история).

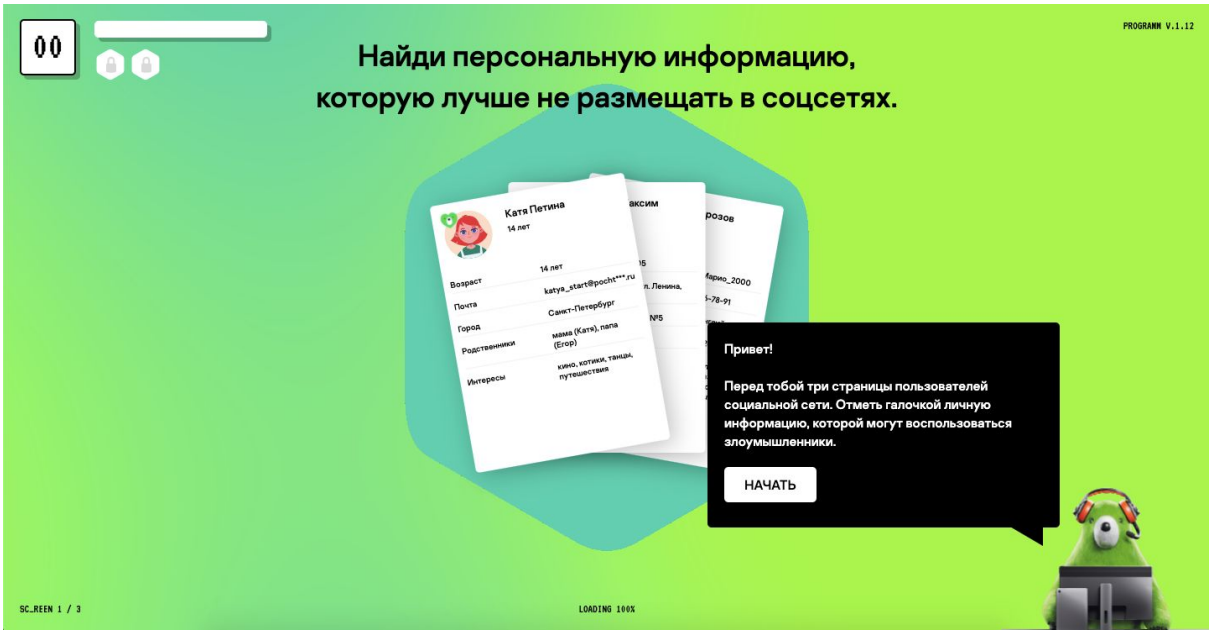
В начале тренажера вниманию ученика предлагается комикс. Основное действие происходит в «Академии безопасности», куда герои поступают на факультет «Защита персональных данных». Герои хотят стать кибердетективами. Для этого они должны успешно справиться с испытаниями, а именно выполнить задания тренажера. Для каждого задания разработана своя предыстория.

Герои урока:

- Персонажи из прошлогоднего «Урока цифры» (Запятыня, братья Слэши, Скобец, бабушка Слэшей).
- Второстепенным персонажем истории выступает маскот (персонаж-талисман) «Лаборатории Касперского» зеленый медведь Мидори Кума. Он рассказывает героям о правилах информационной безопасности.

Задание для 1–4 классов

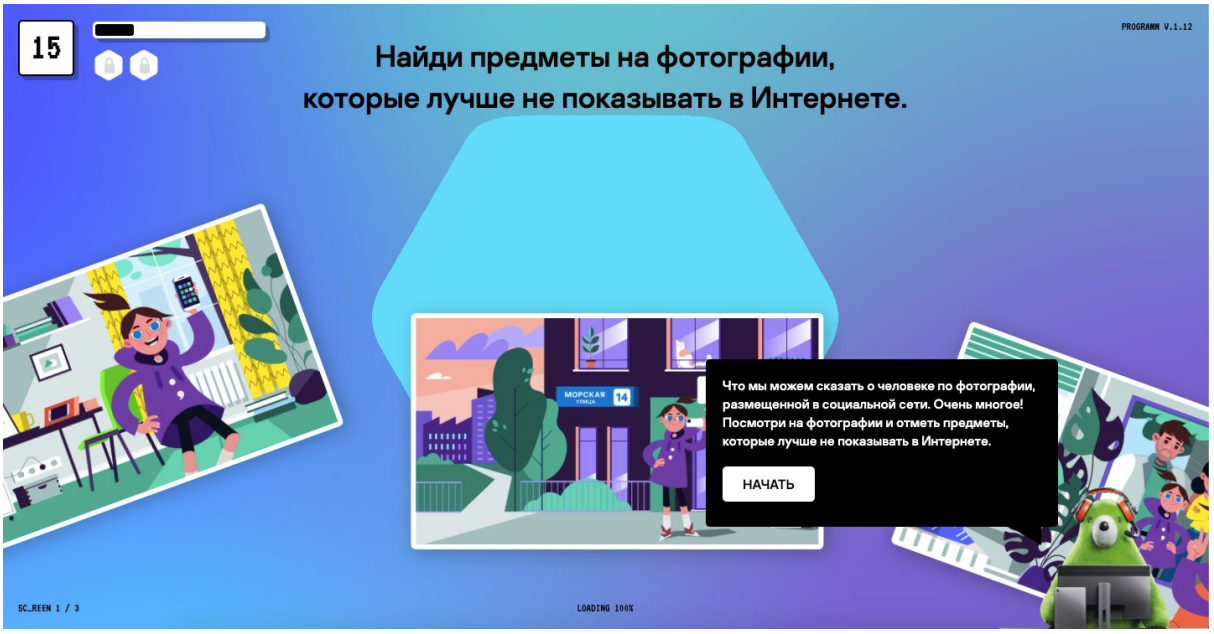
Уровень 1. «Овершеринг», часть 1



Перед учеником открываются три анкеты пользователей соцсети, в которых забыли установить настройки приватности. Нужно найти в этих анкетах персональную и личную информацию, которую лучше не

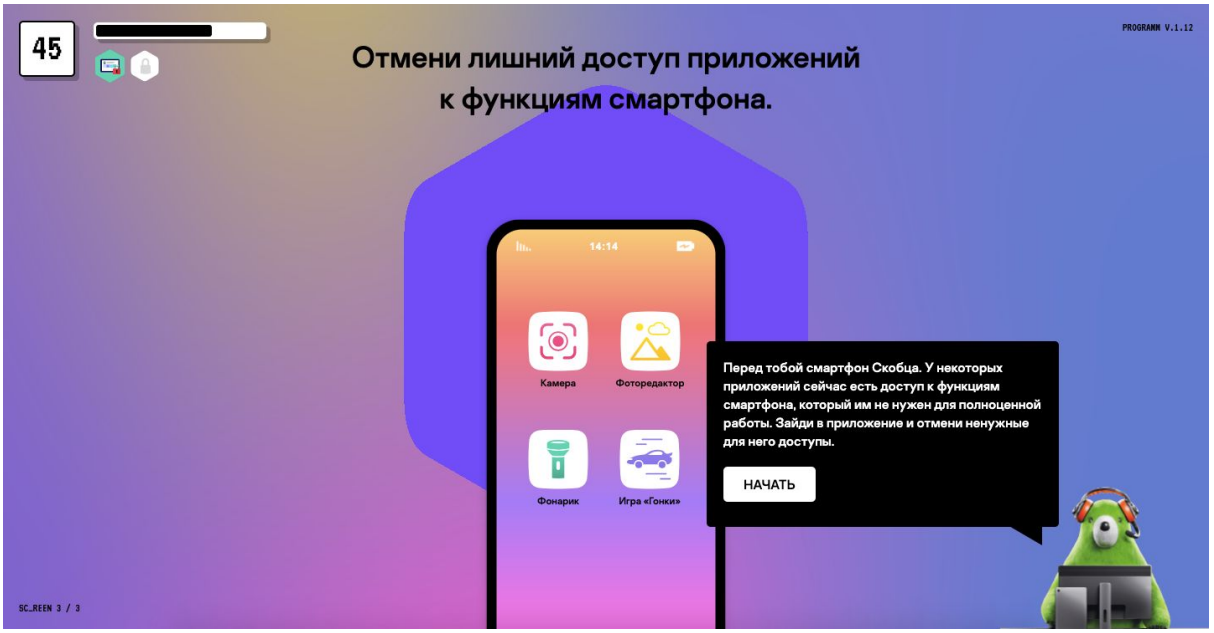
размещать в Интернете. Такой информацией может быть: телефонный номер, электронная почта, дата рождения и так далее.

Уровень 2. «Овершеринг», часть 2



На экране появляются фотографии, которые Запятыня разместила в соцсети. Ребятам нужно найти предметы, которые лучше не показывать посторонним людям. Например, это может быть стикер с паролем или паспорт родителя, случайно попавший в кадр.

Уровень 3. «Разрешения приложений»



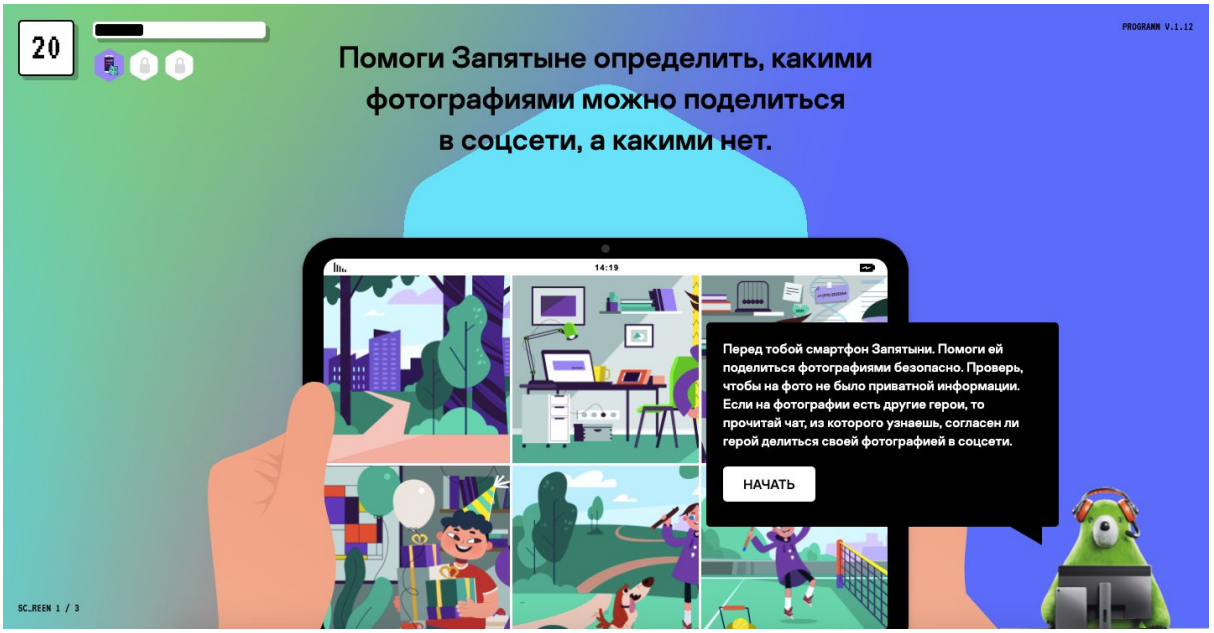
На экране отображается смартфон Скобца, на который установлены приложения, некоторые из которых имеют излишний доступ к функциям смартфона. Ученикам нужно определить, какие доступы к функциям смартфона надо отключить. Например, приложению «Фонарик» нужен доступ только к вспышке, но точно не к контактам.

Задание для 5–7 классов

Уровень 1. «Разрешения приложений»

Это копия уровня 3 из тренажера 1–4 классов.

Уровень 2. «Овершеринг»



Перед учеником находится планшет Запятыни с фотографиями, которыми она хочет поделиться. Ученикам нужно помочь выбрать фотографии, на которых нет лишней персональной информации. Также есть ряд фотографий, на которых запечатлены друзья Запятыни. Ученикам нужно ознакомиться с перепиской героев и понять, дали ли согласие другие герои на публикацию фотографии Запятыней.

Уровень 3. «Мошенничество»

Бабушка одного из персонажей чуть не попалась на уловки телефонного мошенника, который хотел украсть ее деньги. Герои хотят объяснить бабушке, каким образом мошенник хотел украсть ее деньги, чтобы она не попалась больше на уловки злоумышленников. Для этого им нужно заполнить схему, которая представлена на экране. Ученикам нужно расставить действия бабушки и мошенника по порядку.

Задание для 8–11 классов

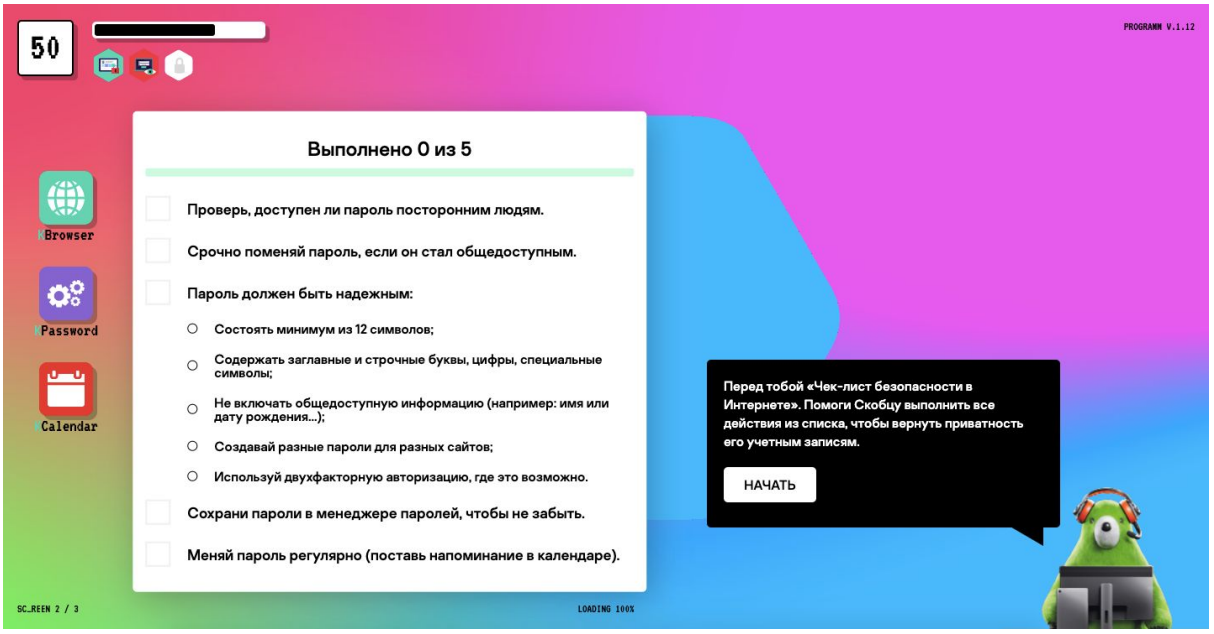
Уровень 1. «Овершеринг»

Это копия уровня 2 из тренажера 5–7 классов.

Уровень 2. «Мошенничество»

Это копия уровня 3 из тренажера 5–7 классов.

Уровень 3. «Настройка приватности»



Экран тренажера — рабочий стол компьютера Скобца. В этом уровне ученикам нужно помочь Скобцу восстановить приватность его учетных записей, которые были скомпрометированы. Для этого понадобится сделать ряд действий, которые представлены в чек-листе.

Приложение 1. Технические требования для проведения урока

Рекомендуемая конфигурация ПК учеников для работы в тренажере:

1. Процессор Intel Core.
2. ОЗУ 4Gb.
3. Монитор с разрешением от 1024x768 до 1920x1080.
4. OS:
   - Windows 7 и новее,
   - macOS 10.13 High Sierra и новее,
   - iOS 10 и новее,
   - Android 4.4 и новее.
5. Доступ в Интернет: не менее 10 Mbit/s.
6. Браузер:
   - Google Chrome 60 и новее,
   - Safari 11 и новее (за исключением Safari for Windows),
   - Opera 44 и новее,
   - Яндекс.Браузер 17.4 и новее.

При использовании мониторов минимального разрешения необходимо применять функцию масштабирования браузера: (Ctrl + «-», Ctrl + «стрелка вниз»).

Вне зависимости от используемой конфигурации рекомендуется до урока открыть и пройти тренажер на компьютере ученика для проверки совместимости.

В случае невозможности использования тренажера в формате онлайн, необходимо провести урок по сценарию методических рекомендаций по проведению урока без Интернета (методические рекомендации находятся на сайте «Урока цифры»).

Приложение 2. Профессии в области информационной безопасности

Консультант по безопасности личного профиля

Проводит проверку активностей и данных клиента в Сети на предмет уязвимостей и помогает обеспечить конфиденциальность и общую безопасность. В том числе помогает настроить приватность профиля в социальных сетях, отредактировать или удалить лишнюю информацию.

Исследователь мобильных угроз

Анализирует работу мобильных приложений и операционных систем в смартфонах и планшетах. Помогает распознать вредоносные программы, которые могут маскироваться под мобильные игры и другие приложения.

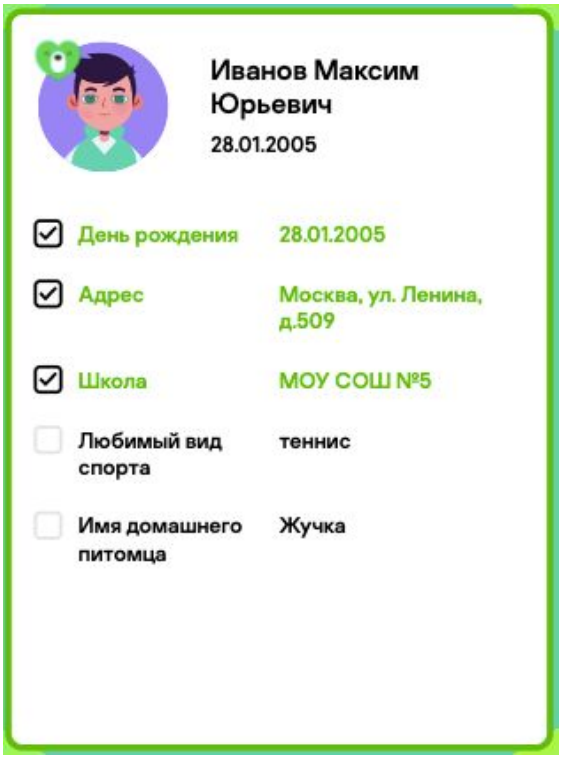
Веб-контент аналитик

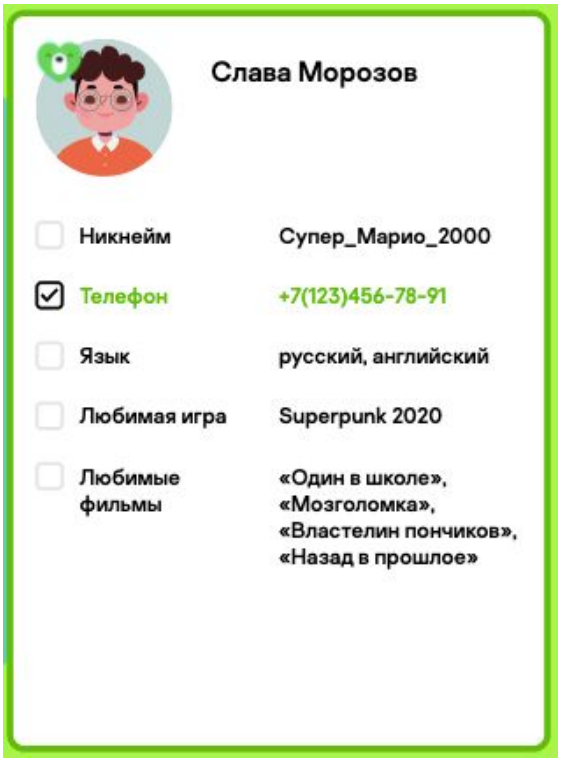
Изучает сайты и сервисы с точки зрения возможности кражи персональной и платежной информации пользователя. Анализирует и раскрывает мошеннические схемы (мошенничество, фишинг, спам). Помогает улучшить информационную безопасность для банков, интернет-магазинов и многих других компаний.

Эксперт по кибербезопасности

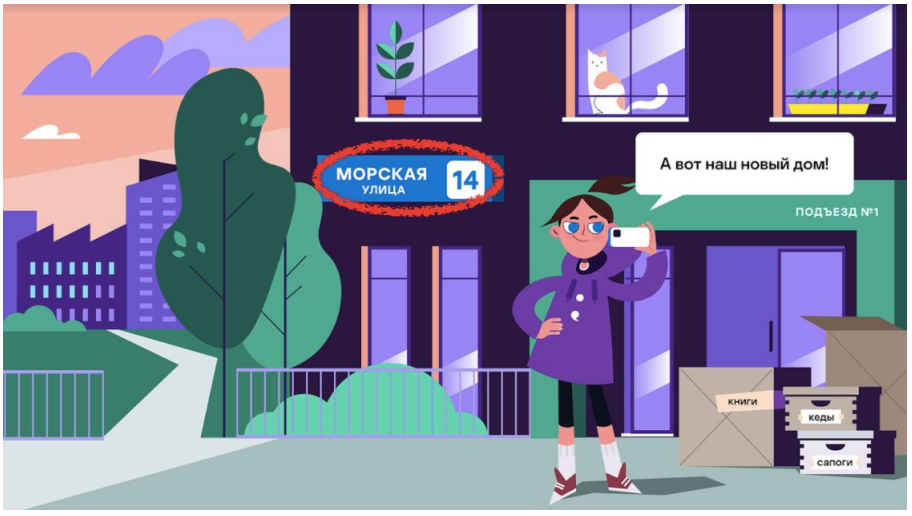
Разрабатывает правила информационной безопасности для частных лиц и компаний. Анализирует возможные киберугрозы и помогает с ними бороться, участвует в совершенствовании защитных решений.

Приложение 3. Решение задания 1–4 классов «Овершеринг», часть 1

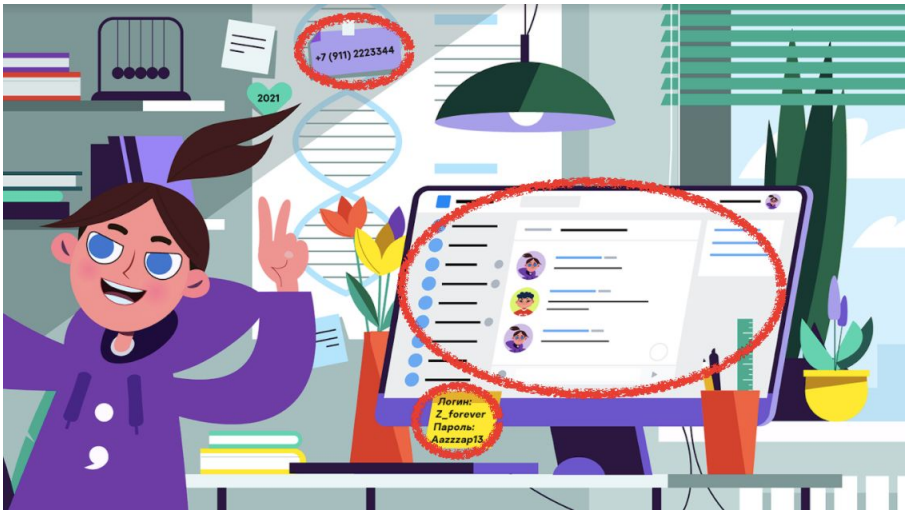




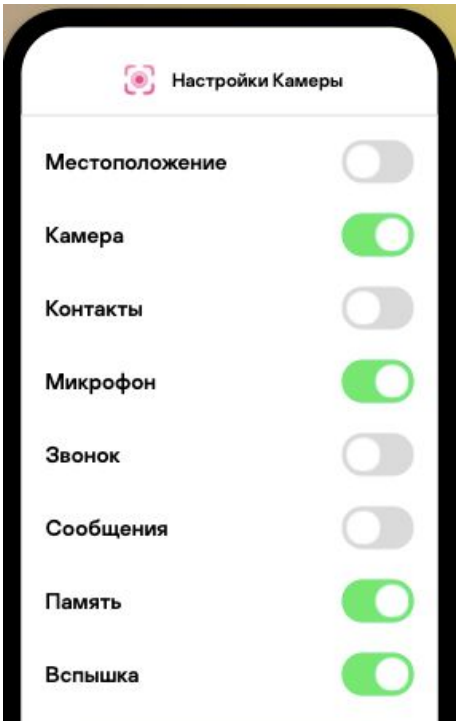
Приложение 4. Решение задания 1–4 классов «Овершеринг», часть 2

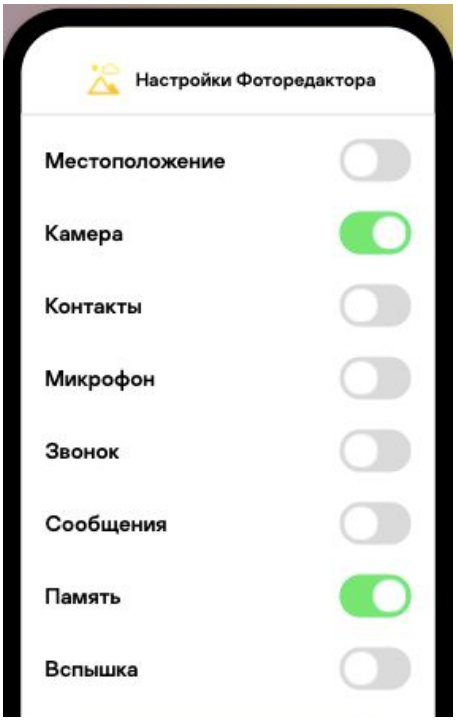


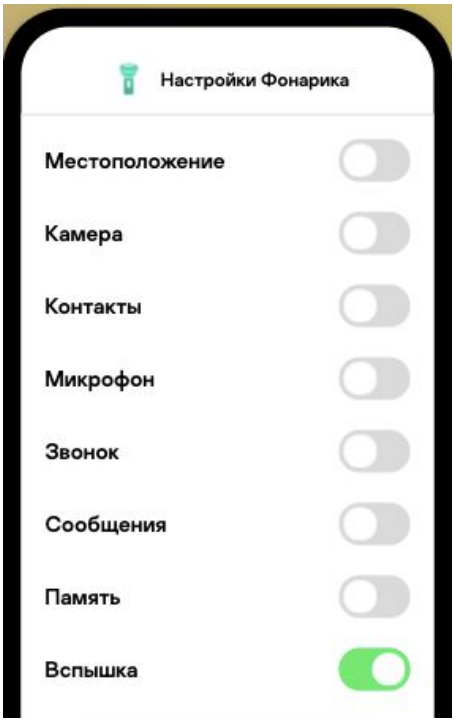

УРА!
СЛЕШ♥
15

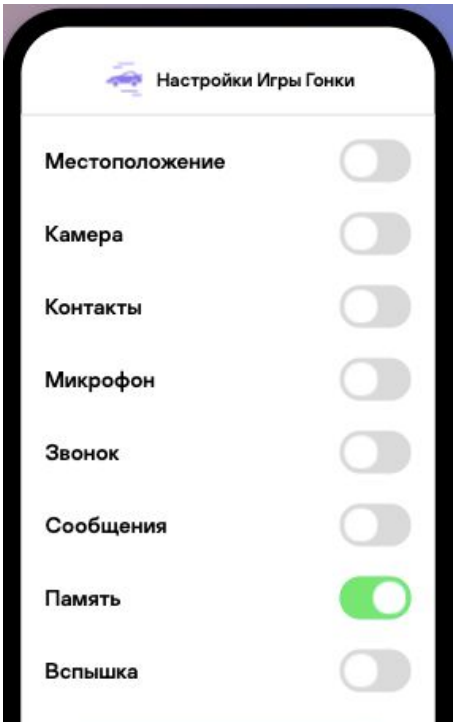

+7 (911) 2223344
2021
Логин:
Z_forever
Пароль:
Aazzzap13

Приложение 5. Решение задания 1–7 классов «Разрешения приложений»

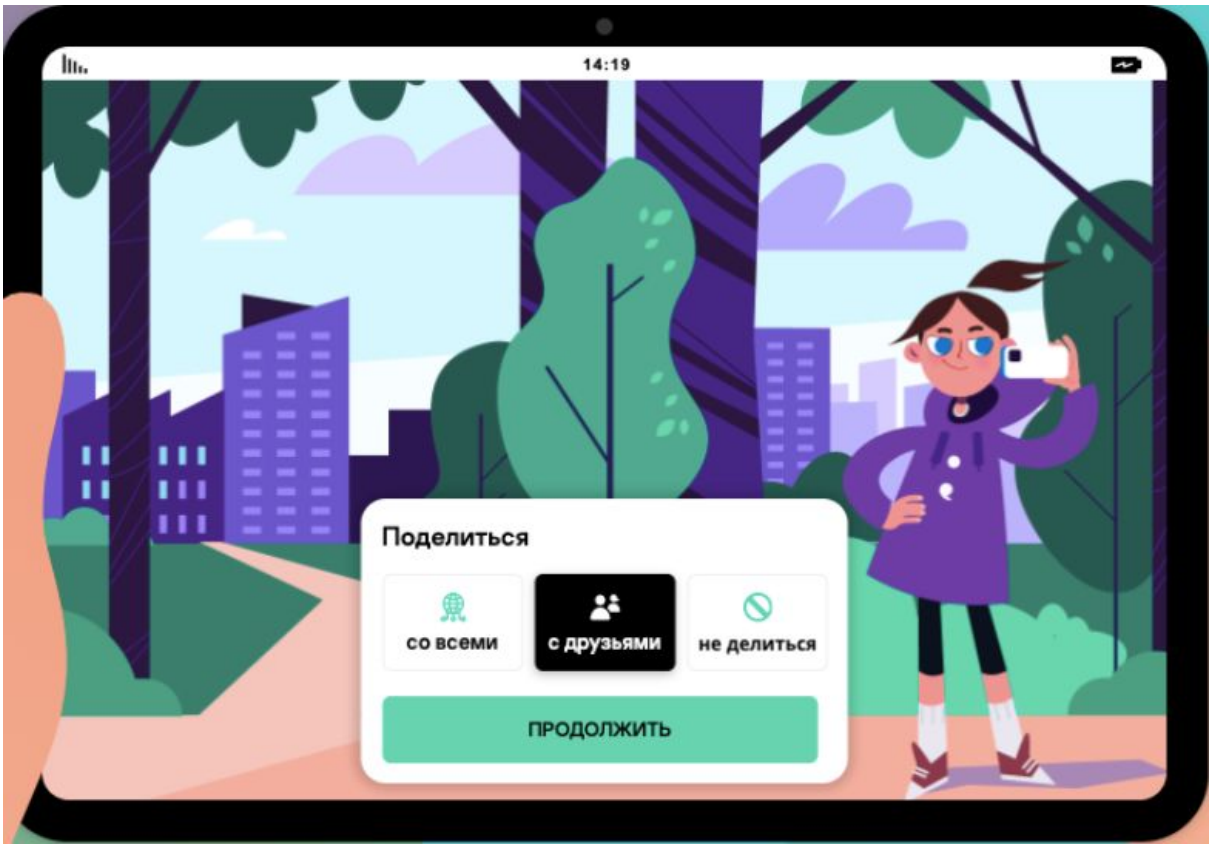


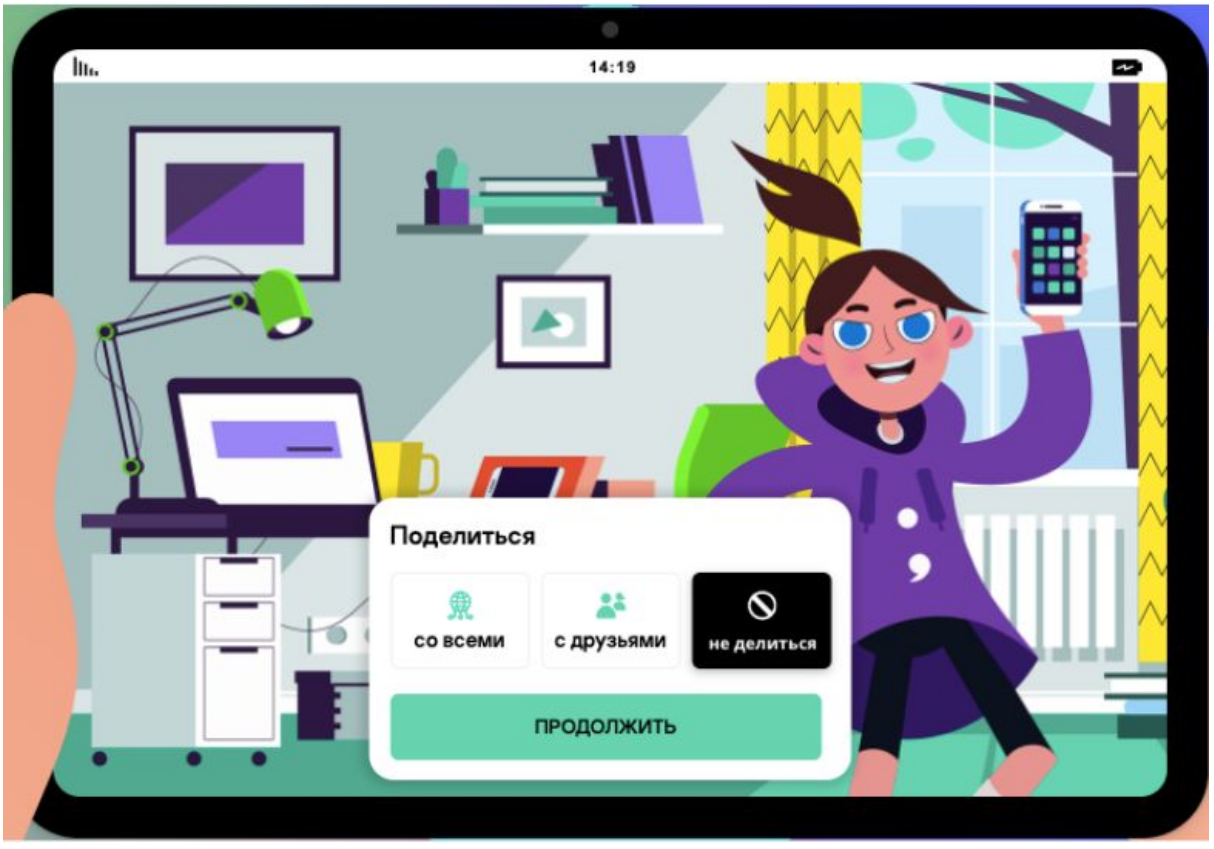


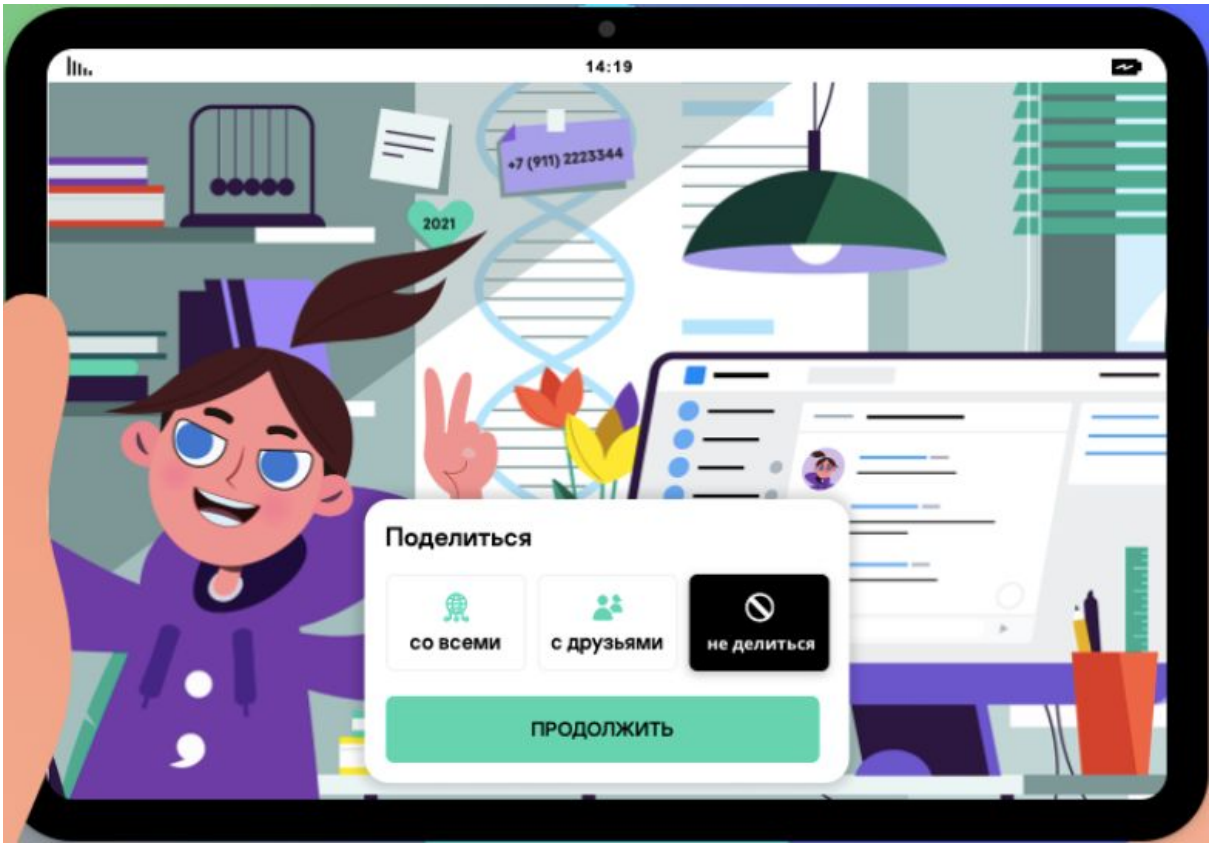


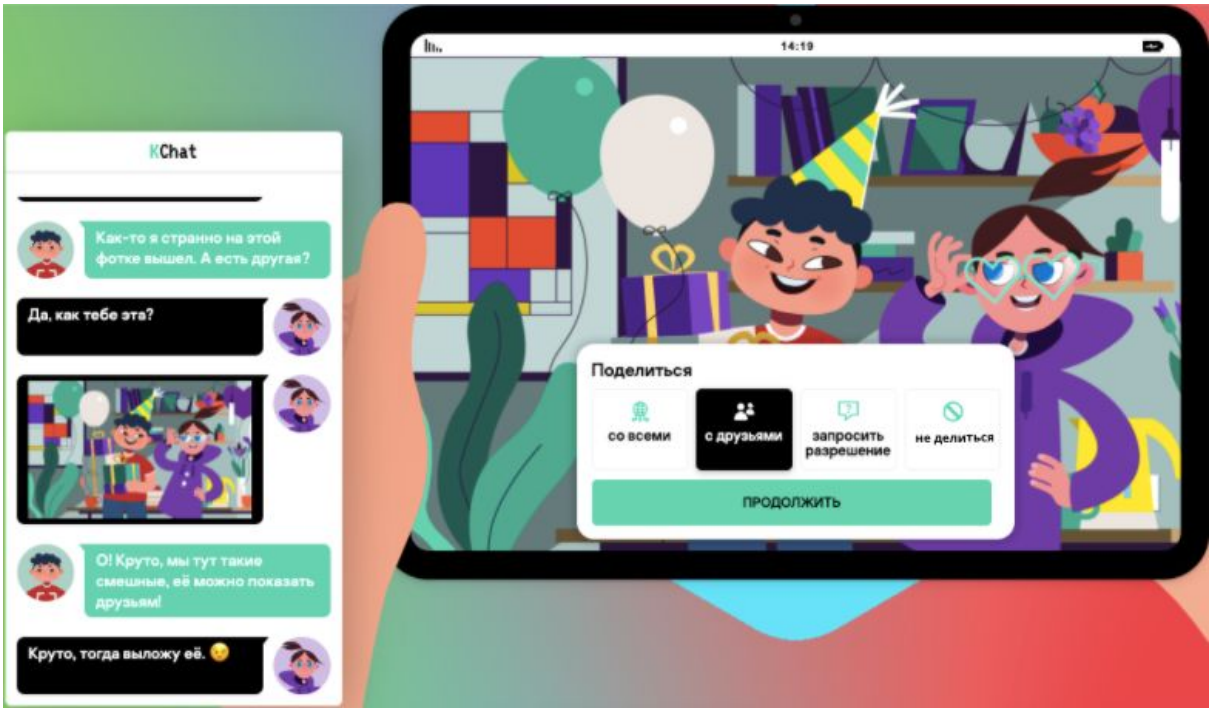


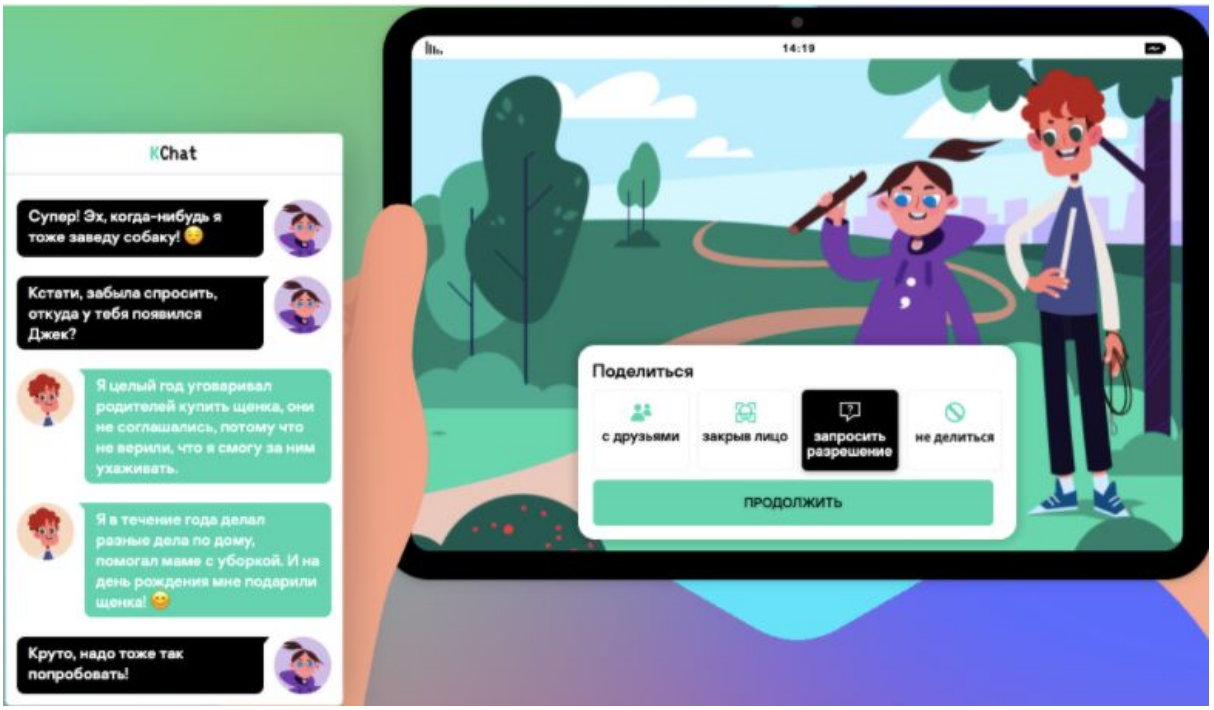
Приложение 6. Решение задания 5–11 классов «Овершеринг»

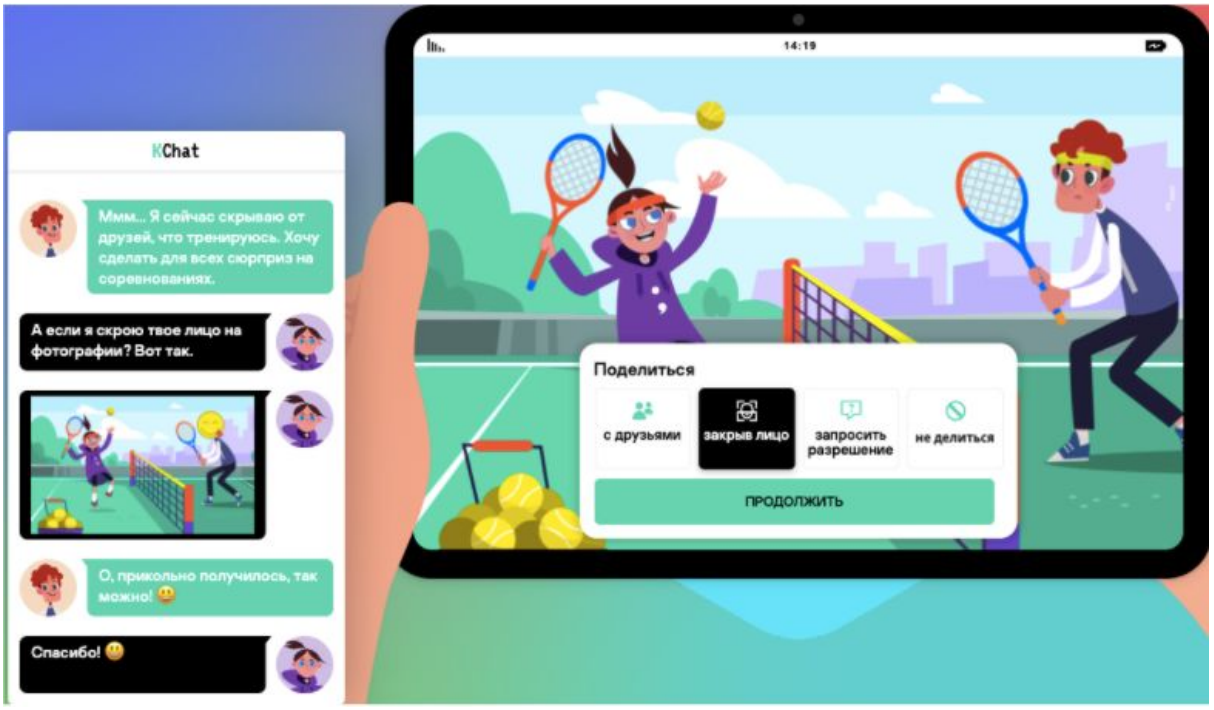




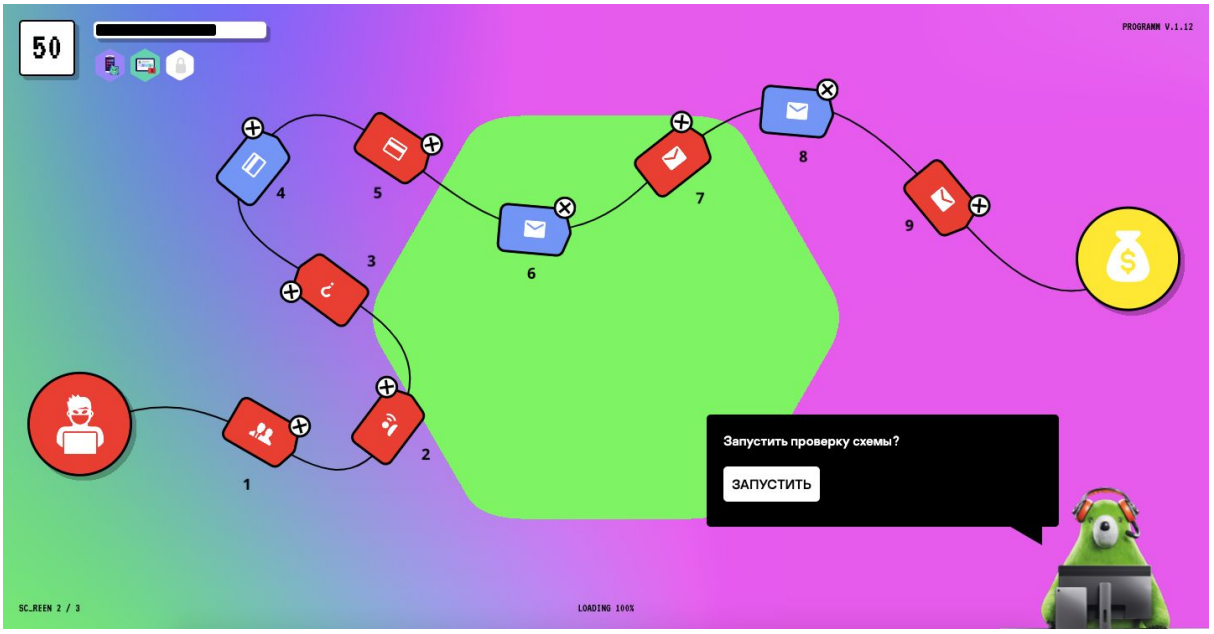

14:19
+7 (911) 2223344
2021
Поделиться
со всеми
с друзьями
не делиться
ПРОДОЛЖИТЬ


KChat
Как-то я странно на этой фотке вышел. А есть другая?
Да, как тебе эта?
О! Круто, мы тут такие смешные, её можно показать друзьям!
Круто, тогда выложу её.
14:19
Поделиться
со всеми
с друзьями
запросить разрешение
не делиться
ПРОДОЛЖИТЬ


KChat
Супер! Эх, когда-нибудь я тоже заведу собаку!
Кстати, забыла спросить, откуда у тебя появился Джек?
Я целый год уговаривал родителей купить щенка, они не соглашались, потому что не верили, что я смогу за ним ухаживать.
Я в течение года делал разные дела по дому, помогал маме с уборкой. И на день рождения мне подарили щенка!
Круто, надо тоже так попробовать!
14:19
Поделиться
с друзьями
закрыв лицо
запросить разрешение
не делиться
ПРОДОЛЖИТЬ

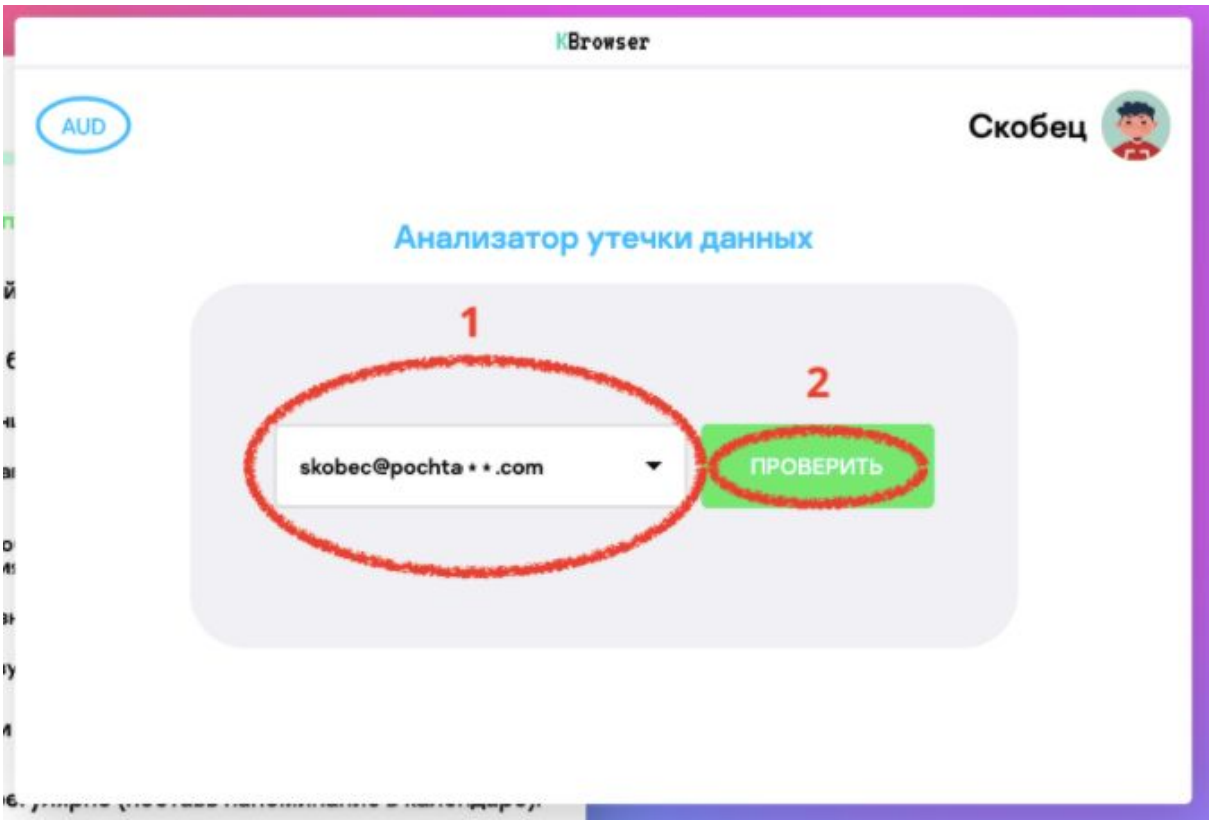

KChat
Ммм... Я сейчас скрываю от друзей, что тренируюсь. Хочу сделать для всех сюрприз на соревнованиях.
А если я скрою твое лицо на фотографии? Вот так.
О, прикольно получилось, так можно!
Спасибо!
14:19
Поделиться
с друзьями
закрыв лицо
запросить разрешение
не делиться
ПРОДОЛЖИТЬ

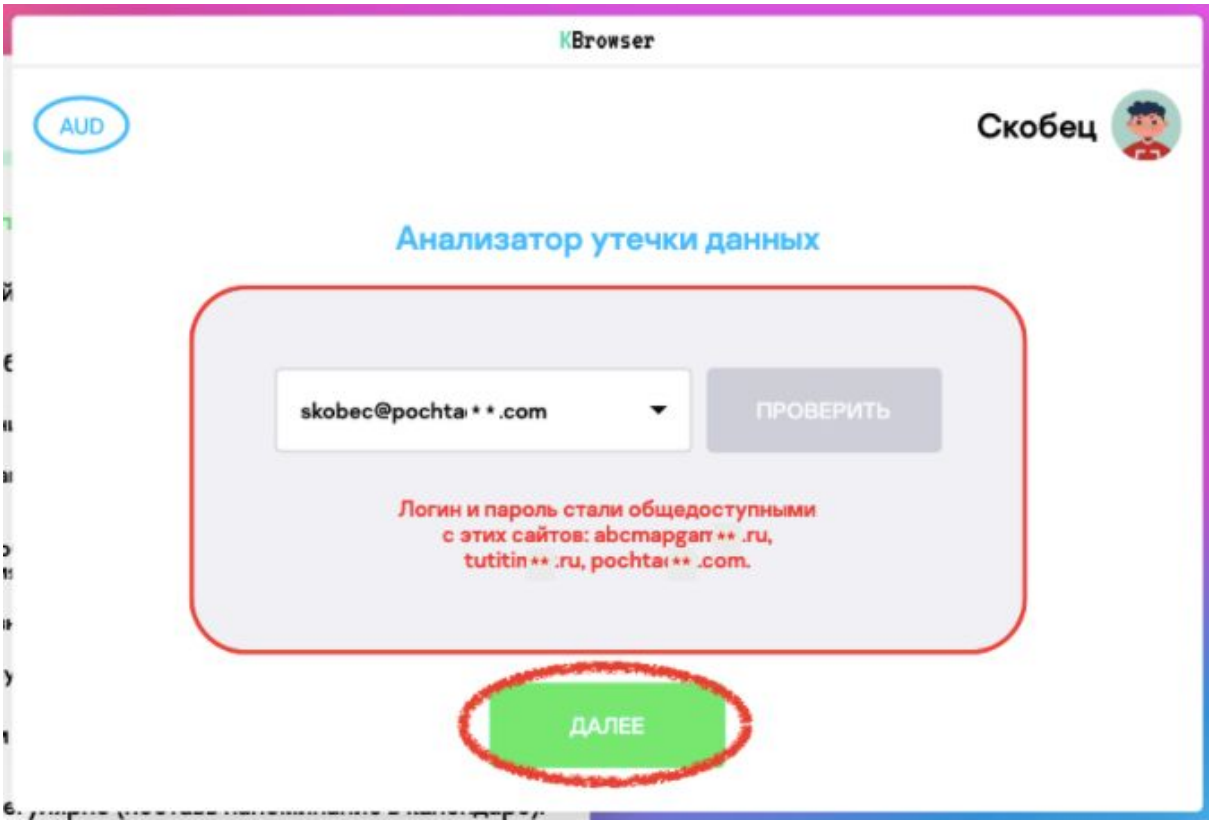
Приложение 7. Решение задания 5–11 классов «Мошенничество»

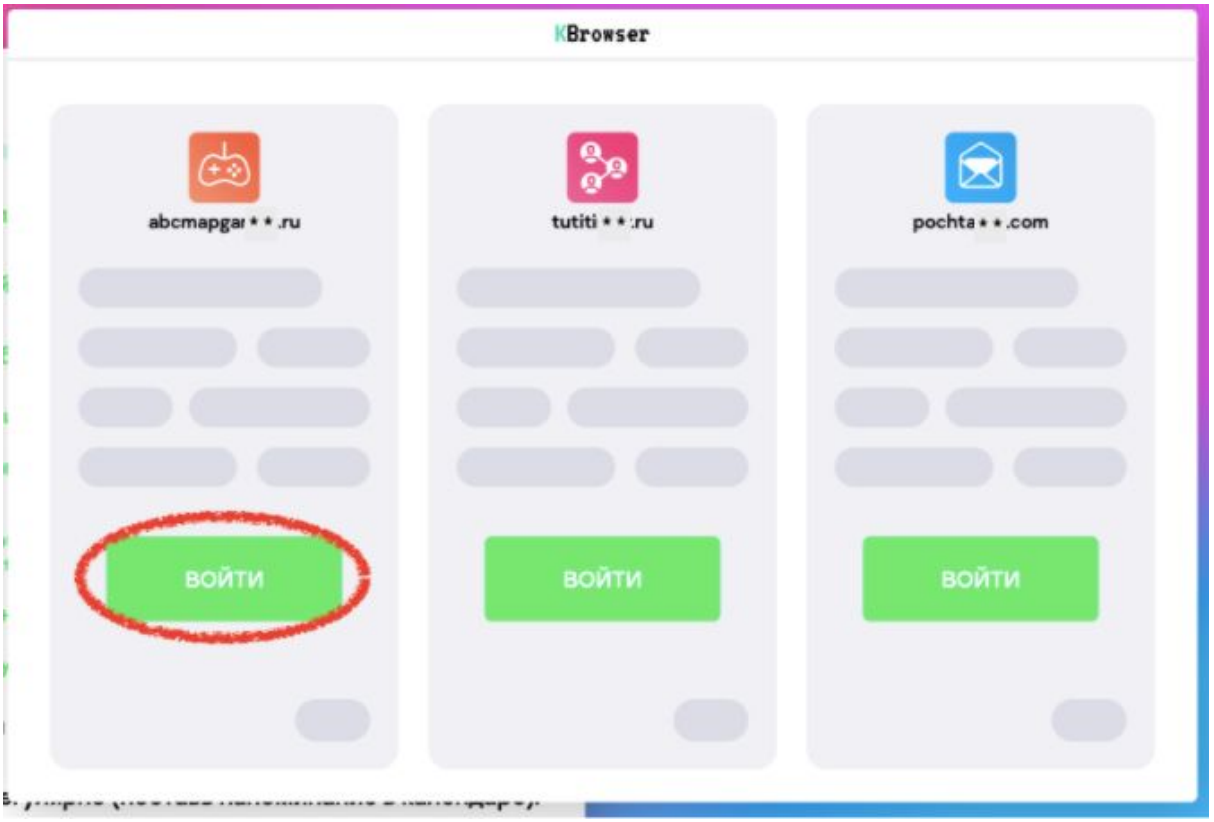


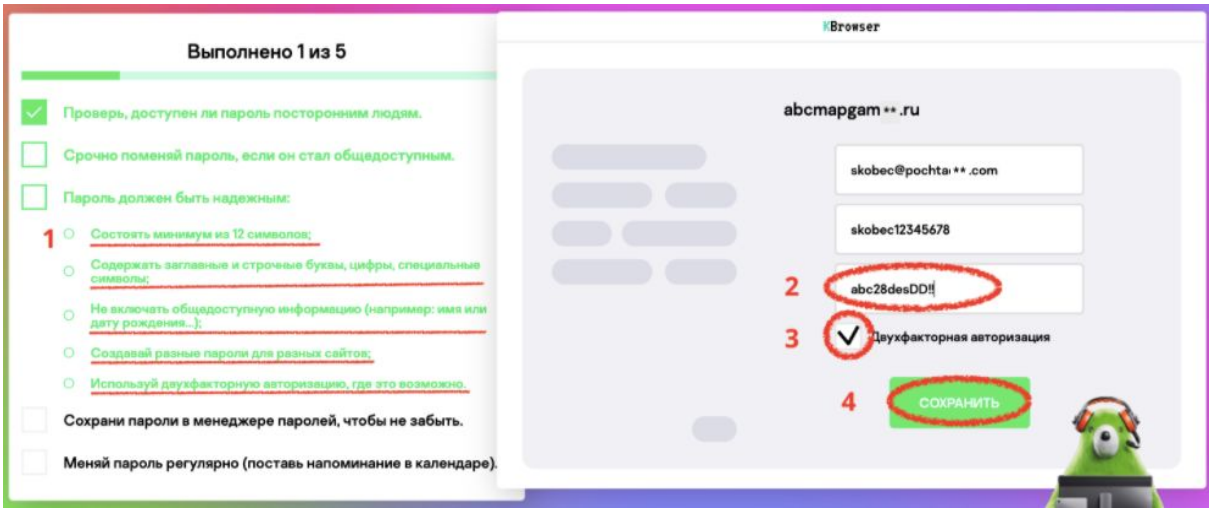
1. Злоумышленник: Звонит. Представляется сотрудником банка.
2. Злоумышленник: Рассказывает «историю» про взлом карты.
3. Злоумышленник: Задает вопросы, чтобы узнать платежную информацию.
4. Пользователь: Сообщает платежную информацию (номер карты, дату, CVV-код).
5. Злоумышленник: Вводит данные карты в форму для перевода денег.
6. Пользователь: Получает СМС от банка или push-уведомление с паролем для завершения перевода.
7. Злоумышленник: Просит сообщить код из СМС или push-уведомления.
8. Пользователь: Сообщает код мошеннику.
9. Злоумышленник: Вводит код и завершает денежный перевод.

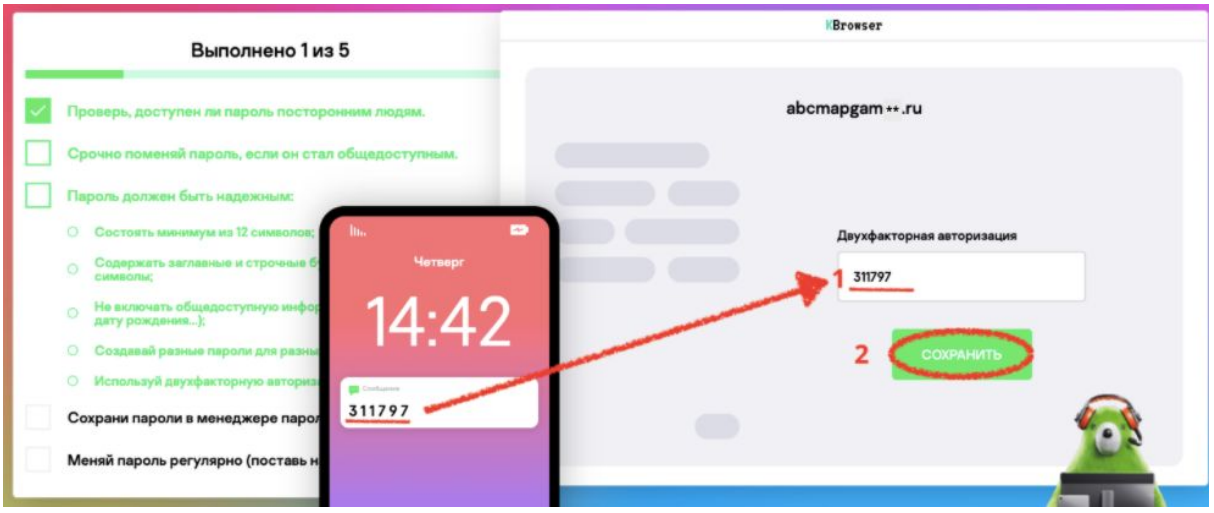
Приложение 8. Решение задания 8–11 классов «Настройка приватности»

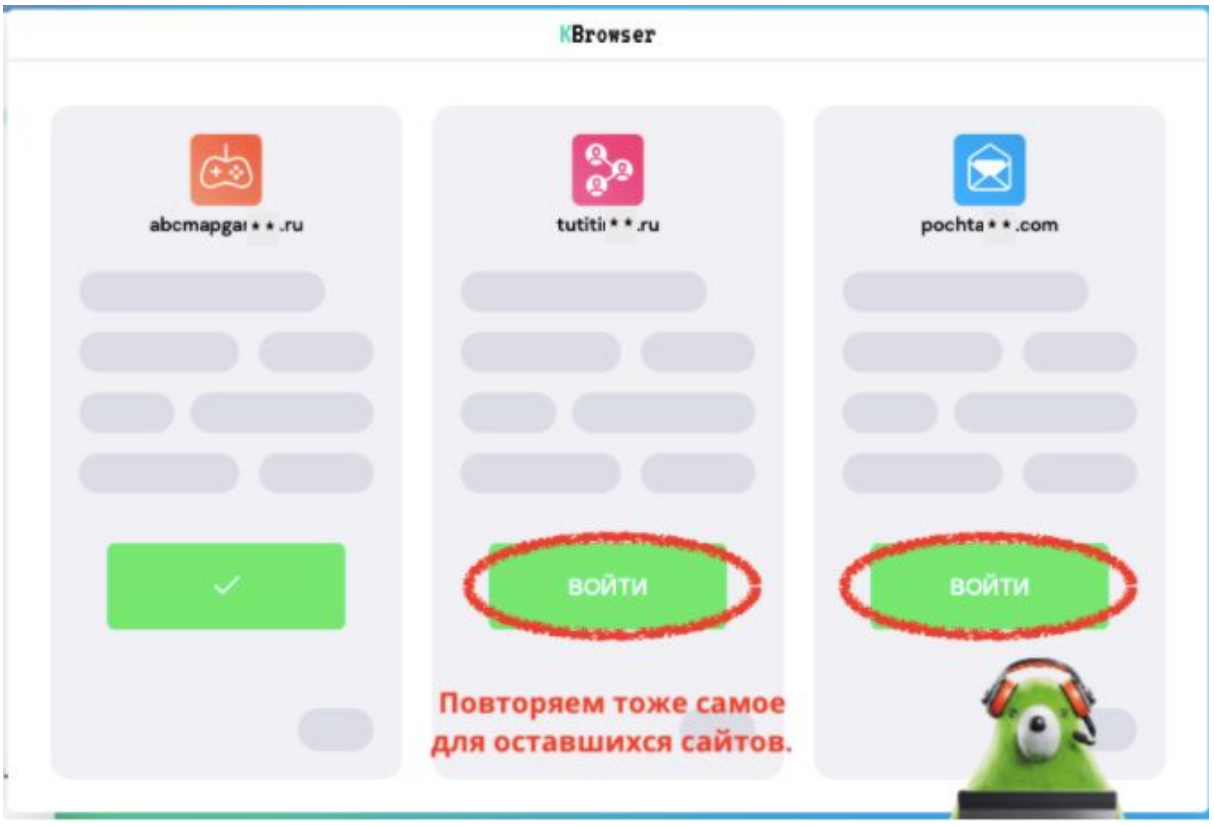




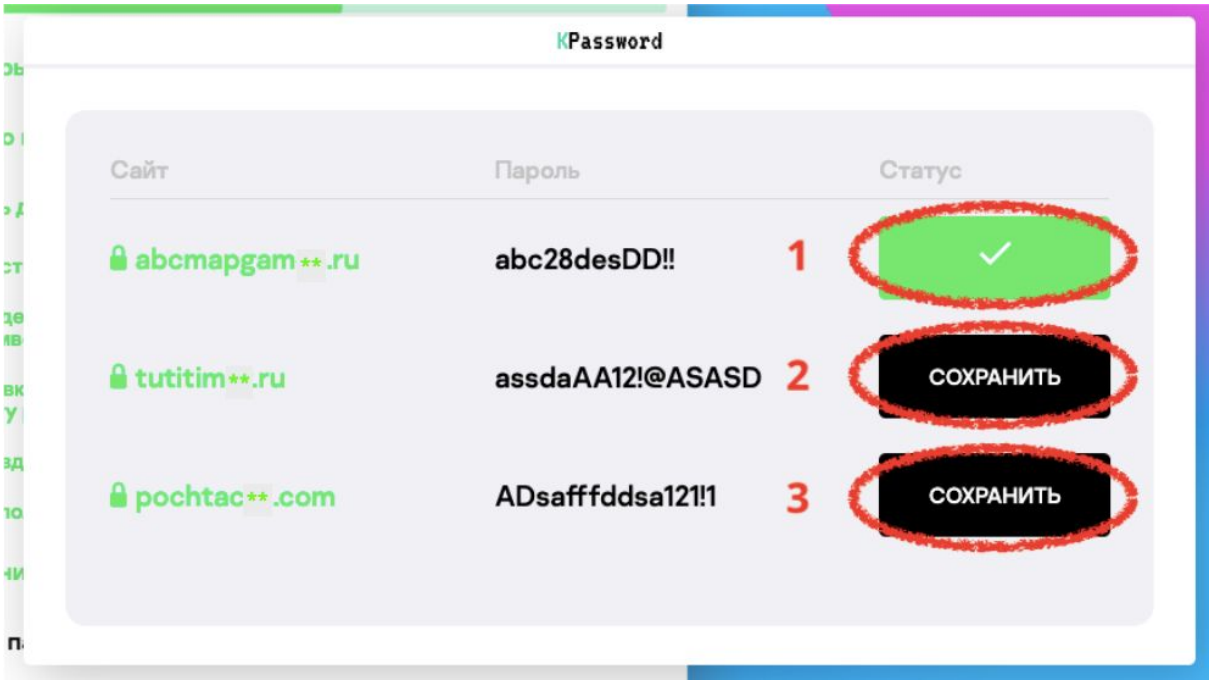

KBrowser
abcmapgar * * .ru
tutiti * * .ru
pochta * * .com
ВОЙТИ
ВОЙТИ
ВОЙТИ

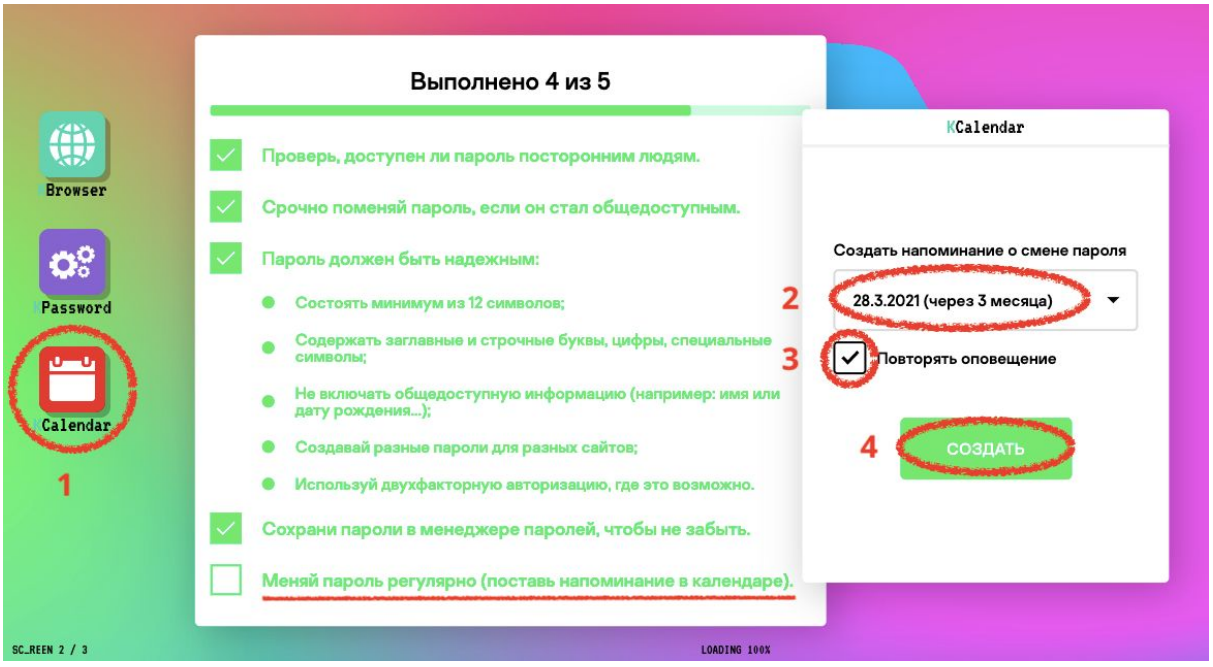

Выполнено 1 из 5
Проверь, доступен ли пароль посторонним людям.
Срочно поменяй пароль, если он стал общедоступным.
Пароль должен быть надежным:
1
Состоять минимум из 12 символов;
Содержать заглавные и строчные буквы, цифры, специальные символы;
Не включать общедоступную информацию (например: имя или дату рождения...);
Создавай разные пароли для разных сайтов;
Используй двухфакторную авторизацию, где это возможно.
Сохрани пароли в менеджере паролей, чтобы не забыть.
Меняй пароль регулярно (поставь напоминание в календаре).
KBrowser
abcmapgam ** .ru
skobec@pochta ** .com
skobec12345678
2
abc28desDD!!
3
Двухфакторная авторизация
4
СОХРАНИТЬ


Выполнено 1 из 5
Проверь, доступен ли пароль посторонним людям.
Срочно поменяй пароль, если он стал общедоступным.
Пароль должен быть надежным:
Состоять минимум из 12 символов;
Сохрани пароли в менеджере паро
Меняй пароль регулярно (поставь н
Четверг
14:42
311797
KBrowser
abcmapgam**.ru
Двухфакторная авторизация
1
311797
2
СОХРАНИТЬ


KBrowser
abcmapga**.ru
tutiti**.ru
pochta**.com
ВОЙТИ
ВОЙТИ
Повторяем тоже самое
для оставшихся сайтов.


KBrowser
KPassword
KCalendar
Выполнено 3 из 5
Проверь, доступен ли пароль посторонним людям.
Срочно поменяй пароль, если он стал общедоступным.
Пароль должен быть надежным:
Состоять минимум из 12 символов;
Содержать заглавные и строчные буквы, цифры, специальные символы;
Не включать общедоступную информацию (например: имя или дату рождения...);
Создавай разные пароли для разных сайтов;
Используй двухфакторную авторизацию, где это возможно.
Сохрани пароли в менеджере паролей, чтобы не забыть.
Меняй пароль регулярно (поставь напоминание в календаре).


KPassword
Сайт
Пароль
Статус
abcmapgam**.ru
abc28desDD!!
1
tutitim**.ru
assdaAA12!@ASASD
2
СОХРАНИТЬ
pochtac**.com
ADsafffddsa121!1
3
СОХРАНИТЬ


Browser
Password
Calendar
1
Выполнено 4 из 5
Проверь, доступен ли пароль посторонним людям.
Срочно поменяй пароль, если он стал общедоступным.
Пароль должен быть надежным:
Состоять минимум из 12 символов;
Содержать заглавные и строчные буквы, цифры, специальные символы;
Не включать общедоступную информацию (например: имя или дату рождения...);
Создавай разные пароли для разных сайтов;
Используй двухфакторную авторизацию, где это возможно.
Сохрани пароли в менеджере паролей, чтобы не забыть.
Меняй пароль регулярно (поставь напоминание в календаре).
KCalendar
Создать напоминание о смене пароля
2
28.3.2021 (через 3 месяца)
3
Повторять оповещение
4
СОЗДАТЬ
SC_REEN 2 / 3
LOADING 100%