УРОК ЦИФРЫ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по организации и проведению в школах Российской Федерации тематического урока «Кибербезопасность будущего» в рамках Всероссийской образовательной акции «Урок Цифры»

Москва, 2024

Содержание

Аннотация

Методические рекомендации разработаны для помощи педагогам в проведении занятий и уроков в рамках Всероссийской образовательной акции «Урок Цифры» по теме «Кибербезопасность будущего». Акция «Урок Цифры» имеет просветительскую направленность, способствует развитию цифровых навыков, популяризации передовых технологических направлений среди школьников, раннему профессиональному самоопределению. Тематика урока посвящена основным правилам кибербезопасности и проблемам в этой области.

Методические рекомендации по проведению «Урока Цифры» по теме «Кибербезопасность будущего» будут полезны представителям администрации образовательных организаций общего и дополнительного образования, учителям информатики, математики, классным руководителям, педагогам дополнительного образования, педагогам коммерческих кружков, а также преподавателям и студентам педагогических вузов.

В основу методических рекомендаций положен успешный практический опыт компании в организации стажировок safeboard.kaspersky.ru, тематических уроков и лекций. Про накопленный опыт и экспертизу по теме детской безопасности в сети можно подробнее узнать на kids.kaspersky.ru.

Методические рекомендации содержат ссылки на материалы для проведения «Урока Цифры» по теме «Кибербезопасность будущего», которые находятся в открытом доступе на сайте акции «Урок Цифры» и могут быть успешно использованы педагогами дополнительного образования и школьными учителями не только для проведения «Урока Цифры», но и для проведения занятий, классных часов, профориентационных мероприятий, мастер-классов и других мероприятий для обучающихся

Общие понятия кибербезопасности

Кибербезопасность — это набор процессов, передовых практик и технологий, которые помогают защитить критически важные системы и сети от цифровых атак. По мере распространения данных и увеличения числа людей, работающих и подключающихся к сети из разных точек, злоумышленники стали разрабатывать изощренные методы получения доступа к ресурсам и кражи данных, саботажа бизнеса или вымогательства денег. С каждым годом количество атак увеличивается, а преступники разрабатывают новые методы уклонения от обнаружения. Эффективная программа кибербезопасности охватывает людей, процессы и технологические решения, которые в совокупности снижают риск нарушения работы компании, финансовых потерь и репутационного ущерба в результате атаки.

Типы угроз кибербезопасности

Угроза кибербезопасности — это преднамеренная попытка получить доступ к информационной системе пользователя или организации. Злоумышленники постоянно совершенствуют свои методы атак, чтобы обойти инструменты обнаружения и использовать новые уязвимости, но при этом они используют и некоторые известные методы, к противодействию которым можно подготовиться.

1. Вредоносные программы

Вредоносные программы — общий термин для всего вредоносного ПО, в том числе червей, программ-шпионов и вирусов. Их цель — нанесение ущерба компьютерам или сетям путем изменения или удаления файлов, извлечения конфиденциальных данных, таких как пароли и номера счетов, или отправки вредоносных электронных писем или трафика.

2. Фишинг

Фишинг — вид интернет-мошенничества, цель которого — получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации. Также фишинг — это вид социотехники, при котором используются сообщения электронной почты, а также текстовые или голосовые сообщения, отправленные якобы из надежных источников. Они помогают убедить людей сообщить конфиденциальную информацию или перейти по незнакомой ссылке.

3. Программы-вымогатели

Программа-вымогатель — вредоносное ПО, которое шифрует данные или блокирует доступ к ним и требует заплатить за снятие блокировки или дешифровку файлов. Существуют программы-вымогатели как для настольных систем, так и для мобильных устройств.

4. **Внутренние угрозы**

При внутренней угрозе причиной нарушения безопасности или финансовых потерь становятся люди, уже имеющие доступ к некоторым системам, например сотрудники, подрядчики или клиенты. Иногда это происходит непреднамеренно, например когда сотрудник случайно размещает конфиденциальную информацию в личной облачной учетной записи.

5. **Социальная инженерия**

Социальная инженерия подразумевает манипуляции действиями человека без использования технических средств. В контексте кибербезопасности это незаметное принуждение пользователя сделать что-то, что подвергает риску его безопасность или безопасность организации, в которой он работает.

Успех в значительной степени зависит от удачной маскировки вредоносных и нежелательных сообщений под легитимные (в некоторых могут быть даже советы по борьбе с киберпреступностью).

Цель — вызвать ответную реакцию у жертвы: щелкнуть по зараженному вложению электронной почты, перейти по вредоносной ссылке или ответить на ложное уведомление.

6. **Дипфейк**

Дипфейк — реалистичная подмена фото-, аудио- и видеоматериалов, созданная с помощью нейросетей. Атакующие могут использовать биометрические данные, полученные без ведома их владельцев или полностью сгенерированные ИИ. Также дипфейк-атаки включают социальную инженерию. Например, ИИ имитирует официальное лицо или старшего по должности и от их имени направляет запрос сотруднику на перевод денег.

Почему кибербезопасность важна?

В современном мире всё связано между собой как никогда раньше. Глобальная экономика зависит от того, как люди остаются на связи, находясь в разных часовых поясах, и получают доступ к важной информации из любой точки мира. Кибербезопасность обеспечивает производительность, давая людям уверенность в том, что они могут работать и общаться в интернете без нарушения доступности, целостности и конфиденциальности. Правильные решения и процессы позволяют предприятиям и правительствам использовать преимущества технологий для улучшения коммуникации и предоставления услуг, не увеличивая риск атак.

Умный дом и умные помощники

Роботы-пылесосы, смарт-холодильники, голосовые колонки, автоматические системы освещения — это технологии, которые уже полноправно вошли в жизнь человека. Они значительно упрощают быт, освобождая время. Но приборы сами по себе не делают дом умным, ведь концепция smart home — это целая система.

Умный дом — это гибкая автоматическая система, которую пользователь конструирует и настраивает в соответствии со своими потребностями. Владелец сам определяет, какие устройства и где установить. Умный дом делает повседневную жизнь проще и позволяет не переживать о не закрытой в спешке двери или невыключенном утюге. Чаще всего в умном доме регулируются видеонаблюдение, освещение, отопление, также настраивается климат-контроль, и это лишь малая часть технологических возможностей. Автоматизация систем преследует три основные цели: обеспечение безопасности, экономия ресурсов, повышение комфорта.

Система умного дома включается в себя три типа устройств:

- Контроллер — мозг системы, принимающий сигналы от датчиков и дающий команды исполнителям. Это ключевой элемент системы — центр управления, который соединяет все части системы друг с другом с возможностью удаленного доступа. Он собирает и обрабатывает информацию со всех датчиков и оборудования, раздает задачи приборам согласно программе. Через него же осуществляется удаленный доступ к системе.

- Датчики — принимают информацию из внешнего мира и дают соответствующие сигналы. Например, датчик протечек реагирует при контакте с водой. Датчики следят за событиями в доме, отправляют оповещения, участвуют в разработанных пользователем сценариях.

- Актуаторы — исполнительные устройства, получают команды от контроллера или датчика и исполняют их по сценарию, созданному пользователем. Это умные розетки; выключатели; сирены; электрические реле, включающие и выключающие по сигналу свет в помещении.

Носимые устройства

Носимые технологии, также известные как носимые устройства, — это категория электронных устройств, которые можно носить как аксессуары, встраивать в одежду или даже татуировать на коже. Эти устройства представляют собой гаджеты, имеющие практическое применение, работающие на микропроцессорах и обладающие способностью отправлять и получать данные через интернет.

Как работают носимые технологии?

Носимые технологии включают в себя микропроцессор и подключаются к интернету. Изначально популярность среди потребителей завоевали трекеры фитнес-активности. По мере развития технологий наручные часы превратились в экраны, способные работать с надежными мобильными приложениями. Гарнитуры Bluetooth, смарт-часы и очки с веб-интерфейсом позволяют людям получать данные из сетей Wi-Fi. Игровая индустрия также внесла свой вклад в развитие носимых устройств, выпустив гарнитуры виртуальной и дополненной реальности.

Примеры носимых технологий

В последние годы активно разрабатываются и внедряются носимые технологии, адаптированные для использования в медицине и здравоохранении. Вот некоторые примеры:

1. Носимые устройства, используемые для мониторинга качества местного воздуха, измерения уровня загрязняющих веществ и определения «горячих точек» для жителей с заболеваниями дыхательных путей.
2. Интеллектуальный пластырь, который может обнаруживать ранние признаки рака груди и передавать информацию в лабораторию для анализа.
3. Носимые мониторы медицинского оповещения: эти устройства повышают мобильность и независимость пожилых и ослабленных людей.
4. Умные татуировки: гибкие электронные датчики, встроенные в умные татуировки, разрабатываются для мониторинга сердечной и мозговой активности, нарушений сна и работы мышц.
5. Отслеживание болезни Паркинсона: специализированные смарт-часы отслеживают симптомы болезни Паркинсона и передают данные, позволяя разрабатывать индивидуальные планы лечения.

Будущее носимых технологий

Потенциал носимых технологий огромен, и их будущее таит в себе захватывающие возможности. Может быть, по мере развития технологий мы можем ожидать дальнейшего прогресса в области медицины, позволяющего осуществлять более точный и персонализированный мониторинг и лечение. Кроме того, носимые технологии могут найти применение в различных отраслях, таких как спорт, развлечения, мода и транспорт.

В России носимые технологии способны произвести революцию в здравоохранении, повысить безопасность на рабочем месте и улучшить повседневную жизнь. Благодаря развитию возможностей подключения и аналитики данных носимые устройства могут способствовать развитию умных городов и оптимизации различных процессов.

Важно отметить, что по мере того, как носимые технологии все больше интегрируются в нашу повседневную жизнь, необходимо будет решать вопросы, связанные с конфиденциальностью, безопасностью данных и этическими последствиями.

Цели, задачи, подготовка к уроку

Основной целью акции «Урок Цифры» по теме «Кибербезопасность будущего» является создание условий для развития у школьников интереса к проблемам кибербезопасности и их потенциальное вовлечение в изучение этой сферы через:

- знакомство с общими понятиями кибербезопасности;
- пробуждение интереса к проблемам и правилам кибербезопасности;
- погружение в технологии, используемые в сферах, связанных с кибербезопасностью;
- знакомство с перспективами развития кибермедицины, умного дома и инвазивных технологий.

Задачи урока:

- познакомить школьников с основными проблемами и задачами, которые стоят перед сотрудниками области кибербезопасности;
- познакомить школьников с профессиональной деятельностью в области технологий, связанных с кибербезопасностью;
- погрузить школьников в современные кибертехнологии.

Рекомендации для проведения урока

Подготовка к уроку для проведения в классе:

- самостоятельно воспользоваться тренажером для соответствующего возраста на одном из компьютеров, которые будут использоваться учениками;
- просмотреть памятку к уроку;
- просмотреть опорные конспекты для учащихся;
- посмотреть видеоролик по теме «Кибербезопасность будущего»;
- сохранить на компьютер видеоролик с сайта урокцифры.рф;
- подготовить кабинет к уроку;
- изучить данный документ, сформулировать собственный план занятия на основе предложенного.

Рекомендации для проведения урока в классе без доступа в интернет

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.

Подготовка к уроку:

- изучить данный документ, посмотреть видеолекцию и презентацию к уроку
- сохранить заранее видеоролик и презентацию на компьютере с доступом в Интернет
- подготовить опорные конспекты и ручки по количеству учеников
- подготовить кабинет к уроку
- сформулировать собственный план занятия на основе предложенного.

Общие рекомендации по работе в онлайн-формате

1. Настройте платформу для проведения урока так, чтобы включать микрофоны учащихся могли только вы, например по поднятию руки. Это обеспечит вам тишину на занятии, но и оставит возможность задавать вопросы.

2. Заранее проверьте звук своего микрофона и возможность писать в чате.
3. Убедитесь, что учащиеся могут видеть ваш экран с опорной презентацией и видео.
4. Запланируйте время на проверку технических моментов в начале урока.
5. Поставьте часы в зоне видимости, чтобы посвятить нужное количество времени каждому этапу урока.

Рекомендации по проведению урока
«Кибербезопасность будущего» в онлайн-формате

1. Заранее разошлите ссылку на тренажер и проверьте, что все задания открываются корректно.
2. Разошлите опорные конспекты и определитесь, будут ли учащиеся заполнять их сами в качестве домашнего задания или заполнение будет происходить по ходу урока.
3. Для 1–4 и 5–8 классов убедитесь, что вы можете показать тренажер и решить задания вместе с учащимися.
4. Заранее продумайте время обсуждений с учащимися и количество человек, которых сможете опросить по каждому из вопросов опорной презентации.

Предлагаемый план занятия

Этап	Содержание этапа	Длительность этапа
1. Организационная часть	Приветствуем учащихся и проверяем их готовность к уроку	2,5 мин.
2. Анонс занятия	Формулируем для учеников задачу на урок (можно взять формулировки из данных методических рекомендаций) Обсуждаем основные понятия темы	10 мин.
3. Просмотр вводного видео	Смотрим видеоролик по теме «Кибербезопасность будущего»	10 мин.
4. Обсуждение нового материала	Обсуждаем просмотренный ролик Отвечаем на вопросы учащихся	5 мин.
5. Работа за компьютером	Демонстрируем вход в тренажер Помогаем ученикам при возникновении у них затруднений	15 мин.
6. Рефлексия	Фиксируем результат урока	2,5 мин.

Ожидаемые практические результаты

В результате проведения акции «Урок Цифры» ожидается, что у участников урока будет инициирован интерес к профессиям в области кибертехнологий, к сферам применения этих технологий в жизни. Привлечение внимания школьников к данной тематике является стратегически важным для государства и общества результатом, потому как кибербезопасность является важной отраслью развития современного мира.

Развитие интереса к изучению проблем и правил кибербезопасности — важный образовательный результат, поэтому, погружая школьников в современные достижения и проблемы, связанные с цифровыми технологиями, необходимо формировать правильное отношение к фундаментальной и прикладной науке, показывать, как они связаны с развитием экономики, улучшают качество жизни и работы людей. Важно сформировать у обучающихся знания об основных правилах кибербезопасности, а также способствовать развитию общей научной культуры, понимания связи между развитием науки и экспериментальными фактами, лежащими в основе этого развития.

Педагогические техники и методические приемы при проведении «Урока Цифры» ориентированы на формирование у обучающихся навыков регулятивных универсальных учебных действий через вовлечение их в деятельность по постановке целей, выбор способа их достижения, участие в ситуативной рефлексии в конце занятия, что является одной из основных задач, сформулированных в Федеральном государственном образовательном стандарте общего образования.

«Урок Цифры» ориентирован на развитие универсальных учебных действий:

- продуктивное сотрудничество и совместная деятельность с одноклассниками и учителем;
- работа в группе, умение находить общее решение и разрешать конфликты на основе согласования позиций и учета интересов;
- умение формулировать, аргументировать и отстаивать свое мнение;
- умение классифицировать, обобщать, сравнивать, выявлять закономерности и противоречия в рассматриваемых фактах;
- умение оценить себя, усвоенный материал и объем того, что еще предстоит изучить.

Основные содержательные аспекты урока

Весь комплекс теоретических и практических материалов, разработанных к уроку, направлен на привлечение внимания школьников к теме кибертехнологий и к областям их применения. Тема достаточно сложная, требует от педагогов понимания сути технологий, осведомленности о существующих современных разработках, умения привести примеры и обсудить их с учениками.

В ходе урока целесообразно показать, что внедрение кибертехнологий способно качественно изменить многие сферы жизни.

Сегодня существует достаточно много интересных и прорывных разработок в предлагаемой области, которые могут уже в ближайшем будущем лечь в основу решений для многих сфер жизни.

Важно донести до школьников, что кибертехнологии охватывают все сферы деятельности и будут внедряться повсеместно; в каждой отрасли, в том числе и в образовании, будут востребованы специалисты, владеющие этими технологиями. Также необходимо заострить внимание на важности соблюдения правил кибербезопасности.

Список полезных материалов и первоисточников

1. Детская безопасность — kids.kaspersky.ru
2. Блог «Лаборатории Касперского» — kaspersky.ru/blog/
3. YouTube-канал «Лаборатории Касперского» —youtube.com/@KasperskyRussia
4. Что такое кибербезопасность — kaspersky.ru/resource-center
5. Что такое умный дом — kaspersky.ru/resource-center
6. Носимые технологии — kaspersky.ru/about
7. Энциклопедия «Лаборатории Касперского» — encyclopedia.kaspersky.ru
8. Проверка пароля — password.kaspersky.com

Список материалов к «Уроку Цифры» по теме «Кибербезопасность будущего»

1. Методические рекомендации по организации и проведению в школах Российской Федерации тематического урока «Кибербезопасность будущего» в рамках Всероссийской образовательной акции «Урок Цифры».

2. Памятка для учителей.

3. Рекомендации для родителей.

4. Опорная презентация педагога для проведения «Урока Цифры»:

   - 1–4 классы;
   - 5–8 классы;
   - 9–11 классы.

5. Интерактивные практические задания:

   - 1–4 классы;
   - 5–8 классы;
   - 9–11 классы.

6. Опорный конспект для учащихся:

   - 1–4 классы;
   - 5–8 классы;
   - 9–11 классы.

Приложение 1. Технические требования

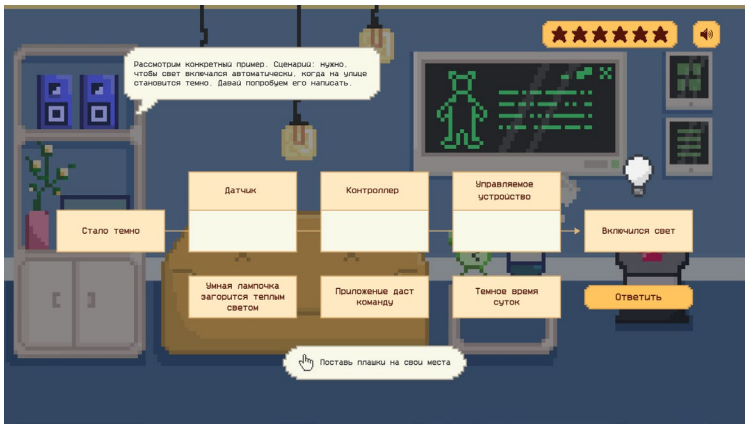
Рекомендуемая конфигурация ПК учеников для работы в тренажере:

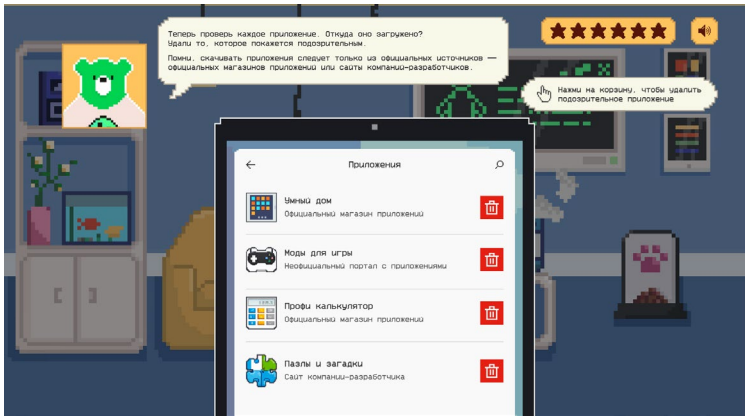
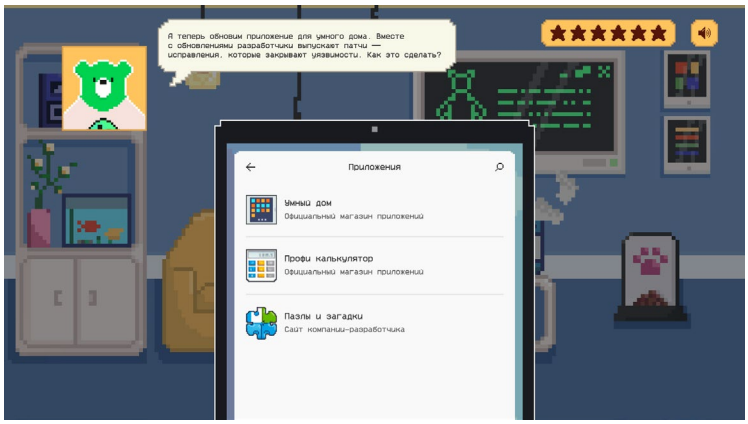
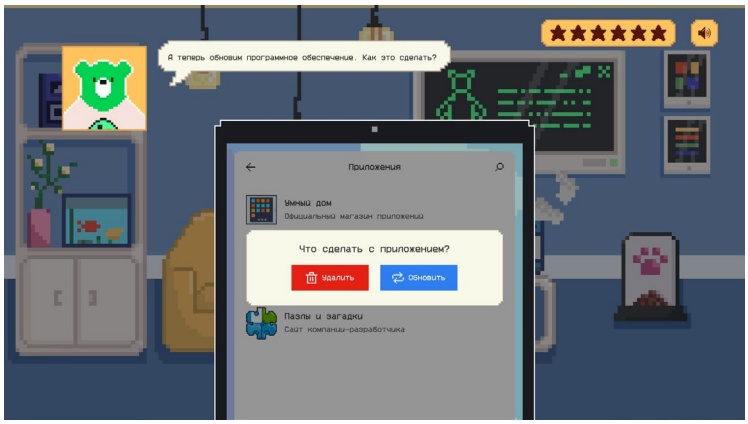
- Процессор Intel Core.
- ОЗУ 4 Гб.
- Монитор с разрешением от 1024 × 768 до 1920 × 1080.
- OS:
  - Windows 7 и новее;
  - macOS High Sierra 10.13 и новее;
  - iOS 10 и новее;
  - Android 4.4 и новее.
- Доступ в интернет — не менее 10 Мбит/с.
- Браузер:
  - Google Chrome 60 и новее;
  - Safari 11 и новее (за исключением Safari for Windows);
  - Opera 44 и новее;
  - Яндекс.Браузер 17.4 и новее.

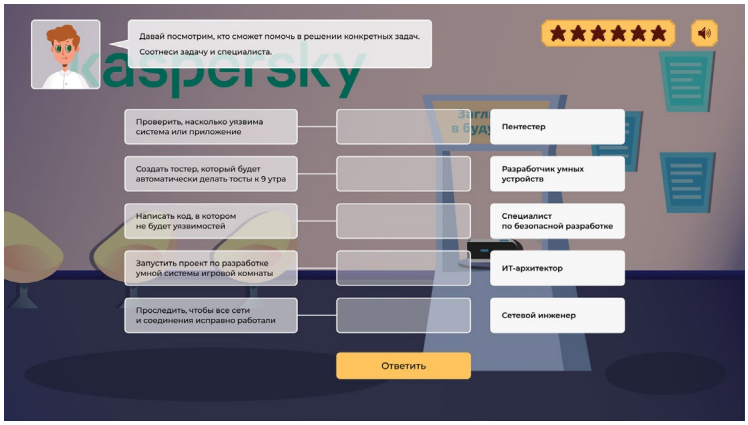
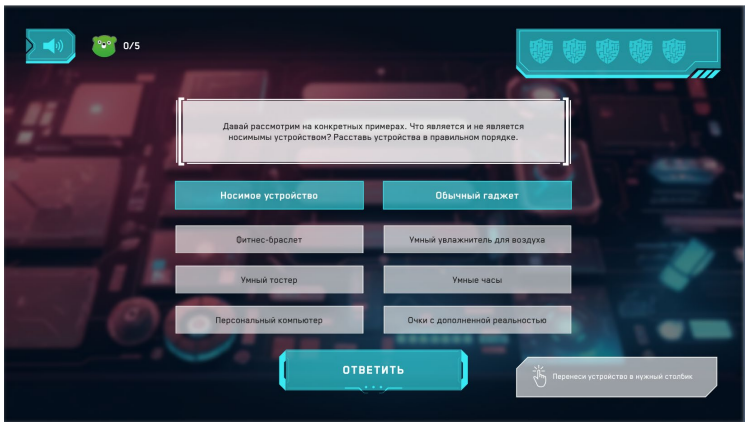
При использовании мониторов минимального разрешения необходимо применять функцию масштабирования браузера: Ctrl + «-», Ctrl + «стрелка вниз».

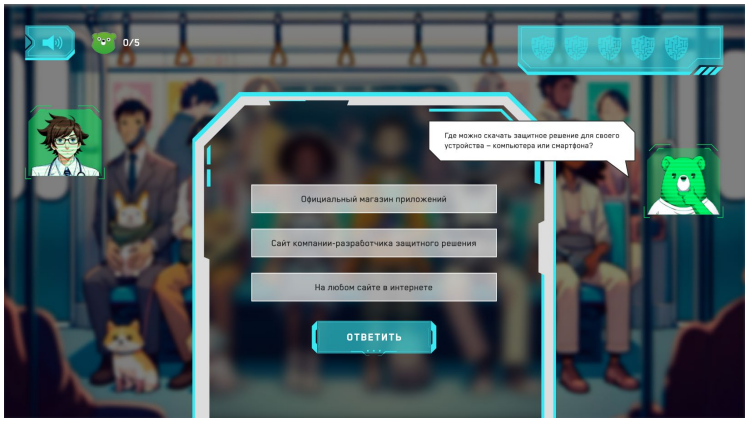
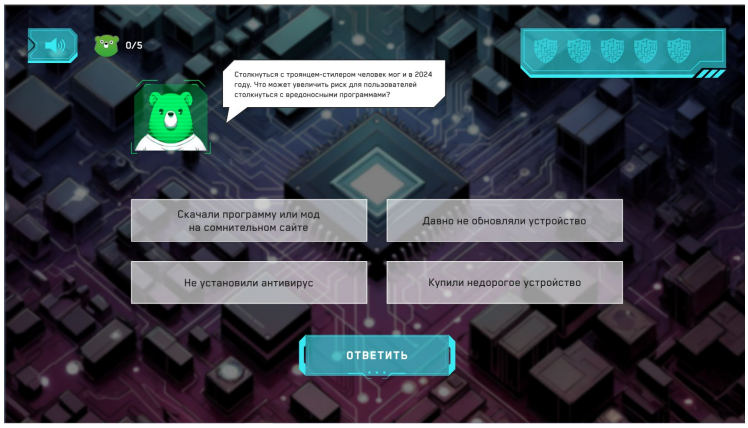
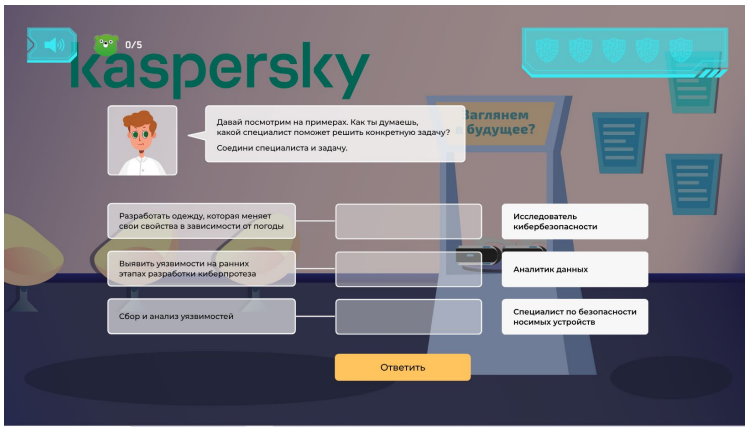
Вне зависимости от используемой конфигурации рекомендуется до урока открыть и пройти тренажер на компьютере ученика для проверки совместимости.

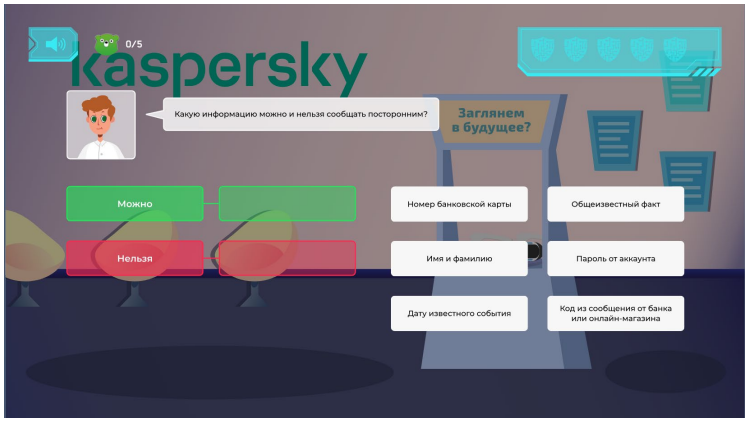
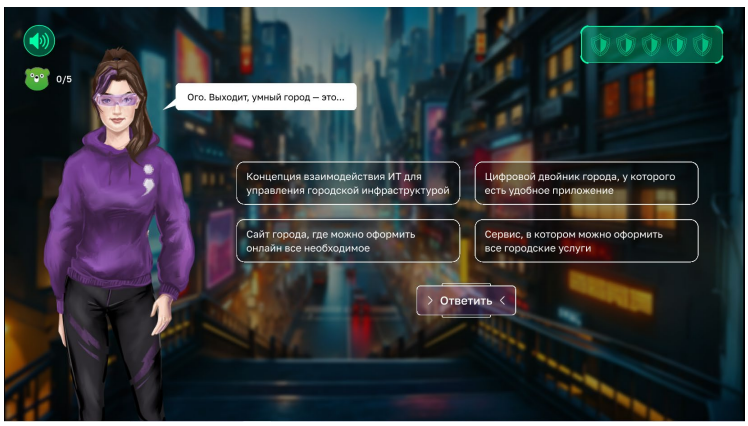
Приложение 2. Ответы на задания

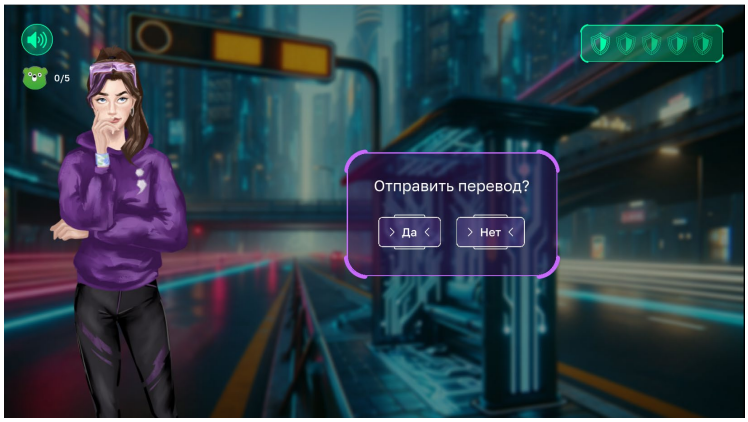
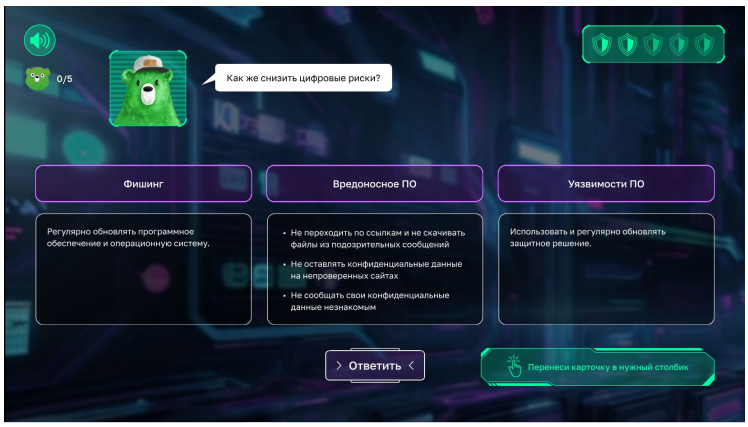
№	Скриншот задания	Верный ответ
Тренажер для начинающих испытателей (1-4 класс)		
1		Датчик — Темное время суток Контроллер — Приложение даст команду Управляемое устройство — Умная лампочка загорится теплым светом
2		Умный дом подвергают риску следующие действия пользователей: • Не поменяли пароль после покупки • Давно не обновляли ПО • Использовали устаревшее устройство
3		Надежным является пароль: 12_Asp@vmdoP’3w202

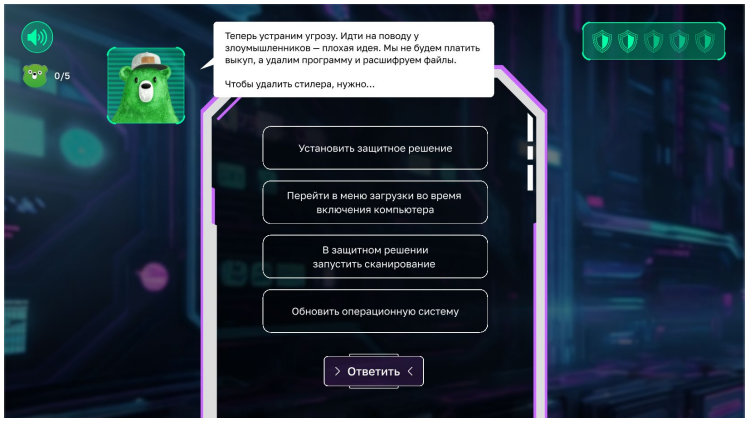
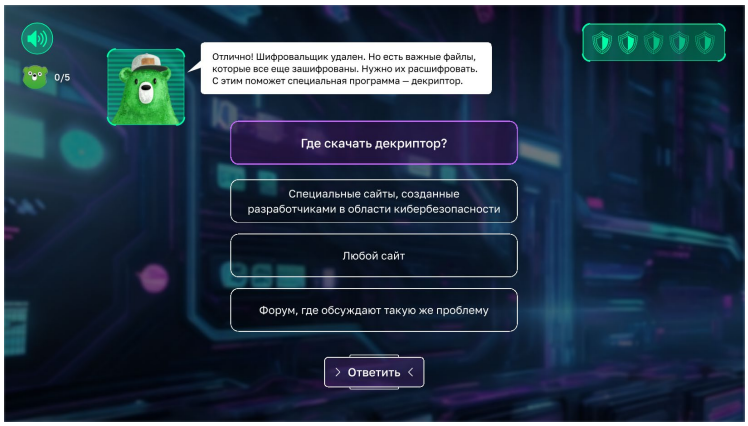
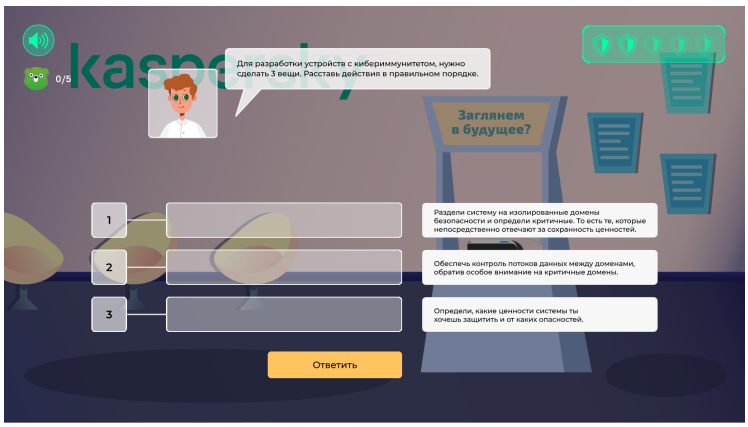
4		Подозрительным является приложение: Моды для игры Неофициальный портал с приложениями
5	 	Правильная последовательность действий: Выбрать приложение «Умный дом» → Нажать «Обновить»

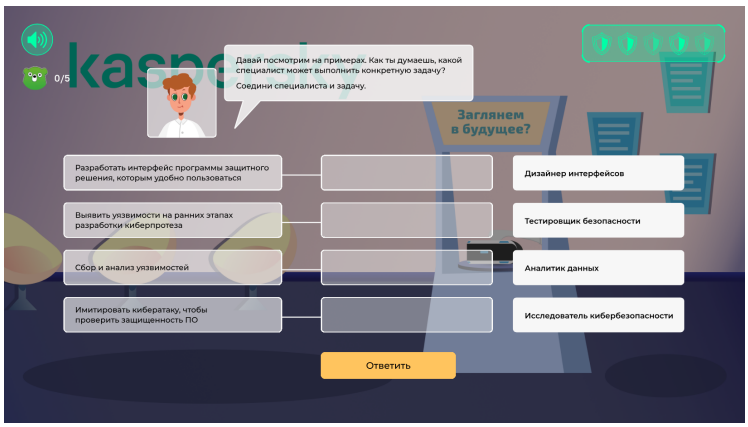
6		Проверить, насколько уязвима система или приложение — Пентестер Создать тостер, который будет автоматически делать тосты к 9 утра — Разработчик умных устройств Написать код, в котором не будет уязвимостей — Специалист по безопасной разработке Запустить проект по разработке умной системы игровой комнаты — ИТ-архитектор Следить, чтобы все сети и соединения исправно работали — Сетевой инженер
Тренажер для опытных специалистов (5-8 класс)		
1		Носимыми устройствами являются: • Фитнес-браслет • Умные часы • Очки с дополненной реальностью Обычными гаджетами являются: • Умный увлажнитель воздуха • Умный тостер

		• Персональный компьютер
2		Верные варианты: • Официальный магазин приложений • Сайт компании-разработчика защитного решения
3		Увеличить риск могут следующие действия: • Скачали программу или мод на сомнительном сайте • Давно не обновляли устройство • Не установили антивирус
4		Разработать одежду, которая меняет свои свойства в зависимости от погоды — Специалист по безопасности носимых устройств Выявить уязвимости на ранних этапах разработки киберпротеза — Исследователь кибербезопасности Собрать и проанализировать уязвимости — Аналитик

		данных
5		Можно сообщать: • Общеизвестный факт • Дату известного события Нельзя сообщать: • Номер банковской карты • Имя и фамилию • Пароль от аккаунта • Код из сообщения от банка или онлайн-магазина
Тренажер для закаленных специалистов (9-11 класс)		
1		Верный вариант: • Концепция взаимодействия ИТ для управления городской инфраструктурой

2		Верное действие: Нет (не отправлять перевод)
3		Снизить цифровые риски фишинга помогают следующие действия: • Не переходить по ссылкам и не скачивать файлы из подозрительных сообщений • Не оставлять конфиденциальные данные на непроверенных сайтах • Не сообщать свои конфиденциальные данные незнакомым Снизить цифровые риски заражения вредоносным ПО помогают следующие действия: • Использовать и регулярно обновлять защитное решение Снизить цифровые риски уязвимостей ПО помогают следующие действия: • Регулярно обновлять программное

		обеспечение и операционную систему
		Верные варианты: • Установить защитное решение • В защитном решении запустить сканирование
		Верный вариант: • Специальные сайты, созданные разработчиками в области кибербезопасности
4		Верная последовательность: 1. Определи, какие ценности системы ты хочешь защитить и от каких опасностей 2. Раздели систему на изолированные домены безопасности и определи критичные. То есть те, которые непосредственно отвечают за сохранность ценностей

		3. Обеспечь контроль потоков данных между доменами, обратив особое внимание на критичные домены
5		Разработать интерфейс программы защитного решения, которым удобно пользоваться — Дизайнер интерфейсов Выявить уязвимости на ранних этапах разработки киберпротеза — Исследователь кибербезопасности Собрать и проанализировать уязвимости — Аналитик данных Имитировать кибератаку, чтобы проверить защищенность ПО — Тестировщик безопасности