**Слайд 1**

Здравствуйте, меня зовут Мельников Илья. Я представляю проект «Чат-бот - игра по информационной безопасности» в Telegram.

**Слайд 2**

С каждым годом количество кибератак увеличивается. Последствиями являются утечка конфиденциальной информации, финансовые потери и упущенная выгода. При этом потребность в специалистах в сфере информационной безопасности постоянно растет. Именно поэтому велика роль профориентационной работы в образовательных организациях.

Однако на изучение темы «Информационная безопасность» в 10 классе отводится только 2 часа, что позволяет лишь обзорно познакомить с данным вопросом. Все это делает актуальной разработку ресурсов по информационной безопасности.

**Слайд 3**

Цель проекта – разработка игры по информационной безопасности, в рамках которой ученики познакомятся с видами угроз и атак на информационную безопасность, а также методами их раскрытия и профилактики. Задачи проекта представлены на слайде.

**Слайд 4**

Свидетельством успешной реализации проекта будут показатели, представленные на слайде. Главный показатель - это интерес учеников к игре и прохождение ее до конца.

**Слайд 5**

В настоящее время появляется множество ресурсов, посвященных вопросам защиты информации, в том числе и онлайн-игр. Мы проанализировали некоторые из них.

Игра по кибербезопасности SPOOFY направлена на решение типичных ситуаций защиты личной информации.

Игра И-риски направлена на знакомство с основными рисками в сфере информационной безопасности, а также формирование стратегии безопасного поведения у школьников разного возраста.

Обе эти игры ориентированы на обеспечение личной безопасности и не очень подходит для изучения вопросов защиты информации и профориентации.

Очень качественным продуктом являются игры от проекта **Урок цифры**. Они направлены на знакомство с понятием фишинга, видами киберугроз, навыками безопасного поведения в сети Интернет. Однако они не предполагают выполнения реальных практических заданий по вопросам защиты информации.

Другая группа игр представляет собой игры для профессионалов в сфере информационной безопасности. Например, игра от компании Касперский.

Получается, что игр для изучения вопросов защиты информации в свободном доступе не существует. Все это делает актуальной разработку собственного продукта.

**Слайд 6**

Наша игра предназначена для учащихся 8-11 классов. Она должна обладать простым и понятным интерфейсом, быть доступной в мессенджере, обеспечивать сохранение прогресса учеников.

**Слайд 7**

Существуют различные варианты реализации онлайн-игр. Т.к. главным аспектом для нас является удобство предложенного решения, то на основе опроса учащихся нами был выбран вариант игры -чат-бота, который не нужно будет дополнительно устанавливать и настраивать, а достаточно будет перейти по ссылке.

**Слайд 8**

На основе анализа различных инструментов разработки чат-ботов нами был выбран вариант самостоятельной разработки на языке программирования Python с использованием библиотеки Aiogram.

**Слайд 9**

Для реализации проекта используется следующие модули:

* база данных SQL Lite, модули на языке Python, а также дополнительные файлы, которые подгружаются по ходу работы чат-бота.

Общая структура проекта представлена на слайде.

**Слайд 10**

Данные о прогрессе участников сохраняются в базе данных. Структура и таблицы базы данных представлены на слайде.

**Слайд 11**

Легенда игры заключается в том, что участник является сотрудникам отдела информационной безопасности крупной компании. В этой компании произошла серия инцидентов, приведших к финансовым потерям, а также серьезной проблемой стала утечка конфиденциальной информации. Задача участника – провести расследование, определить нарушителей и предложить меры по защите информации.

В начале игры пользователь получает текстовое сообщение с описанием этой легенды, а затем подгружается видео.

**Слайд 12**

На первом этапе решается проблема утечки конфиденциальной информации. Игрок выбирает одного из трех персонажей. Каждый герой отправляет звуковое сообщение и файлы, которые вызвали подозрение у специалиста по информационной безопасности.

**Слайд 13**

На первом этапе пользователь получает файлы, которые выступают в роли стегоконтейнеров. Для получения информации из этого файла необходимо открыть файл hex-редактором. Зная принципы хранения формата bmp, можно выявить биты, в которых скрыта дополнительная информация.

**Слайд 14**

Второй этап игры посвящен методам социальной инженерии. На этом этапе идет работа уже с новыми героями.

Герои предоставляют объяснения по поводу случаев информационной атаки, которой они подверглись. Анализируя эти объяснения, нужно определить, какой метод социальной инженерии применялся.

**Слайд 15**

Третий этап посвящен выбору мер защиты информации. При выполнении заданий участник получает баллы за правильные ответы. В конце игры пользователю предоставляется общий результат игры. В дальнейшем планируется публикация рейтингов участников игры, а также реализация отдельного входа для учителя для просмотра данных о прохождении игры учениками.

**Слайд 16**

В ходе разработки игры проводилось тестирование. Для этого был разработан набор тестов.

Результат тестирования показал, что все представленные ситуации обрабатываются корректно, в соответствии с предъявленными требованиями. Использование результата проекта интуитивно понятно и не вызывает затруднений у пользователей.

**Слайд 17**

Разработанная нами игра предлагает ученикам выполнить задания по информационной безопасности. Это позволяет познакомиться с простейшими примерами ситуаций, с которыми может сталкиваться специалист по защите информации. Использование такой игры может повысить мотивацию школьников к изучению темы «информационная безопасность». Кроме того, наличие практических заданий и теоретической информации позволяет решить важную задачу в сфере информационной безопасности – профориентация учеников, и привлечение их к профессиям в сфере информационной безопасности.

**Слайд 18**

Спасибо за внимание