ДЕНЬ IT-ЗНАНИЙ 2025/26

Добрый день! В этом файле мы собрали материалы для проведения занятий. Сценарии занятий и презентации можно использовать для проведения классного часа или внеклассной работы.

Тема урока: Информационная безопасность.

Цель урока: Способствовать осознанному выбору профессии в IT среди школьников.

Задачи урока:

1. Сформировать системное понимание многообразия профессий внутри IT-индустрии.
2. Познакомить с разнообразием направлений в сфере информационных технологий.
3. Познакомить с карьерными и образовательными возможностями VK

Модели и форматы работы на занятии: фронтальная работа с учениками.

Общее время занятия: 40-45 мин (1 ак.час)

Оборудование для проведения урока: проектор и/или интерактивная доска для демонстрации презентации. Колонки для воспроизведения звука.

Рекомендуемая дата занятия: любой учебный день.

Возраст учеников: материалы акции рассчитаны на учеников 7-11 классов.

Базовый план выступления рассчитан на 40-45 минут (1 академический час) и состоит из четырёх этапов.

Этап	Содердание	Время	Оборудование
Этап актуализации знаний. Мотивация учебной деятельности обучающихся	Анимационный видеоролик	7 минут	Проектор и/или интерактивная доска для демонстрации презентации.
Организационный этап. Постановка цели и задач.		3 минут	
Этап освоения новых знаний, проверка понимания и закрепление	О направлении	5 минут	
	Профессии внутри направления IT	10 минут	
	Примеры на продуктах VK	5 минут	
	Практическая часть	10 минут	
Этап подведения итогов занятия. Устная или письменная рефлексия		5 минут	

СЦЕНАРИЙ УРОКА

Номер слайда	Речь для спикера	Дополнительные рекомендации к речи и примечания
Организационный этап. Постановка цели и задач.		
Слайд 1	Здравствуйте, ребята! Меня зовут [ваше имя]. Компания VK проводит профориентационную акцию «День IT-знаний».	
Слайд 2	Если в уроке не участвует сотрудник VK, этот слайд пропустите. Если урок ведет эксперт VK, то это место, где он немного расскажет о себе.	
Слайд 3	Для начала – небольшой квиз, чтобы проверить, что вы уже знаете! **Озвучить вопрос аудитории.** "Что первое приходит вам в голову, когда вы слышите 'информационная безопасность'? **2-3 ответа от аудитории.**	

Номер слайда	Речь для спикера	Дополнительные рекомендации к речи и примечания
Актуализация знаний		
Слайд 4	Озвучить вопрос аудитории. Как называется самый безопасный способ входа VK ID? Дальше идет голосование. Кто считает, что первый вариант верный? (поднимают руки). Кто считает, что второй вариант? (поднимают руки) и тд.	
Слайд 5	Правильным является вариант 2. Вход по скану лица или отпечатку пальца является наиболее безопасным вариантом, так как "под капотом" этой функции - сложные технологии, которые не позволяют авторизоваться на поддельном, то есть фишинговом сайте, а также предоставляет эту возможность только с доверенного устройства, которое привязано в аккаунту. Кроме того скопировать биометрические данные практически невозможно и хранятся они исключительно на устройстве пользователя. Пояснения: 1. "Алохомора" — это заклинание от Гарри Поттера для открывания замков. Так же и в цифровом мире: мы хотим, чтобы вход был безопасным, но максимально простым и быстрым. 2. Двухфакторная аутентификация — это как дверь с двумя замками (пароль + код из смс) Беспарольная (безбарьерная) аутентификация — такого способа аутентификации в принципе не существует.	
Слайд 6	Озвучить вопрос аудитории. Какой пароль является наиболее надежным? Дальше идет голосование. Кто считает, что первый вариант верный? (поднимают руки). Кто считает, что второй вариант? (поднимают руки) и тд.	
Слайд 7	Правильный ответ 3. **Пояснение:** Этот пароль является сильным потому, что он сочетает в себе несколько ключевых принципов создания надежных паролей, которые сильно усложняют жизнь злоумышленникам. Можно уточнить у аудитории, что это за принципы. Обсудить вместе с ними: 1. Он состоит из 12 символов. Чем длиннее пароль, тем больше комбинаций нужно перебрать программе-взломщику. Взлом 8-символьного пароля может занять часы, а 12-символьного — уже сотни лет. 2. Он сложный. В нем присутствуют четыре типа символов: прописные буквы, строчные буквы, цифры и специальные символы. 3. Он неочевидный: пароль не содержит личной информации или простых последовательностей, а также не является словом из какого-либо языка. Однако такой пароль сложно запомнить (или найти способ безопасно хранить). Поэтому для удобства и безопасности лучше использовать менеджеры паролей.	

Номер слайда	Речь для спикера	Дополнительные рекомендации к речи и примечания
Слайд 8	**Озвучить вопрос аудитории.** Стоит ли переходить по ссылке? Участвуем ли в голосовании? **Дальше идет голосование.** Поднимите руки, кто считает, что стоит проголосовать? А кто считает, что нет?	
Слайд 9	Схемы с конкурсами являются сегодня одним из самых популярных мошеннических ходов в социальных сетях и мессенджерах. Лучше не переходить по ссылкам с просьбой проголосовать, даже если ссылку отправил друг. С 99,9 % вероятностью, это мошенничество. После перехода по ссылке для голосования появляется страница аутентификации, на которой нужно ввести номер телефона, чтобы получить код — совершения входа в аккаунт уникальности. После ввода доступ к аккаунту попадает к мошенникам, так как ресурс является поддельным, то есть фишиновым. Поэтому будьте бдительны и не переходите по ссылкам, без тщательной проверки их достоверности. Не рискуйте своими аккаунтами, данными и другой личной информацией.	
Слайд 10	**Вопрос:** Справа перечислены разные типы фишинговых атак. Одно название из списка – выдуманное. Какое? **Дальше идет голосование.** Кто считает, что первый вариант верный? (поднимают руки). Кто считает, что второй вариант? (поднимают руки) и тд.	
Слайд 11	**Правильный ответ – 3.** Емейлинг — выдуманное слово. Правильный термин для email-фишинга — просто фишинг или электронный фишинг. **Пояснение:** Фишинг — это когда злоумышленники притворяются кем-то знакомым или надежным (другом, банком, соцсетью), чтобы выдать ваши данные. Вишинг (Vishing) — голосовой фишинг (звонок). Смишинг (Smishing) — фишинг через SMS. Уэйлинг (Whaling) — фишинг на "крупную рыбу" (директоров, важных персон). Например, вам пишет руководитель вашего руководителя. Особенно внимательными нужно относиться к звонкам и сообщениям. Искусственный интеллект может подделывать голоса и даже замещать лица людей на видео.	
Слайд 12	**Вопрос:** Когда говорят, что «ресурс недоступен», иногда это значит, что на него была совершена атака. О каком типе атак идет речь? **Дальше идет голосование.** Кто считает, что первый вариант верный? (поднимают руки). Кто считает, что второй вариант? (поднимают руки) и тд.	

Номер слайда	Речь для спикера	Дополнительные рекомендации к речи и примечания
Слайд 13	Правильный ответ – 2. **Аудитории можно задать наводящий вопрос.** Поднимали ли руки те, кто не мог зайти на какой-либо сайтв игру или ВК из-за того, что 'сервера лежат'? Это и есть результат DDoS-атаки. Это попытка злоумышленников вывести из строя сайт или онлайн-сервис, массово отправляя на него запросы с множества устройств. Цель — перегрузить систему, чтобы она перестала отвечать на обращения пользователей. Злоумышленники создают огромный поток ложных запросов к серверу, он не справляется и "падает". Brute Force — это подбор паролей, Вредоносное ПО — вирусы, а Фишинг — обман.	
Изучение нового материала		
Слайд 14	Информационная безопасность (ИБ) в IT — это: Создание защиты «по умолчанию». Встроенная безопасность на этапе разработки продукта, чтобы им можно было пользоваться без рисков. ИБ с самого начала работаем вместе с разработчиками, чтобы новые приложения в VK и сервисах сразу были надежными. Обеспечение работы сервисов. Защита от атак, которые могут остановить работу социальных сетей, игр или образовательных платформ. Да, атаки действительно случаются. Задача ИБ — быть тем самым Щитом. Они постоянно мониторят угрозы, отражают атаки и учатся на них, чтобы завтра защита была еще круче. Безопасно обращаться, передавать и хранить данные. Это про доверие. Ваши фото, переписки, платежи — это личные данные. Главная задача IT-компаний — сделать так, чтобы они оставались вашими. Чтобы они никуда не утекли и чтобы к ним не получили доступ те, кому не следует. Это ответственность перед пользователями. Гарантия того, что личные переписки, фото и платежные данные не попадут в руки мошенников. Современная ИБ — это не про запреты и капюшоны. Это про технологии, интеллект и ответственность.	
Первичное усвоение и закрепление		
Слайд 15	Теперь, когда мы разобрались, что из себя представляет современная информационная безопасность, давайте посмотрим, люди каких профессий делают это направление таким, какое оно есть! Но кто эти люди, которые всё это делают? Давайте представим, что мы создаём новый крутой мессенджер. Кто позаботится о том, чтобы его нельзя было взломать, пока он ещё даже не запущен?	Первые хакеры — это энтузиасты, которые изучали, как работают системы (компьютеры, сети, программы). Их мотив — не навредить, а понять, улучшить, найти неочевидные возможности.

Номер слайда	Речь для спикера	Дополнительные рекомендации к речи и примечания
Слайд 15	На самом деле, информационная безопасность начинается с этапа разработки, главный принцип: «Лучше заранее предотвратить проблему, чем потом героически её чинить». Application Security (безопасность приложений) инженеры — специалист по комплексной безопасности школы. Работники из этого отдела не ищут обычные баги, а специально выискивают дыры в коде до того, как приложение “вышло в прод”, то есть попало в пользование обычных людей. Они знают наиболее популярные уязвимости, а также ищут новые, ранее неизвестные для исправления на этапе разработке 1. **Аналитики и архитекторы безопасности** Подключаются к разработке продукта на этапе планирования. Они оценивают риски и помогают спроектировать систему сразу правильно, чтобы не переделывать потом. 2. **Программисты с навыками безопасной разработки** Это те самые разработчики, которые пишут код для ВКонтакте, игр, любых приложений. Но они отличаются одной суперсилой: они с самого начала пишут код так, чтобы в нём было сложно оставить уязвимость. Их не нужно заставлять думать о безопасности — они делают это по привычке. Такие программисты — на вес золота на всём IT-рынке, а не только в отделах безопасности!	Со временем сообщество разделилось на тех, кто использует навыки во вред (Black Hat), и тех, кто использует их для защиты (White Hat). **Black Hat —** нарушают закон, крадут данные, зарабатывают на атаках. **White Hat —** работают легально, находят уязвимости, чтобы их устранить. Их называют «этичными хакерами».
Слайд 16	Мы посмотрели на тех, кто встраивает безопасность прямо в код. Но что происходит, когда продукт уже запущен и работает? Как защитить его от реальных атак? Здесь мы поговорим о тех, кто активно защищает безопасность данных компании и пользователей. 1. **Архитекторы и инженеры ИБ (SecOps-инженеры)** Сначала нужно построить крепкие стены и надежные механизмы защиты. Этим занимаются архитекторы и инженеры. Они не пишут код для функций ВК, они создают и настраивают системы безопасности: сетевую защиту, системы шифрования, сложные правила доступ а и многое другое. Они — главные строители обороны всей компании, а также следят за верной эксплуатацией всех внедренных решений. 2. **Центр обеспечения безопасности (SOC)** Стены построены. Теперь нужны круглосуточные часовые. В компании есть специальный центр Security Operations Center (центр мониторинга и реагирования на ициденты) — это наша комната с мониторами наблюдения. Аналитики центра постоянно следят за всеми что происходит в сетях компании. Их задача — заметить подозрительную активность: например, что кто-то пытается подобрать отмычки к воротам (подбирает пароли) или прорыть подкоп (провести хакерскую атаку). Они первыми обнаруживают угрозу, бьют тревогу и максимально быстро предотвращают атаку. Зачастую свою карьеру ИБ-специалисты начинают именно аналитиком SOC.	

Номер слайда	Речь для спикера	Дополнительные рекомендации к речи и примечания
Слайд 16	3. **Цифровые криминалисты** Если атака всё же произошла, наступает время цифровых детективов или криминалистов. Они проводят расследование: смотрят, как злоумышленник проник внутрь, что он успел сделать, какие "улики" (логи, записи) после себя оставил. Их работа помогает не только устранить последствия взлома, но и укрепить защиту на будущее, чтобы не допустить повторения. Они ищут слабые места, которые пропустили все остальные. Такие специалисты также занимаются разведкой угроз: они ищут в разных источниках потенциальные новые вектора атак, которыми могут воспользоваться мошенники и выстраивают заблаговременную защиту. Все они — не менее крутые хакеры. Просто они взламывают не системы, а задачи по защите наших данных.	
Слайд 17	Мы уже познакомились с теми, кто строит защиту, и теми, кто её охраняет. Но как проверить, насколько эта защита вообще крепкая? Для этого есть “белые хакеры,” которые работают на сторону добра. Они атакуют, но делают это исключительно для того, чтобы сделать защиту крепче. 1. **Пентестеры (тестировщики на проникновение)** Их задача — найти конкретные уязвимости в системе: проверить, надежна ли стена, нет ли хотя бы одной уязвимой строчки кода. Они действуют по заранее согласованному сценарию и ищут известные уязвимости. Можно сказать, они проводят контрольную закупку безопасности: всё легально, но очень дотошно. 2. **Операторы Red Team (“Красной команды”)** А это — «тайные агенты». Они действуют как настоящие шпионы! Их задача — провести полномасштабную операцию по взлому. Здесь уже нет никаких согласованных сценариев, только цель — показать, где система дала сбой. Они не просто ищут дыры в стенах — они могут подделать документы, чтобы обмануть стражу (социальная инженерия), отправить поддельное письмо от имени высокопоставленных руководителей (фишинг) или незаметно проникнуть в замок под видом торговца. Они ведут себя в точности как настоящие хакеры. После успешной атаки они всё раскрывают: учат охрану не верить поддельным письмам, а архитекторам — закрывать найденные лазейки. 3. **Багхантеры (охотники за ошибками)** А это — «независимые искатели приключений». Они не работают напрямую на компанию, но ищут уязвимости в разных сайтах, приложениях из чистого любопытства или азарта. Если они находят брешь, они не используют её во зло, а вежливо пишут владельцу: «Эй, у тебя тут дыра в стене, советую заделать». За это компании благодарят их и платят вознаграждение! Многие багхантеры работают в компаниях, а багхантингом занимаются в качестве собственного профессионального развития и дополнительного - иногда очень существенного - заработка. Например, сейчас если багхантеры найдут уязвимость в мессенджере MAX, они могут получить до 5 млн руб. Багхантинг также является хорошим стартом для работы в ИБ. Все эти роли объединяет одно: они взламывают системы, чтобы сделать их лучше. Они не нарушают закон — они работают в рамках правил, чтобы помочь компаниям стать неуязвимыми для реальных угроз.	Пентестеры, багхантеры и другие — это и есть современные White Hat-хакеры. Они находят уязвимости, чтобы их исправить, а не использовать.

Номер слайда	Речь для спикера	Дополнительные рекомендации к речи и примечания
Слайд 18	Теперь давайте представим, что мы придумали суперсовременную систему защиты. В ней разбираются десять гениальных инженеров. Но есть проблема: никто другой в компании не понимает, как ей пользоваться, зачем она нужна, и все её боятся. **Вопрос аудитории:** Как вы думаете, что произойдет? **Правильный ответ:** вероятнее всего, систему будут игнорировать. 1. **Специалисты по киберкультуре** Это — «имиджмейкеры» цифровой безопасности. Их задача — сделать так, чтобы тема информационной безопасности внутри компании стала... модной! Они придумывают внутренние конкурсы, создают стильные памятки, проводят обучение в формате игр). Они делают из скучных инструкций — увлекательный контент. Это как пиарщики, но пиарят они — безопасность. 2. **Специалисты по осведомленности** Они знают, что самый слабый элемент в любой системе — это человек. Их задача — научить всех сотрудников компании основам цифровой гигиены: не переходить по подозрительным ссылкам в письмах, создавать сложные пароли, не подключаться к публичному Wi-Fi без VPN. Они не читают скучные лекции, а придумывают, как донести важные правила просто и запоминающиеся. Именно они спасают нас от фишинга! 3. **Маркетологи информационной безопасности** И, наконец, люди, которые рассказывают о безопасности вне компании — пользователям. Например, когда в VK появляется новая фиша — вход по отпечатку пальца или двухфакторная аутентификация, — именно маркетологи ИБ придумывают, как красиво и понятно объяснить людям, что это и зачем нужно. Без этих людей вся защита, которую строят инженеры, просто не сработает. Потому что иногда сложнее, чем создать защиту, только объяснить людям, зачем и как ей пользоваться.	
Слайд 19	Давайте посмотрим, как специалисты разных профессий внутри направления взаимодействую между собой? Перед вами — карта профессий в информационной безопасности. Условно все роли можно разделить на четыре больших направления: Создатели — те, кто встраивает безопасность в продукты на этапе разработки. Защитники — те, кто охраняет системы круглосуточно. Нападающие на стороне добра — те, кто ищет уязвимости, чтобы их устранить. Коммуникаторы — те, кто объясняет, учит и делает ИБ понятной для всех. Обратите внимание: это не строгое разделение. Специалисты часто работают на стыке направлений. Например, пентестер (нападающий) тесно сотрудничает с разработчиком (создателем), чтобы устранить уязвимость. И помните: любая из этих ролей — это вклад в безопасность цифрового мира.	В ИБ есть место не только для тех, кто разбирается в коде. Если вы гуманитарий — вам может быть интересно направление киберкультуры. Если любите расследовать — обратите внимание на цифровую криминалистику. Если вам нравится стратегия и анализ — вам может подойти роль в Red Team.

Номер слайда	Речь для спикера	Дополнительные рекомендации к речи и примечания
Слайд 20	Хотите увидеть, как эти навыки работают в реальном продукте? Тогда давайте посмотрим на примере одной из функций ВКонтакте. Вы наверняка знаете, что в VK можно войти не только по логину и паролю, но и с помощью биометрии — по лицу или отпечатку пальца. VK ID служит единой точкой входа для множества сервисов, что позволяет пользователям безопасно переключаться между различными продуктами VK. Когда вы настраиваете вход по лицу, ваше устройство (телефон или компьютер) создает цифровой шаблон — уникальную математическую модель вашего лица. Этот шаблон хранится только на вашем устройстве в зашифрованном виде. VK не получает и не хранит ваши биометрические данные. Почему это безопасно? Нет пароля — нечего украсть. Злоумышленник не сможет подобрать или украсть ваш пароль, потому что его просто нет. Данные только у вас. Ваше лицо — это ваш ключ, и он остаётся только с вами. Подделать почти невозможно. Современные алгоритмы распознавания умеют отличать фотографию или маску от реального человека. Так, например, когда вы используете вход по лицу в VK — это результат работы всех этих систем. Security Gate (платформа для безопасной разработки ПО) проверил код этой функции, SOC (оперативный центр обеспечения безопасности) защищает серверы, где хранятся данные, а наши специалисты создали инструкции для пользователей. Обратите внимание, как комплексно подходит VK к обеспечению информационной безопасности. Продукты защищиены на всех уровнях — от серверов до каждого сотрудника и пользователя. Ключевой вывод. Важно понимать, что безопасность — это не одна технология, а комплекс мер, которые работают вместе.	Продуктом в IT называют решение, разработанное с помощью программного кода, которое решает конкретные задачи. Например, это может быть мобильное приложение, облачная платформа для хранения фотографий или документов, программное обеспечение и многое другое. **Чем продукт в IT отличается от проекта?** Проект имеет четкое начало и конец. Продукт же живет и развивается годами (пока он востребован). Работа над продуктов циклична и никогда не прекращается: сбор обратной связи, анализ данных, планирование улучшений, выпуск новых версий. **В качестве примера можно привести:** Проект: “Ребята, давайте за 3 месяца сделаем возможность ставить разные реакции на посты”. Разработали, запустили — проект завершен. Продукт: А вот сам ВКонтакте — это продукт. Он был создан много лет назад, но до сих пор его постоянно улучшают: добавляют новые функции (те же реакции), исправляют ошибки, меняют дизайн. Задача команды продукта — чтобы соцсеть оставалась современной, удобной и чтобы ею продолжали пользоваться миллионы людей
Творческое применение знаний		
Слайд 21	Давайте попрактикуемся и представим себя на месте специалистов ИБ. В компании ежедневно появляется сотни и тысячи строк кода. Не всегда разработчики задумываются (и даже знают) о принципах безопасной разработки и готовы уделять безопасности достаточное внимание. Так как основная их задача – быстрей выводить IT-продукты на рынок. Если специалисты Информационной безопасности будут вручную проверять каждый новый проект — их выход в таком случае замедлятся в разы. Бизнес будет не доволен и разработчики либо будут игнорировать требование ИБ, либо искать пути обхода ограничений. Тогда ИБ предлагает особый инструмент, который автоматически проверяет код, находит уязвимости и даже предлагает решения.	

Номер слайда	Речь для спикера	Дополнительные рекомендации к речи и примечания
Слайд 21	**Но появилась новая проблема:** люди не любят новшества в работе и не спешат ими пользоваться. Для этого необходима грамотная кампания по популяризации безопасной разработки, ее важности, а также продвижение нового решения. **Задание для аудитории:** опишите программу мероприятий, которая поможет в компании выстроить правильный процесс выпуска продуктов на рынок.	
Слайд 22	**Идеальное решение —** это не просто «внедрили инструмент и заставили пользоваться». Это комплексная программа, которая меняет культуру разработки. 1. **Исследуем:** Сначала мы узнаём, почему разработчики не хотят пользоваться инструментом. Проводим опросы, интервью, смотрим метрики. Может, они не понимают, как им пользоваться VK Security Gateuserться? Или он действительно неудобный? 2. **Обучаем:** Создаём курсы, инструкции, видео — чтобы каждый разработчик знал, как писать безопасный код и зачем это нужно. 3. **Поддерживаем:** Открываем чат поддержки, пишем ответы на возможные вопросы, чтобы в любой момент можно было задать вопрос и быстро получить помощь. 4. **Мотивируем:** Здесь — самое интересное! Мы внедряем систему геймификации: Даём бейджи и статусы за использование новой программы. Присваиваем звание Чемпионов (значками во внутренней системы) тем, кто активно помогает коллегам и следит за безопасностью. Дарим стикерпаки и мерч — это всегда работает! 5. **Интегрируем:** Проводим совернования и конкурсы — чтобы разработчики могли применить знания на практике и почувствовать себя «белыми хакерами». Участвуем во внутренних мероприятиях: записываем подкасты, ведём блоги, размещаем посты на цифровых экранах в офисе. 6. **Рассказываем миру:** Поддерживаем имидж VK как компании, которая заботится о безопасности. Именно так они начинают видеть в безопасности не врага, а помощника — и сами становятся её представителями и защитниками.	
Слайд 23	Пароли должны были исчезнуть ещё 20 лет назад, но они до сих пор с нами. Почему? **В чём проблема?** • Пользователи создают простые пароли: 123456, qwerty, password. • Используют один и тот же пароль на всех сайтах. • Хранят их в заметках, браузерах или просто в голове — это ненадежно. • Не включают двухфакторную аутентификацию (2FA), даже когда это возможно. **К чему это приводит?** • Утечки данных: если взломают один сервис, злоумышленники получат доступ ко всем вашим аккаунтам. • Взломы личных и рабочих аккаунтов. • Финансовые потери и репутационные риски для компаний. **Задача для аудитории:** Что может сделать такая компания, как VK, чтобы защитить своих пользователей и сотрудников?	Второй кейс можно использовать, если остается много времени до конца урока. При условии, что времени остается мало – его можно пропустить.

Номер слайда	Речь для спикера	Дополнительные рекомендации к речи и примечания
Слайд 24	Самое простое, но очевидное решение: отказаться от паролей! Нет пароля – нет проблем. Пользователи могут выбирать способы входа по коду из смс, пуш-уведомления, звонку сбросу. Входить в свой аккаунт по скану лица или отпечатку пальцев, с использованием специальных ключей или благодаря технологии криптографических ключей, которые встроены в само устройство. Эти способы повышают защищенность аккаунтов и делают процесс входа более удобным и быстрым.	
Завершение и рефлексия		
Слайд 25	**Итак, мы с вами прошли большой путь:** разобрались, что отличает современную сферу информационной безопасности, узнали о ключевых профессиях в этой сфере и даже выяснили, какие навыки нужны, чтобы в ней преуспеть. **Давайте подведем главные итоги:** **Информационная безопасность —** это не скучно и не страшно! Это огромный мир, где есть место каждому: и тем, кто любит технологии, и тем, кто предпочитает общаться с людьми, учить, объяснять или творчески подходить к задачам. **Не обязательно быть гением с рождения.** Начать можно в любой момент, даже если вы пока не разбираетесь в программировании. Главное — интерес и желание учиться. Не пытайтесь объять необъятное: начните с малого — пройдите курс, почитайте статьи, попробуйте себя в CTF-соревнованиях. **Ваша карьера начинается уже сейчас.** Не ждите диплома или «того самого момента». Уже сегодня вы можете подписаться на образовательные каналы, следить за новостями в сфере ИБ и пробовать свои силы. Помните: даже самые крутые специалисты начинали с нуля. Помните, что в сфере IT у вас есть шанс сделать мир вокруг лучше и стать частью большой команды. А сфера ИБ не смотря на свою популярность, на самом деле, является довольно узким профессиональным сообществом: вам достаточно проявить себя, чтобы вас запомнили, стали рекомендовать, а крупные компании стали готовы даже бороться за вашу экспертизу.	
Слайд 26-29	Вы можете попробовать себя в роли специалистов IT-сферы уже сегодня прямо внутри мессенджера Вконтакте. Переходите по QR-коду в мини-приложение и стартуйте в IT уже сегодня. Вы можете также ознакомиться с нашими открытыми курсами на платформе VK Education. А также подписывайтесь на наше сообщество во Вконтакте, а также переходите на портал VK Education!	
Слайд 30	Заключительное слово спикера: напутственное слово, благодарность за внимание. По QR-коду школьники могут перейти в бот, который откроет доступ к стикерам в мессенджере MAX.	