Технологическая карта урока в рамках нового сезона проекта «Цифровой ликбез»

Цели урока: сформировать базовые правила безопасной работы с личными аккаунтами в сервисах Интернета, раскрыть сущность понятия «дипфейк», сформировать представление о ценности персональных данных, размещаемых в Интернете.

Задачи урока:

— познакомить учащихся с понятием «Безопасность аккаунта» и его особенностями;
— научить распознавать потенциально опасные схемы, которые могут использовать злоумышленники, чтобы украсть аккаунт или получить доступ к персональным данным;
— познакомить учащихся с понятиями «Дипфейк» и «Доксинг», а также их особенностями;
— повысить уровень осведомленности о мошеннических схемах с использованием дипфейк технологий и определить спектр возможностей применения технологии дипфейк;
— научить предотвращать публичное распространение личной информации.

Ход урока

Слайд	Комментарий педагога	Примечание
Слайд №1	Приветствую всех на уроке в рамках нового сезона проекта «Цифровой ликбез». Мы изучим основы цифровой грамотности и правила кибербезопасности в современном мире. В этом нам поможет начинающая журналистка Лина, которая проходит стажировку в компании «Карасевский».	Все видеоролики доступны на сайте проекта: **https://digital-likbez.datalesson.ru**
Слайд №2	Сегодня мы подробно поговорим о краже аккаунтов и понятиях «Дипфейк» и «Доксинг».	

Слайд №3	Начнем с темы «Кража аккаунтов». Поднимите, пожалуйста, руки те из вас, у кого есть аккаунты в мессенджерах, играх или социальных сетях? А кто из вас сталкивался с кражей или попыткой кражи аккаунта?	
Слайд №4	Давайте посмотрим видеоролик и разберемся, как же злоумышленники могут украсть ваш аккаунт.	Ссылка на видеоролик:
	Все ли было понятно в видеоролике? Сталкивались ли вы с похожими ситуациями в своей жизни?	
Слайд №5	Давайте рассмотрим несколько ситуаций, которые могут повлечь за собой кражу вашего аккаунта и личных данных.	
Слайд №6	На слайде пример: Ваш друг просит перейти по ссылке и проголосовать за него в конкурсе, который для него очень важен. Как определить, что это сообщение от злоумышленника?	
Слайд №7	Во-первых, обратите внимание на ссылку. Если ссылка содержит опечатки или выглядит подозрительно, это фишинговая ссылка, не переходите по ней.	

	Страница сайта с голосованием никогда не будет запрашивать номер телефона, банковской карты и других личных данных. Свяжитесь с другом, от которого получили сообщение, по телефону и уточните, действительно ли он участвует в конкурсе.	
Слайд №8	На слайде пример: Вы получили сообщение с предложением выиграть новый телефон, перейдя по ссылке.	
Слайд №9	Это снова уловка злоумышленников. Настороженно относитесь к очень щедрым предложениям в Интернете. Например, к возможности что-то выиграть или заработать, лишь перейдя по ссылке.	
Слайд №10	Давайте закрепим полученные знания и ответим на несколько вопросов.	
Слайд №11	Вопрос 1. Каким должен быть пароль для разных аккаунтов? Выберите наиболее полный ответ. А) он должен состоять из более чем 12 символов, цифр и специальных символов Б) он должен быть уникальным и состоять из более чем 12 символов, цифр и специальных символов В) это должен быть номер телефона, так как его легко запомнить	

	Г) паролем должен быть домашний адрес, так как его легко запомнить	
Слайд №12	Правильный ответ на этот вопрос – Б (он должен быть уникальным и состоять из более чем 12 символов, цифр и специальных символов)	
Слайд №13	Вопрос 2. Вы получили сообщение, в котором есть ссылка на незнакомый вас ресурс. Ваши действия (Выберите несколько вариантов): А) открою ссылку, но не буду вводить никаких данных Б) не стану ничего делать, даже если явно попросят перейти по ссылке В) разошлю друзьям/родным, пусть сначала они попробуют Г) удалю пользователя из книги контактов	
Слайд №14	Правильный ответ на этот вопрос – А и Б (открою ссылку, но не буду вводить никаких данных; не стану ничего делать, даже если явно попросят перейти по ссылке)	
Слайд №15	Вопрос 3. Вы получили сообщение о том, что выиграли в лотерею денежный приз, но нигде не принимали участие. Вас просят оплатить небольшую комиссию за обработку вашего платежа и после этого обещают перевести денежные средства	

	на ваш счет. Ваши действия (Выберите один ответ): А) все сделаю, как они просят Б) разошлю друзьям, пусть они тоже поучаствуют В) никак не стану реагировать и отвечать, так как очень похоже на мошенничество Г) почитаю в Интернете, если не найду ничего плохого, то все переведу им деньги	
Слайд №16	Правильный ответ на этот вопрос – В (никак не стану реагировать и отвечать, так как очень похоже на мошенничество)	
Слайд №17	Вопрос 4. От каких сервисов злоумышленники могут украсть данные для авторизации (Выберите несколько вариантов)? А) от мессенджеров Б) от социальных сетей В) от игровых сервисов Г) от онлайн библиотеки	
Слайд №18	Правильный ответ на этот вопрос – А, Б, В, Г	
Слайд №19	Вопрос 5. Где безопаснее скачивать новые приложения на телефон/планшет (Выберите несколько вариантов)?	

	А) на сайте разработчика Б) на специализированных форумах В) на сайтах производителей Г) спрашиваю друзей, они мне присылают ссылку	
Слайд №20	Правильный ответ на этот вопрос – А и В	
Слайд №21	Отлично! Итак, как же защитить аккаунты от кражи?	
Слайд №22	• Не верьте сообщениям, в которых вас просят сделать что-то очень быстро (например, перейти по ссылке), даже если его прислал ваш друг; • Свяжитесь с другом любым другим удобным способом и уточните, не взломали ли его; • Не верьте очень щедрым предложениям в Интернете. Например, что-то выиграть или заработать большую сумму, перейдя по ссылке; • Не скачивайте программы и игры из непроверенных источников, даже если вам предлагают самую новую версию – только из официальных магазинов; • Настройте дополнительное подтверждение входа по коду, то есть двухфакторную аутентификацию; • Установите антивирусную защиту, чтобы не перейти по фишинговой ссылке.	

Слайд №23	А теперь давайте поговорим о том, как злоумышленники используют новые технологии для обмана пользователей в Интернете.	
	Как вы думаете, можно ли с помощью технологий подделать голос человека или даже создать видео с его точной копией?	
Слайд №24	Дипфейк – это технология, которая позволяет с использованием машинного обучения создавать подделки изображений, видео- или аудиоданных.	
Слайд №25	Давайте посмотрим видеоролик и узнаем, как же злоумышленники могут создать поддельные видео и использовать их в мошеннических целях.	Ссылка на видеоролик:
	Все ли было понятно в видеоролике? Сталкивались ли вы с похожими ситуациями в своей жизни?	
Слайд №26	Теперь пришло время попрактиковаться. На слайде вы увидите признаки видео или фото, созданных с помощью дипфейк технологии. Укажите, что из указанных признаков может помочь определить подделку.	
Слайд №27	На слайде перечислены варианты:	

	• Речь отстает от движения губ; • Плавные движения; • Сказанное или сделанное на видео не характерно для этого человека, если вы его хорошо знаете; • Картинка слишком яркая; • Слишком гладкое лицо, волосы; • Видео длится больше минуты; • Присутствие неестественных теней; • Публикация видео в ненадежном источнике или источнике, известного своей плохой (ненадежной) репутаций; • На фото есть логотип известной компании.	
Слайд №28	А теперь давайте посмотрим, что же из перечисленного действительно поможет определить подделку. Поможет: • Речь отстает от движения губ; • Сказанное или сделанное на видео не характерно для этого человека, если вы его хорошо знаете; • Слишком гладкое лицо, волосы; • Присутствие неестественных теней;	

	• Публикация видео в ненадежном источнике или источнике, известного своей плохой (ненадежной) репутаций. Не поможет: • Плавные движения; • Видео длится больше минуты; • Картинка слишком яркая; • На фото есть логотип известной компании.	
Слайд №29	Вы отлично справились с заданием! Давайте подытожим, как не попасться на уловки злоумышленников, которые используют дипфейк технологии.	
Слайд №30	• Если вы сомневаетесь в подлинности видео или фото, обратите внимание на качество изображения, цвет кожи или глаз, движения; • Внимательно прислушайтесь к качеству звука и речи на видео; • Не отвечайте на щедрые предложения с фото или видео известных вам людей или знакомых; • Установите антивирусное решение, которое сможет распознавать подделки.	

Слайд №31	И последняя на сегодня тема – «Доксинг». Давайте поговорим о том, как информация, которая является подтверждением вашей личности, может распространиться в Интернете без вашего разрешения.	
	Какую информацию в Интернете о себе вы публикуете? Поднимите, пожалуйста, руки те из вас, у кого, например, в социальных сетях опубликованы номер телефона, номер школы или домашний адрес?	
Слайд №32	Доксинг – это раскрытие в сети идентифицирующей информации о ком-либо, такой как настоящее имя, домашний адрес, место работы, номер телефона, финансовая и другая личная информация. Впоследствии эта информация распространяется без разрешения.	
Слайд №33	Давайте посмотрим видеоролик и узнаем, как же злоумышленники могут раскрыть ваши личные данные.	Ссылка на видеоролик:
	Все ли было понятно в видеоролике? Сталкивались ли вы с похожими ситуациями в своей жизни?	
Слайд №34	Теперь пришло время попрактиковаться. На слайдах вы увидите несколько примеров данных, которые	

	могут быть опубликованы в Интернете. Определите, какие из них идентифицируют вашу личность или личность ваших знакомых.	
Слайд №35	На слайде пример: Номер телефона друга	
Слайд №36	Верно, номер телефона может идентифицировать личность человека.	
Слайд №37	На слайде пример: Фото вашего любимого исполнителя	
Слайд №38	Да, фото любимого исполнителя совсем ничего не говорит о вашей личности.	
Слайд №39	На слайде пример: Текст задачи из домашнего задания	
Слайд №40	Точно, это не поможет злоумышленникам определить кто вы.	
Слайд №41	На слайде пример: Ваш адрес, указанный в социальных сетях	

Слайд №42	Верно, адрес может помочь определить вашу личность	
Слайд №43	На слайде пример: Фотография билетов в отпуск	
Слайд №44	Да, на билетах всегда пишется информация о пассажире – имя и фамилия. Поэтому фото всего билета может помочь злоумышленникам узнать ваши данные.	
Слайд №45	Вы отлично справились с заданием! Давайте определим, как не стать жертвой доксинга.	
Слайд №46	• Не публикуйте свои личные данные и данные ваших друзей и близких (например, настоящее имя или фамилию, номер телефона, адрес и место учебы или работы); • Не выкладывайте фото личных переписок и не пересылайте их другим людям; • Не храните личные данные в открытых источниках или облачных хранилищах; • Для защиты своих аккаунтов используйте только уникальные и сложные пароли.	
Слайд № 47	Наш урок подошел к концу. Вы отлично поработали!	

	Соблюдайте безопасность в сети и до новых встреч в новом сезоне проекта «Цифровой ликбез»!	