Контур ЦИФРОВОЙ ЛИКБЕЗ

Технологическая карта урока «Как работает простая электронная подпись?»

Цель урока: повышение уровня цифровой грамотности у обучающихся.

Задачи урока:

- познакомить обучающихся с понятием «простая электронная подпись» (сокр. – ПЭП);
- рассмотреть примеры использования простой электронной подписи;
- представить возможности и опасности, связанные с использованием ПЭП;
- объяснить, как финансовая безопасность связана с простой электронной подписью;
- рассказать о правилах защиты доступов, денежных средств и личной информации с помощью технологии простой электронной подписи.

Ход урока

Слайд	Комментарии педагога
Слайд № 1	Добрый день! Сегодня мы пройдём новый урок в рамках нового сезона всероссийского просветительского проекта «Цифровой ликбез». Урок подготовлен экспертами «СКБ Контур» – компанией, которая разрабатывает продукты для бизнеса: бухгалтерия, учёт и закупки, обмен документами, проверка партнёров. Урок посвящён защите нашей личной информации и денежных средств при действиях в интернете. Разобраться в новой теме помогут герои видеоролика — участники театрального кружка «Котурн» и их наставник.

Слайд № 2	Тема нашего урока – простая электронная подпись. Ребята, поднимите руку, кто хотя бы раз пользовался простой электронной подписью? Знаете, что это такое и зачем она нужна? Скорее всего каждый из вас уже столкнулся с простой электронной подписью, просто не догадывается об этом. Итак, как работает простая электронная подпись и что это?
Слайд № 3	Простая электронная подпись (сокр. – ПЭП) – это уникальная последовательность символов, которая используется для идентификации человека и получения его согласия на какие-либо действия. В ряде случаев эта последовательность представлена в виде кода и/или пароля. Но простой электронной подписью является и галочка, проставленная в поле согласия. А в одной судебной практике даже было дело, когда за ПЭП посчитали лайк на сообщение в Telegram. Авторизуясь на сайте и совершая там действия, вводя код из смс в поле оплаты или проставляя галочку в поле согласия мы идентифицируем себя и подтверждаем, что действие происходит от нашего лица.
Слайд № 4	ПЭП – это и логин с паролем. Мы авторизуемся на сайте – подтверждаем нашу личность и получаем доступ к данным и каким-либо возможностям. В ряде случаев после авторизации мы повторно подтверждаем согласие на операцию, например, при оплате товаров и услуг вводим код из смс в поле оплаты.

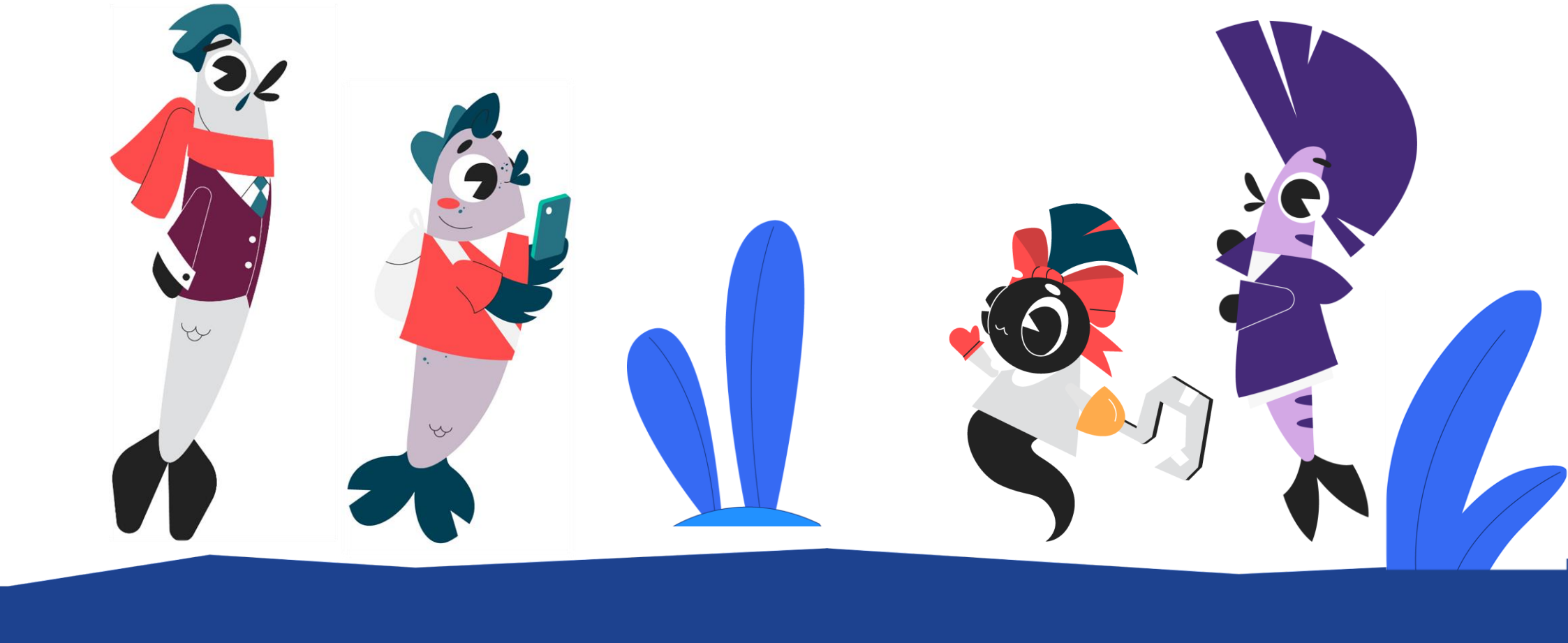
Слайд № 5	Чаще всего мы сталкиваемся с ПЭП, когда оплачиваем покупки через интернет (билеты в кино, доставка еды, товары на маркетплейсах и т.д.). Нам приходит код подтверждения в смс, чтобы мы подтвердили банковский перевод. Но области применения ПЭП шире. Мы можем получать посылки и письма на почте без заполнения извещения и предъявления паспорта. Мы используем ПЭП при заходе на портал «Госуслуг» – так как через него нам оказываются государственные услуги, он имеет усиленную защиту. ПЭП выступает вторым фактором авторизации. Ряд финансовых организаций (банки) также используют ПЭП для второго фактора авторизации или подтверждения согласия на какие-либо услуги. Галочка в форме согласия тоже является простой электронной подписью. Поэтому будьте внимательны, когда на предложение каких-либо условий вы проставляете галочку и нажимаете на кнопку «Принимаю» или «Согласен». В случае вашего несогласия с последующими действиями вам будет сложно откатить всё назад.
Слайд № 6	Ребята, давайте подытожим, какие возможности нам даёт ПЭП? Мы экономим время на получении каких-то услуг (не стояли в очереди, а купили билеты онлайн), можем не носить с собой документы (получили посылку без паспорта), сокращаем передвижение (купили товары в маркетплейсе).

Слайд №7	ПЭП экономит наши время и ресурсы, но накладывает на нас определённую ответственность – мы должны быть внимательными при обращении со своим смартфоном и использовании кодов и паролей. Если экран смартфона не будет заблокирован, а сам телефон попадёт в чужие руки, то есть опасность, что посторонние люди получат доступ к нашим данным и деньгам. Например, если в приложении доставки пиццы автосохранён пароль для входа, то кто-то может оплатить её с нашего счёта. Для пиццерии и для банка операция будет значиться, как инициированная и подтверждённая нами.
Слайд № 8	Вернуть деньги назад будет чрезвычайно сложно. Если мы ввели ПЭП при оплате услуг, то это будет равнозначно подписанию заявления на банковский перевод. Раньше для кражи денег требовалось вскрыть сейф или украсть кошелёк, а сегодня достаточно заполучить ключ электронной подписи и, например, перевести деньги на свой счёт. Поэтому будьте предусмотрительны.

Слайд № 9	Ребята, давайте подумаем, как защитить свои данные, деньги, доступы на сайты. Что вы посоветуете толстолобику Мише и себе? Важно следить за своими вещами – не оставляйте телефон где попало, блокируйте экран телефона. Придумывайте сложные пароли. Если вам звонят и под каким либо предлогом просят сообщить код из смс или push-уведомления – прекращайте разговор и ни в коем случае код не сообщайте. Для того, чтобы заметить пропажу денег со счёта и просто быть в курсе своих средств, необходимо систематично вести учёт потраченных денег. Есть масса приложений, которые позволяют записывать свои траты и указывать категории покупок. Прежде чем ставить галочку и нажимать кнопку «Принимаю» или «Согласен», внимательно читайте, что именно вам предлагают. Иначе можете попасть в неловкую ситуацию, например, ваши фотографии будут использовать для рекламы. Соблюдайте основные правила пользования смартфоном, которые мы неоднократно затрагивали: пользуйтесь только проверенными ссылками, скачивайте файлы с надёжных сайтов, обновляйте антивирус. Посмотрите, есть ли на вашем телефон функция «Найти устройство». Мы можем думать: «Это же просто смс!». Помните, ребята, даже простые действия в интернете могут иметь серьёзные последствия.

Слайд № 10	Давайте закрепим полученные сегодня знания на реальном примере из жизни. Представьте, что вам позвонил человек и представился оператором сотовой связи. Он сообщил вам, что скоро услуги связи будут прекращены, отключится мобильный интернет, потому что закончился срок действия договора (документ, который заключили родители при покупке сим-карты с оператором сотовой связи). Но вы можете легко продлить договор. Надо только назвать код из смс, который придёт в ближайшее время. Как вы поступите?
Слайд № 11	Скорее всего это звонят мошенники. А код из смс они хотят использовать, например, для доступа к вашему счёту или для подтверждения денежного перевода с него. Если бы вам действительно звонил сотовый оператор, то для продления договора пригласил бы вас в ближайший офис связи или сориентировал вас на мобильное приложение. К тому же, договор о предоставлении услуг мобильной связи чаще всего бессрочный за редким исключением. Не сообщайте код из смс подтверждения посторонним людям и не продолжайте разговор. Мошенники хитрые и изворотливые. Они постоянно придумывают новые легенды для выманивания кода подтверждения (простой электронной подписи).

Слайд № 12	Наш урок подходит к концу. Насколько полезным для вас был сегодняшний урок? Что нового вы узнали? Хотите поделиться знаниями с родителями? Какой главный вывод можете сделать? Сегодня интернет открывает перед нами много возможностей, чтобы быть эффективными и тратить меньше усилий на рутинные операции. Но главное пользоваться ими с умом. Так как возможности накладывают на нас дополнительную ответственность – быть бдительными и внимательными.



Словарь

Простая электронная подпись – это комбинация логина и пароля, которая применяется для входа на сайт, получения доступа к электронной почте, онлайн оплаты товаров или услуг. Она необходима для идентификации пользователя, совершающего те или иные действия.

Ключ электронной подписи – уникальная последовательность символов (коды, пароли), предназначенная для создания электронной подписи. Ключ электронной подписи (логин и пароль) может формироваться как на стороне пользователя, так и на стороне информационной системы. Если для авторизации подключена двухфакторная аутентификация, то к связке «логин-пароль» добавляется код, отправляемый пользователю в смс-сообщении.