

План конспект урока по теме «Финансовое мошенничество»

Класс: 10

Форма урока: круглый стол.

Тип урока: комбинированный.

Цель: рассмотреть виды финансового мошенничества,

Задачи: - рассмотреть виды финансового мошенничества:

фальшивомонетки, фальшивые банки, кредит на Ваше имя; -выявить куда можно заявить в случаи мошенничества.

Средства обучения: раздаточный материал, мультимедийный проектор.

Ход урока.

№ П/П	Этапы урока	Деятельность учителя.	Деятельность учеников.
1	Организационный момент.	Приветствие учеников. Создание организационного настроя.	Внимательно слушают учителя.
2	Актуализация знаний.	Учитель показывает слайды жизненных ситуаций. Вопрос: Что общего в этих ситуациях?	Анализируют ситуации. Отвечают на вопрос и формулируют тему урока. «Финансовое мошенничество»
3	Изучение нового материала	Вопросы классу: «Что такое мошенничество? Как вы думаете, как давно люди стали зарабатывать на обмане других людей. Чаще всего мошенники прибегают к использованию сети интернет для массового обмана граждан. Мошенники зачастую осуществляют хакерские атаки на финансовые	Высказывают свою точку зрения.(заранее подготовлена краткая историческая информация о мошенниках)

		<p>организации государства, используя доверчивость и малоинформированность граждан страны. Если каждый гражданин будет бдительным, знать и соблюдать правила защиты своих персональных данных, устанавливать специальные приложения, которые будут защищать безопасных выход в интернет, то каждый сможет сохранить свои деньги и репутацию. Как вы думаете, кто чаще всего становится жертвами мошенничества?</p> <p>Учитель заранее раздал информацию о видах мошенничества.</p>	<p>Ответы учащихся: малоинформированные граждане(подростки, пенсионеры и т.д) Формируют проблему: Нужно ли информировать граждан о финансовых мошенниках? Учащиеся рассказывают о видах мошенничества. Высказывая свою точку зрения.Группа экспертов: формирует памятку. Как не стать жертвой финансовых мошенников.</p>
4.	Закрепление	Вопрос к классу, с какими видами финансового мошенничества вы	Ответы учащихся

		сегодня познакомить?	
5.	Итог урока.	Слушает учеников. Помогает в формировании итога урока. Выставляет оценки за работу на уроке.	Ученики формируют выводы. Группа экспертов озвучивает памятку.

Приложение.

Мошенничество в современном мире отличается исключительной многоликостью, адаптивностью, динамизмом и способностью к модернизации, распространяясь на все виды коммерческой, предпринимательской, финансовой, банковской, бюджетной, кредитной, имущественной и иной деятельности. В связи с усложнением механизмов функционирования хозяйственного комплекса мошенничество стало более изощренным и приобрело ярко выраженный интеллектуальный характер.

Статьей 159 УК РФ мошенничество определяется как «хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием». Финансовое мошенничество – совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.

Величайшие мошенники в истории человечества.

Ученик 1.

Все мы когда либо встречали на своем жизненном пути людей, которые пытались нас обмануть и втянуть в какую-нибудь аферу. Имя им – мошенники. Можете ли вы вообразить, что мошенничество может быть искусством, о котором рассказывают легенды? Мошенничество может вызывать восхищение, настолько тонко и профессионально проворачивают свои аферы мастера-мошенники. Представляем вашему вниманию список из десяти самых великих мошенников за всю историю человечества. 1. На первом месте, безусловно, человек продавший Эйфелеву башню – Виктор Люстиг. Граф Виктор Люстиг(также переводится как Ластиг, Лустиг) (1890-1947) считается одним из самых талантливых мошенников из когда-либо живших на свете. Виктор Люстиг родился в Богемии, Чехия. Свой мошеннический талант он проявил еще в достаточно раннем возрасте. Когда ему было около двадцати лет он сделал фальшивый станок для печатания денег. Когда Люстиг демонстрировал станок клиенту, то при этом жалобно причитал, что машинка может печатать "всего лишь" одну стодолларовую купюру за шесть часов. Клиент, конечно, приобрел станок, так как в то время сто долларов были большой суммой, пусть даже это занимало шесть часов.

Стоил печатный станок тридцать тысяч долларов. В течение следующих двенадцати часов станок выдавал наивному клиенту еще две стодолларовые купюры, но после этого начинал выдавать чистую бумагу. К тому времени, как незадачливый покупатель понял, что его обманули, Люстиг уже был далеко. В 1934 году Виктор Люстиг был арестован и передан суду за подделку денег. За день до суда ему удалось сбежать из федеральной тюрьмы Нью Йорка. Двадцать семь дней спустя он был схвачен в Питсбурге. На суде Люстиг признал себя виновным и получил срок двадцать лет. Его отправили в знаменитую тюрьму Алькатрас в Калифорнии. Он умер в тюремной больнице города Спрингфилд, штат Миссури от пневмонии 9 марта 1947 года. О нем в 1961 году написана книга "Человек, который продал Эйфелеву башню". Автор книги Флойд Миллер (Floyd Miller, The Man Who Sold the Eiffel Tower). Кроме того, многие из его проделок включены в художественные фильмы, рассказывающие о мошенниках._

2. На втором месте находится Фрэнк Абегнейл по кличке "Поймай меня, если сможешь". Уже в семнадцать лет Фрэнк ограбил своего отца на три тысячи четыреста долларов. Как он это сделал? Купив машину, юный Фрэнк уговорил своего отца одолжить ему кредитную карту компании Мобайл (Mobil) занимающейся продажей моторных масел, бензина и запчастей для автомобилей. По кредитной карте он покупал колеса, батареи, двигатели. Затем он продавал это и получал в свое распоряжение наличные деньги, которые он тратил на свидания с девушками. Так как кредитка была на имя его отца, то вскоре кредиторы затребовали от Абегнейла-старшего вернуть им долг в три тысячи четыреста долларов (\$3400). Когда отец призвал его к ответу, Фрэнк сказал ему, что он делал это все из-за девушек: "Они сводят меня с ума", сказал он отцу. Отец простил его, но мать отправила его на четыре месяца в специальную католическую коррекционную школу для юных правонарушителей. Один из его знаменитых трюков был когда он напечатал номер своего счета на чистых депозитных бланках и подсунул эти бланки в пачку с другими. Это означало, что когда человек приходил в банк и заполнял бланк, который подсунул Фрэнк, то деньги поступали не на счет этого человека, а на счет Абегнейла. Таким образом Абегнейл заработал свыше сорока тысяч долларов, прежде чем банк заподозрил неладное. К тому времени, как банк обнаружил, куда уходили деньги клиентов, Абегнейл уже успел снять все деньги со счета и сменил документы, удостоверяющие личность. Кроме обмана банков Абегнейл занимался тем, что выдавал себя за других людей. В течение двух лет он представлялся пилотом авиакомпании Пан Американ Фрэнком Виллиамом, чтобы летать бесплатно по всему миру. Все счета за билеты, еду и жилье отправлялись в авиакомпанию. Абегнейл сделал себе фальшивое удостоверение пилота. Кроме того он получил форму пилота авиакомпании, заявив, что его форма потерялась в химчистке. Позже он представлялся педиатром в госпитале под именем Фрэнк Коннерс. Он перестал выдавать себя за пилота после того, как его чуть не схватила

полиция в аэропорту Нью Орлеана. Он поселился в доме, где его соседом был настоящий врач. Тот уговорил Абегнейла временно поработать в больнице заведующим педиатрическим отделением, пока они не найдут постоянного человека на это место. Когда Абегнейлу было девятнадцать лет, а выглядел он, как мы помним, значительно старше своих лет, он подделал диплом Гарвардского университета, прошел экзамен на профессиональную пригодность и получил работу в офисе генерального прокурора штата Луизиана. Первые два раза он не смог сдать экзамена, но на третий раз, после того как он уже знал какие вопросы задают и после двух недель подготовки он прошел-таки экзамен. В то время Луизиана позволяла проходить такой экзамен юристам много раз.

Абегнейл был схвачен во Франции в 1969 году, когда один из стюардов в самолете узнал его лицо с плаката "Разыскиваются". Двадцать шесть стран, в которых он совершил мошенничества, требовали его передачи себе. Сначала он шесть месяцев сидел в тюрьме во Франции, где он чуть не умер от недоедания и пневмонии, которую он заработал тем, что спать приходилось на каменном полу. Затем его переправили в Швецию, где его судили за подделку чеков. В Швеции он провел еще шесть месяцев в тюрьме. Так как шведские законы запрещают жестокое обращение с заключенными, то в этой тюрьме ему жилось неплохо. Затем его отправили в США, где его приговорили к двенадцати годам тюрьмы. Когда Абегнейла переправляли на самолете в США, он бежал через туалет в самолете. Так как он был знаком с устройством самолетов, он знал, что под унитазом есть решетка, которую можно открыть. Самолет уже почти приземлился и Фрэнк смог выпрыгнуть незамеченным, так как было уже темно. У него были припрятаны двадцать тысяч долларов. Фрэнк собирался купить билет до Бразилии — страны, у которой нет договоренностей с США о выдаче преступников. Он был задержан констеблем Канадской Конной Полиции когда стоял в очереди за билетом.

Сейчас мульти-миллионер Фрэнк Абегнейл владеет компанией "Абегнейл и партнеры" — консалтинговая компания по защите от финансового мошенничества. Он заработал достаточно денег, чтобы вернуть все, что он похитил обманным путем. Он женат, имеет троих сыновей. История Фрэнка Абегнейла была положена в основу фильма Стивена Спилберга "Поймай меня, если сможешь" ("Catch me if you can"), где остроумного мошенника сыграл Леонардо Ди Каприо. В этом фильме Фрэнк Абегнейл получил эпизодическую роль офицера полиции, который арестовывает Леонардо Ди Каприо, игравшего его самого. Фрэнк Абегнейл написал несколько книг. "Искусство воровства" (The Art of the Steal, 2001), в которой он описывает наиболее распространенные мошенничества и напоминает читателям об осторожности. Также в этой книге он рассказывает о том, как распознать вора и предсказывает наступление эры Интернет-мошенничества. После этого он

написал "Руководство по распознаванию кражи" (Real U Guide to Identify Theft) и "Похищение вашей жизни" (Stealing Your Life, 2007). За свои книги Абегнейл заработал свыше двадцати миллионов долларов.

3. Почетное третье место занял мошенник Кристофер Роканкурт, которого прозвали фальшивым Рокфеллером. В 2001 году канадская полиция арестовала мошенника французского происхождения, который провернул ряд грандиозных афер. Кристофер Роканкурт, который родился в 1967 году, утверждал, что он личный друг Билла Клинтона и член семьи Рокфеллеров. Роканкурт был арестован вместе со своей женой — бывшей моделью Playboy Марией Пиа Райес. Женщине инкриминировали жульничество и заведомый обман в корыстных целях ванкуверского бизнесмена на престижном лыжном курорте, расположенном в Вистлере, — излюбленном месте отдыха богатых туристов из Европы и США. По сведениям полиции, Роканкурт бежал в Канаду после того, как был арестован в Восточном Хэмптоне (штат Нью-Йорк) в августе 2000 года. Тогда его обвиняли в том, что он умело ввел в заблуждение десятки состоятельных американцев и выманил у них почти 1 млн долларов. Преступник открыто рекламировал себя в СМИ под именем Кристофера Рокфеллера. На самом деле его мать была проституткой, а отец алкоголиком — уже в возрасте 5 лет родители сдали Кристофера в приют. Когда мошенничество в США было раскрыто, жулику пришлось срочно бежать в Канаду. Служащие отеля в Вистлере рассказали полиции, что Роканкурт всем представлялся знаменитым автогонщиком международного класса, который, чтобы избежать назойливого внимания поклонников, вынужден жить под вымышленным именем. Одна из обманутых им жертв заявила, что аферист также изображал из себя влиятельного финансиста. Известно, что другим людям он представлялся как чемпион по боксу, он также изображал кинопродюсера. Некоторое время самозванец дружил с Микки Рурком. В марте 2002 года Роканкурт был выдан США. Он признал себя виновным по 3 из 11 пунктов обвинения, включая кражу, контрабанду, взяточничество и лжесвидетельство. Он признался, что надул состоятельных граждан на 40 миллионов долларов.

Виды мошенничества:

Ученик 2. Фальшивомонетничество

Мошенничества появились еще в древности как неизменный атрибут «делового мира». Купцы обманывали покупателей, продавали им негодный товар по завышенной цене (бобровую шерсть смешивали с кошачьей, в бочки с салом добавляли гнилое и тому подобное). А другая сторона, не оставаясь в долгу, платила за товар порченными монетами или товарами.

В Древнем Риме донос на фальшивомонетчика сулил гражданину пожизненное освобождение от налогов, а рабу — свободу. Самих же

фальшивомонетчиков сжигали и бросали на растерзание зверям. В Индии таких преступников разрезали бритвами, а во Франции – варили заживо.

На Руси первый фальшивомонетчик был задержан в 1447 году. Им оказался литейщик и весовщик драгоценных металлов Федотка Жеребец, который лил рубли без особого на то разрешения и из некачественного сырья. В 18 веке в России мошенники печатали фальшивые ассигнации и вексели.

Одним из самых знаменитых фальшивомонетчиков советского периода стал Виктор Баранов, который в сарае на своем участке изготавливал 50- и 25-рублевые поддельные купюры. Причем подделки были настолько качественны, что специалисты Гознака поначалу приняли фальшивые купюры за собственные, только изготовленные с нарушением технологии, а милиция считала Виктора Баранова курьером фальшивомонетчиков, который решил взять всю вину на себя, чтобы выгородить сообщников. Потому что не может один человек изготавливать фальшивые деньги такого безупречного качества!

Настоящий бум фальшивомонетничества зафиксирован в 90-х годах с появлением компьютерных технологий. Сегодня задумываться о введении новых защитных знаков на купюрах Гознаку приходится каждые 7-10 лет. Это примерно тот срок, в течение которого преступники успевают изготовить подделку достаточно хорошего качества.

Рынок финансовых услуг развивается поразительными темпами, появляются новые виды платежных средств – карты. А мошенники придумывают все новые схемы получения чужих денег.

Ученик 3.Кардинг

Кардинг – неформальное название мошеннических операций, связанных с банковскими картами, в которых используются сама карта или ее реквизиты. Есть несколько видов кардинга. Первое – это использование потерянных, либо украденных карт, когда банк вовремя не блокирует счет пропавшей карточки, и мошенник его обнуляет. Второе – подделка карт, когда полученная незаконным путем информация о чужой карте эмбоссировается на пластик (белый пластик) или записывается на магнитную полосу подделки или подлинной карты.

Реквизиты платежных карт, как правило, берут со взломанных серверов интернет-магазинов, платежных и расчетных систем, а также с персональных компьютеров (либо непосредственно, либо через программы удаленного доступа, так называемые «трояны» и «черви»).

Еще один вид – заказ по почте, телефону, Интернету различных товаров и услуг с использованием данных платежной карточки человеком, не являющимся владельцем этой карты. Кстати, в проекте закона о [потребительском кредите](#) предусмотрен запрет рассылки пластиковых карт по почте.

Есть две разновидности кардинга – скимминг и фишинг.

Ученик 4.Скиминг

С расширением банкоматных сетей случаи нападения на них растут в арифметической прогрессии. В ход идут самые разные инструменты: лом,

бензопила, кувалда, топор и даже газовая горелка. Подобные сообщения появляются в российских СМИ практически ежедневно.

Но если вскрытие банкоматов – это все же проблема банка, то беда клиентов кредитной организации – в более изощренных способах мошенничества, самым распространенным из которых является так называемый скимминг. Суть его заключается в том, что на банкоматы устанавливается специальное считывающее устройство – так называемый скиммер, который копирует магнитную полосу карты, одновременно устанавливается видеокамера, позволяющая считать пин-код. Напомним, в начале марта этого года объектом такой [аферы](#) стал банкомат в уфимском отделении Альфа-банка.

Также мошенники могут использовать насадку, которая надевается на настоящую клавиатуру и внешне повторяет оригинальные кнопки. Поддельная клавиатура запоминает все нажатые клавиши, в том числе и пин-код.

Можно перехватить данные, которые банкомат отправляет в банк, дабы удостовериться в наличии запрашиваемой суммы денег на счету. Для этого мошенникам надо подключиться к соответствующему кабелю и, не разрывая его, считать необходимые данные. Технически этот вариант сложен для исполнения, но срабатывает почти всегда. Еще один вариант – установка в людном месте фальшивого банкомата.

Ученик 5. Фишинг

Фишинг (от англ. – рыбалка) – это особый вид компьютерного мошенничества. Фишинг-атаки организуются следующим образом: киберпреступники создают [подложный сайт](#), который выглядит в точности так же, как сайт банка, интернет-магазина и других сайтов, позволяющих проводить финансовые расчеты через Интернет. Затем мошенники пытаются обманным путем добиться, чтобы пользователь посетил фальшивый сайт и ввел на нем свои конфиденциальные данные, например регистрационное имя, пароль или пин-код. Используя их, злоумышленники крадут деньги со счетов пользователей.

Зачастую для привлечения пользователей на подложный сайт используется массовая рассылка электронных сообщений, которые выглядят так, как будто они отправлены банком или иным реально существующим финансовым учреждением, но при этом содержат ссылку на подложный сайт. Пройдя по ссылке, вы попадаете на поддельный сайт, где вам предлагается ввести ваши учетные данные. Часто в фишинг-сообщениях используются те же логотипы и оформление, что и в письмах настоящего банка, а также ссылки, похожие на реальный адрес банка в Интернете. Кроме того, сообщение может содержать ваше имя, как будто оно действительно адресовано вам лично. В письмах мошенников обычно приводится правдоподобная причина, требующая ввода вами на сайте «банка» своих данных. Например, ваш банк якобы проводит выборочную проверку безопасности учетных записей или изменил свою компьютерную инфраструктуру, в связи с чем всем клиентам необходимо заново ввести свои личные данные.

Бывает и так, что злоумышленники распространяют вирусные программы через различные интернет-ресурсы – от социальных сетей до обычных новостных сайтов. Клиент, компьютер которого заражен, при попытке войти в личный кабинет перенаправляется на «фишинговые» сайты, которые внешне практически не отличаются от подлинных сайтов интернет-банков

Ученик 6.Смишинг

Смишинг – подвид фишинга. В данном случае мошенничество происходит не через Интернет, а через СМС-сообщения.

Клиент банка получает сообщение от имени банка о том, что возникли некоторые проблемы с его картой, затем следует просьба для решения этих проблем зайти на «фальшивый» сайт или перезвонить по указанному номеру. Одна из разновидностей – «банк» предлагает клиента принять участие в акции. Таким образом, мошенники пытаются выманить реквизиты вашей банковской карты.

Иногда преступники звонят напрямую, говоря, что они являются представителями банка, в котором обслуживается клиент. В ряде случаев авантюристы представляются сотрудниками Банка России и различных федеральных органов исполнительной власти и оповещают о возможности получения денежных компенсаций за ранее приобретенные лекарственные средства, биологически активные добавки и иные категории товаров. Далее предлагается срочно осуществить предоплату в качестве уплаты «налога», «страхового взноса» или «госпошлины», предварительно сообщив свои паспортные данные.

Ученик 7.Кредитные мошенники

Чаще всего мошенники стараются взять кредит или оформить кредитную карту на имя другого человека, не поставив его в известность. В результате банк считает, что кредит взяли именно вы, и начинает предъявлять вам соответствующие требования по его возврату.

Схема получения мошеннического кредита довольно проста. Все, что нужно мошеннику, – персональные данные «заемщика», включая информацию из паспорта, регистрационный адрес и тому подобное.

Напомним один из последних случаев в Башкирии. Недавно суд вынес обвинительный приговор менеджеру по продажам финансовых продуктов ЗАО «Связной Логистика», которая, используя личные данные клиентов, оформила 11 кредитных карт ЗАО «Связной Банк» с лимитом кредитования на общую сумму 510 тысяч рублей. Затем мошенница через банкоматы, расположенные на территории Оренбургской области и Башкирии, сняла эти деньги. Она успела потратить более 465 тысяч рублей.

Еще одна схема мошенничества – так называемые «черные» брокеры. По сути, эта схема похожа с уже широко известными на рынке недвижимости. Так, брокеры обещают оформить кредит в банке, собирают с вас данные, получают кредит на ваше имя, но при этом сообщают вам, что банк отказал в кредите. Таким образом, кредит горе-заемщику платить придется, а доказать что-либо очень сложно.

К сожалению, это не полный перечень всех возможных способов, которые используют мошенники. Чем больше развиваются технологии, тем более современные средства защиты внедряют финансовые организации, но тем изощренней становятся аферы. Однако по-прежнему люди чаще всего попадают на самых простых схемах, забывая об элементарных мерах безопасности.

Памятка. Как не стать жертвой финансового мошенничества.

1.Никогда не теряйте бдительность.

2.Проверяйте информацию, прежде чем что-либо подписывать.

3. Не стоит без расписки и каких-либо подтверждающих документов отдавать деньги кому бы то ни было.

4. Нельзя открывать посторонним людям двери, всегда нужно спрашивать документы, особенно в случаях, когда злоумышленники представляются сотрудниками социальных, коммунальных или иных служб.

5. Ни в коем случае нельзя сообщать незнакомым свои персональные данные, реквизиты счетов или банковских карт, пин-коды, домашние адреса и другую личную информацию.

6.В случае если вы все-таки стали жертвой мошенников, необходимо срочно обратиться в полицию

