ГРУППОВОЙ ПРОЕКТ ПО МОДУЛЮ 8:

«СОДЕРЖАНИЕ И МЕТОДИКА ПРЕПОДАВАНИЯ ТЕМ ПО ФИНАНСОВОМУ МОШЕННИЧЕСТВУ И РИСКАМ»

НА ТЕМУ:

«КОМПЛЕКС ДИДАКТИЧЕСКИХ МАТЕРИАЛОВ ДЛЯ ОБУЧАЮЩИХСЯ 8-9 КЛАССОВ»

ПРОЕКТНАЯ ГРУППА:

Арбузова М.Е.

Бедретдинова И.Н.

Безина Е.А.

Бондарев М.А.

Бородина О.В.

Васильченко В.В.

Васяева М.Н.

Водолазов Д.М.

.

Москва 2020

Содержание.

1. Цели и задачи.
2. Дидактические материалы.

    1) Тестовые задания
    2) Задачи по теме мошенничество и риски в формате ОГЭ

    3) Материалы МЭШ
    4) Игры по теме «Финансовое мошенничество»
    5) Практикум, проблемные задания.
    6) Видеоматериалы
    7) Квизлет.

3. Описание деятельности педагога по возможному использованию на уроках.

1. Цели и задачи.

Цель: ознакомить обучающихся с возможными финансовыми рисками.

Задачи:

- удовлетворение познавательных потребностей обучающихся в области финансов, формирование активной жизненной позиции, основанной на приобретённых знаниях, умениях и способах финансово грамотного поведения;

- приобретение знаний в сфере защиты от финансовых мошенничеств с последующим их применением в повседневной жизни;

- развитие собственной финансовой грамотности и выработка экономически грамотного поведения, а также способов поиска и изучения информации в этой области;

- воспитание интереса обучающихся к дальнейшему получению знаний в сфере финансовой грамотности.

2. Дидактические материалы.

1) Тестовые задания:

1) Совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения — это:

а) Административный проступок

б) Финансовое мошенничество

в) Финансовые риски

г) Особые жизненные ситуации

2) Финансовая пирамида — это:

а) способ обеспечения дохода собственникам капитала за счёт его инвестирования;

б) схема, в которой доход по привлечённым денежным средствам выплачивается за счёт вовлечения новых участников;

в) финансовое учреждение, производящее, хранящее, предоставляющее, распределяющее, обменивающее и контролирующее денежные средства, а также обращение денег и ценных бумаг;

г) нет верного ответа.

3) К признакам финансовой пирамиды можно отнести следующее:

а) декларируемая гарантированная высокая доходность;

б) прибыль за счёт привлечения новых вкладчиков;1.

в) ограниченный доступ к учредительным документам компании;

г) минимальные риски финансовых потерь.

4) К финансовой пирамиде можно отнести:

а) коммерческий банк;

б) кассу взаимопомощи, предлагающую доходность на внесённые средства в размере 40% годовых;

в) государственный пенсионный фонд России;

г) нет верного ответа.

5)К людям на улице может подойти гадалка и предложить погадать. Какие финансовые риски ожидают того, кто согласится на это? Выберите все

правильные ответы.

а) крах иллюзий

б) пропажа кошелька

в) утрата золотых украшений

г) утрата бдительности

д) получение ложной информации о будущем

6)Бизнесмен К. предлагает Вам инвестировать деньги в его бизнес, обещая при этом ежеквартально крупные проценты (25%). К. обращает внимание, что сроки предложения строго лимитированы. Что должно Вас насторожить в этом предприятии? Выберите правильные ответы.

а) отсутствие кредитной истории

б) высокая доходность

в) альтернативная стоимость

г) внешний вид бизнесмена

д) призыв быстро вкладывать деньги

2) Задачи по теме мошенничество и риски в формате ОГЭ

Цель: Задания в форме задач ОГЭ необходимы для понимания и закрепления материала по теме «Финансовое мошенничество и финансовые риски». Учащиеся при решении данных задач имеют возможность проанализировать конкретную ситуацию и высказать свое понимание возможных рисков. Правильное отношение к мошенничеству подразумевает соблюдение простых правил безопасности, критическое отношение к финансовым предложениям и готовность отстаивать свои интересы в сложной ситуации. Кроме того, примеры решения таких задач позволят учащимся успешно решать похожие задания в формате ОГЭ.

Задача 1

В городе N появилась новая инвестиционная компания, о которой никто ранее не знал. В рекламных плакатах, развешанных по всему городу, утверждалось, что эта компания давно работает на финансовом рынке и поэтому способна приносить своим вкладчикам 100% доход в год. Чтобы стать ее инвестором, необходимо сначала внести первоначальный вклад в размере 10 тыс. рублей.

В чем состоит риск инвестирования в такую компанию? Какие действия необходимо осуществить, чтобы обезопасить себя?

Задача 2

Семену пришло сообщение в социальной сети от его друга Петра: «Привет, Семен! Не выручишь деньгами до вторника? А то баланс на телефоне отрицательный, а срочно надо связаться с родителями. Скинь 500 рублей на номер ***».

В чём состоит опасность данной ситуации для личных финансов Семена? Как ему правильно поступить в данной ситуации?

Задача 3

Совершеннолетней Ксении Ярославовне на смартфон пришло сообщение: «Уважаемая Ксения Ярославовна, наш банк, клиентом которого Вы являетесь, проводил розыгрыш 1 млн. рублей, вы оказались победителем. Для подтверждения вашей готовности принять денежный приз пройдите по ссылке ниже в ваш аккаунт в интернет-банкинге нашего банка и нажмите кнопку согласия. После этого Вам на счет будет перечислен выигрыш».

В чём состоит опасность данной ситуации для личных финансов Ксении Ярославовны.? Как ей правильно поступить в данной ситуации?

Задача 4

Совершеннолетней Анне Ф. пришло СМС−сообщение со следующим текстом: Поздравляем! Вы выиграли новый автомобиль BMW, для получения приза свяжитесь с нами по номеру ***. Позвонив по телефону, Анна узнала, что ей необходимо уплатить небольшую сумму в качестве таможенной пошлины за растаможивание автомобиля и получила номер карты, на которую нужна перевести сумму.

В чём состоит опасность данной ситуации для личных финансов Анны Ф.? Как ей правильно поступить в данной ситуации?

Задача 5

Банк предлагает кредит на год под 15% годовых. Знакомый предложил одолжить ту же сумму на тот же срок под 0,1% в день. Предложение знакомого более выгодно.

Так ли это? Какие финансовые риски могут быть в этом случае?

Задача 6

Петр учится в 10-ом классе. Он хочет купить новый смартфон определенной модели и марки, но у него не хватает накопленных денег. Тогда он начинает искать данную модель смартфона в интернете. На одном из сайтов Петр нашел данную модель со стоимостью в три раза ниже, чем в магазине. Единственным условиям, которое насторожило Петра было требование внести 100% предоплаты на электронный кошелек.

В чём состоит опасность данной ситуации для личных финансов Петра? Как ему правильно поступить в данной ситуации?

Задача 7

Листая ленту в социальной сети Аркадий увидел просьбу о помощи ребенку, которому требуется срочная операция, иначе он умрет. В обращении был указан номер карты, на которую можно перечислить материальную помощь.

В чём состоит опасность данной ситуации для личных финансов Аркадия? Как ему правильно поступить в данной ситуации, если он хочет заняться благотворительностью?

Задача 8

Совершеннолетнему Оскару пришло SMS-сообщение с короткого номера: «Уважаемый клиент! Ваша карта заблокирована, перезвоните по телефону *** . Для оперативности приготовьте Ваши паспортные данные и следующие данные по Вашей карте: № и PIN-код. Наш оператор решит данную проблему после вашей идентификации».

В чём состоит опасность данной ситуации для личных финансов Оскара? Как ему правильно поступить в данной ситуации?

Задача 9

Банк предлагает кредит на год под 15% годовых. Знакомый предложил одолжить ту же сумму на тот же срок под 0,1% в день. Предложение знакомого более выгодно.

Так ли это? Какие финансовые риски могут быть в этом случае?

3) Материалы МЭШ.

Библиотека МЭШ содержит образовательные материалы, которые позволяют проводить увлекательные уроки и вовлекать учеников в образовательный процесс

Библиотека МЭШ содержит атомики, а также сценарии уроков, учебные пособия, электронные учебники, образовательные приложения и другие вспомогательные материалы.

Атомики — это авторский контент по отдельным темам: аудиозаписи, видеоролики, изображения.

Вид материала	Тема материала	Адрес материалов
Сценарий урока	Защита от финансовых мошенничеств. Интерактивный урок	**ID:**423387 https://uchebnik.mos.ru/catalogue/material_view/lesson_templates/423387
Сценарий урока	Информационная безопасность в финансовой сфере	**ID:**1086529 https://uchebnik.mos.ru/catalogue/material_view/lesson_templates/1086529
тест	Мошенничество на финансовых рынках	**ID:**4001 https://uchebnik.mos.ru/catalogue/material_view/test_specifications/4001
тест	Деньги. Настоящие и фальшивые.	**ID:**69698 https://uchebnik.mos.ru/catalogue/material_view/test_specifications/69698
тест	SMS-мошенничество	**ID:**4428409 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/4428409
тест	Мошенничество в финансовой сфере Тестовое задание	**ID:**4452441 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/4452441
тест	Защита от финансового мошенничества.	**ID:**2237064 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/2237064
тест	Финансовые махинации	**ID:**842843 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/842843
видео	Гарантируют сверхдоход - это признак мошенничества	**ID:**2529665 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/2529665

видео	Сказка о деньгах. Серия «Если купюра фальшивая»	**ID:**6127123 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/6127123
видео	Не сообщайте никому коды банковских карт	**ID:**2586002 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/2586002
видео	Финансовые махинации с кредитами Видео	**ID:**5493460 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/5493460
видео	Финансовые махинации с кредитами	**ID:**5493460 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/5493460
видео	Подменные номера	**ID:**5326828 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/5326828
видео	Не храните пин-код вместе с картой	**ID:**2586023 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/2586023
видео	Финансовые махинации с кредитами	**ID:**5493460 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/5493460
видео	Финансовые махинации	**ID:**1188665 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/1188665
изображения	Виды финансового мошенничества Изображение	**ID:**5474307 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/5474307
изображения	За мошенничество предусмотрена уголовная ответственность!	**ID:**729251 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/729251
изображения	Виды кредитных махинаций	**ID:**5498519 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/5498519
изображения	Махинации с инвестициями	**ID:**729283 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/729283
изображения	Что делать если вы стали жертвой мошенничества?	**ID:**729277 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/729277

изображения	Пирамиды	**ID:**729319 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/729319
изображения	Признаки финансовой пирамиды	**ID:**729323 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/729323
изображения	Мошенничество	**ID:**826967 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/826967
изображения	Осторожно: не попадись на "удочку" мошенника!	**ID:**729216 https://uchebnik.mos.ru/catalogue/material_view/atomic_objects/729216

4) Игры по теме «Финансовое мошенничество»

«ФИНАНСОВЫЕ МОШЕННИКИ:

КАК РАСПОЗНАТЬ

И НЕ СТАТЬ ЖЕРТВОЙ?»

ЦЕЛЬ ИГРЫ:

в рамках игровой модели, построенной на погружении обучающихся в проблемно-ролевую ситуацию, сформировать навыки рационального финансового поведения в условиях повышенного риска совершения финансовых операций.

Задачи:

а распознавание основных признаков отдельных видов финансового мошенничества;

а выработка моделей поведения в условиях повышенного риска совершения финансовых операций;

а формирование навыков логического обоснования принимаемых финансовых решений на основе объема имеющейся информации и восприятия степени принимаемого на себя риска;

а формирование понятийного аппарата, необходимого для успешной защиты собственных финансов от различного рода финансовых мошенничеств;

а понимание степени влияния принимаемых решений на благополучие конкретного индивидуума и его семьи.

Базовые понятия: финансовое мошенничество, eviltwin/honeypot, нигерийские письма, финансовая пирамида, скимминг, смс-мошенничества, фишинг, кража данных банковских карт.

В результате игры участники должны знать:

● основные виды финансовых мошенничеств;

● ключевые правила безопасности финансовых операций в Интернете и в повседневной жизни;

● последовательность действий при возникновении угрозы финансового мошенничества.

В результате игры участники должны уметь:

● распознавать риски возникновения финансовых мошенничеств при совершении операций;

● выбирать модель поведения при возникновении угрозы финансового мошенничества;

● моделировать риски возникновения новых неизвестных финансовых мошенничеств на основе анализа типичных признаков финансовых мошенничеств.

Количество участников: от 10 до 20 человек.

Роли:

1. Ведущий – модератор, регулирует выполнение правил игры, контролирует ее ход и подводит итоги игры.

2. Жюри – 3 человека, занимаются оценкой правильности выполнения и качества творческой части игры.

3. Капитан команды.

4. Участник команды.

Примечание. Рекомендуется формировать команды численностью в пять человек: капитан и четыре участника.

Материалы: игровые карточки, текст задания, чистая бумага, ручки.

СОДЕРЖАНИЕ ИГРЫ

Современная жизнь наполнена различного рода устройствами, которые облегчают нам совершение разных операций, в том числе и финансовых. Бумажную почту уже давно вытеснили электронные письма; банковские карты постоянно «откусывают» свою долю в расчетах у наличных денег; доступ в Интернет перестал быть привилегией: теперь воспользоваться им может каждый, при этом количество точек для доступа постоянно растет; для совершения банковских операций теперь не обязательно идти в банк: большое количество операций можно осуществить через мобильный телефон. Жизнь стала действительно удобнее. Однако с ростом степени комфорта мы сталкиваемся и с ростом степени риска. Объем сумм, украденных финансовыми мошенниками, и разновидность самих финансовых мошенничеств постоянно растут. Риск потерять свои деньги есть всегда, и если хоть на миг расслабиться и притупить бдительность, это произойдет. Надежда на современные технические средства защиты, безусловно, оправдана, но и ее можно обойти, в результате чего ответственность за возможную потерю собственных денег лежит в конечном счете на самом человеке.

Ход игры

1-й этап – «Знакомство с типичными случаями финансового мошенничества». Игроки изучают карточки, на которых указаны названия финансовых мошенничеств, и пытаются смоделировать ситуации, с которыми могут столкнуться при подобных нарушениях, способы защиты от них.

2-й этап – «Допиши рассказ». Игроки знакомятся с текстом рассказа с пропущенными отдельными фрагментами. Их задача – придумать собственный вариант развития событий.

На первом этапе результаты не подводятся, на втором – их подводят члены жюри, которые за каждый фрагмент, придуманный командой, начисляют баллы в количестве от 1 до 5. По итогам игры выигрывает команда, набравшая наибольшее количество баллов.

Инструкция для участников

В ходе игры Вы погрузитесь в ситуацию, предлагающую прожить один день с ее героем – Олегом. Вам предстоит придумать для него модели финансового поведения в различных ситуациях. Ваша цель – чтобы предлагаемые Вами решения были максимально продуманы, рациональны и не допустили потерю Олегом своих денег. С другой стороны, фрагменты текста, которые вам предлагается придумать, должны быть оригинальны и интересны, для того чтобы жюри смогло выставить за них высокие баллы. Выигравшей будет считаться та команда, которая наберет наибольшее количество баллов по итогам игры.

Инструкция для ведущего

1-й этап. Знакомство с типичными случаями финансового мошенничества (40 минут)

Ведущий сообщает правила игры на данном этапе. Каждой из команд раздаются карточки с названиями типичных финансовых мошенничеств и их краткими описаниями. Членам команды необходимо смоделировать ситуацию, в которой оно могло бы совершиться, и предложить правила поведения, при которых риск попасться на данный вид мошенничества сводился бы к минимуму. Таким образом обсуждение каждого понятия разбивается на два подэтапа:

1) Описать ситуацию, когда вы могли бы столкнуться с данным типом финансового мошенничества (минимально по одному примеру для каждой команды).

2) Предложить правила, при которых можно снизить риск попасться на указанное финансовое мошенничество (высказываются все желающие).

2-й этап. Допиши рассказ (40 минут)

Каждой команде предлагается рассказ, в котором присутствуют пропущенные фрагменты. Задача команды: пояснить, какой вид финансового мошенничества возможен в данном фрагменте, почему принято такое решение, и предложить собственный вариант развития событий. При этом жюри должно учитывать два критерия – правильность выбора вида финансового мошенничества, которому соответствует данный фрагмент, и оригинальность придуманного варианта фрагмента.

СЛОВАРЬ ОСНОВНЫХ ТЕРМИНОВ

Eviltwin/honeypot – вид мошенничества, при котором пользователь подключается к мошеннической wi-fi сети (созданной самим аферистом с помощью обычного ноутбука), после чего все сведения, вводимые пользователем, проходят через компьютер мошенников.

Кража данных финансовых карт (не техническая) – вид финансового мошенничества, при котором при получении доступа к банковской карте клиента злоумышленник копирует все графические данные карты, после чего использует их в собственных целях.

Нигерийское письмо – распространенный вид мошенничества, который основан на массовой рассылке писем (изначально в бумажной форме, затем в электронной) с обещаниями финансового характера (перечислить деньги, оставить наследство, совершить дарение) адресату с условием предварительного совершения определенных финансовых операций последним. Обещания финансового характера никогда не выполняются.

Скимминг – вид мошенничества, при котором третьи лица завладевают электронными данными карты и пин-кодом с помощью технических приборов, расположенных на банкомате (накладная клавиатура, накладка на картоприемник и прочее).

Смс-мошенничества – вид финансовых мошенничеств, при которых производится рассылка смс-сообщений, содержащих ложную информацию и требующих совершить определенные финансовые операции.

Фарминг – вид интернет-мошенничества, при котором от имени общеизвестных компаний жертве предлагается перейти на ее сайт, который внешне почти не отличим от оригинального сайта настоящей компании. На ложной странице сайта пользователю предлагается оставить свои платежные реквизиты, которые, в случае их введения, в дальнейшем используются мошенниками. Каких-либо особых отличий поддельного сайта от настоящего визуальными средствами обычно обнаружить невозможно.

Финансовая пирамида – вид мошенничества, при котором доход участников обеспечивается за счет постоянного притока новых участников. Основным признаком финансовой пирамиды является высокий доход и неопределенность относительно направлений вложения полученных финансовых средств.

Фишинг – вид интернет-мошенничества, при котором от имени общеизвестных компаний жертве предлагается перейти на ее сайт, который внешне почти не отличим от оригинального сайта настоящей компании. На ложной странице сайта пользователю предлагается оставить свои платежные реквизиты, которые, в случае их введения, в дальнейшем используются мошенниками. Мошенничество обычно можно распознать по адресной строке, электронный адрес в которой не соответствует официальному электронному адресу компании.

ПРИЛОЖЕНИЯ

Приложение 1

Рабочий день начинался, как обычно. К 9 часам утра к большому зданию в центре города стекались работники компании. Кто-то весело, кто-то не очень приветствовали друг друга. Наступила среда, до выходных оставалось целых два дня, если не считать сегодняшнего, и особых надежд на неожиданный отдых ни у кого не было.

Олег улыбнулся Ольге, помахал Сергею и сел проверять рабочую почту. Все, как обычно: из общего отдела скинули пару сканов писем, на которые необходимо было срочно ответить, и несколько фотографий сестры. Год назад, когда сестра впервые прислала по ошибке письмо на рабочую почту Олега, он пытался возмущаться. Однако время прошло, и Олег смирился. Неожиданно его взгляд остановился на странном письме. Судя по адресной строке, оно было отправлено с обычного почтового ящика известной российской поисковой системы. Странными были название и, тем более, содержание этого письма. В адресной строке значилось: «Важное сообщение для Вас». Обычно такие письма сразу попадали в спам и до Олега не доходили. Однако в этот день письмо нашло своего

читателя. Олег открыл его и увидел текст на ломаном англо-русском: «Уважаемый Господин! Обращается к Вам миссис Мобуту из Нигерии. Я самая богатая женщина в нашей стране. Недавно случилось со мной несчастье. Я возвращался из поездки к своей Северной плантации кофе и попал в аварию. Горькое несчастье произошло в моей семье – мой муж и мой единственный сын в аварии погиб. Я выжил, но перелом бедра приносит мне ближе к могиле каждый день. Врачи считают, что мне осталось жить совсем недолго – не более одного месяца. Я понимаю, что он прожил счастливую жизнь и те деньги, которые принадлежат мне, не может быть взят с собой в могилу, поэтому я решил пожертвовать им, чтобы любой случайный счастливчик, кто согласится их принять. Так что вам повезло. Я готова составить завещание на Ваше имя, тогда Вы станете полноправным статус владельца на сумму более 125 миллионов долларов. Однако есть одно условие. Вам нужно сделать перевод на сумму 1000 долл в знак согласия на предложение о принятии наследства. Эти символические для меня деньги пойдут на оформление судебных издержек в нашей стране. После улаживания юридических формальностей придет к вам мой адвокат, который будет приносить вам до скорости и будут приглашены в Нигерию. С нетерпением жду Вашего ответа. Искренне Ваша, Миссис Мобуту».

Как должен повести себя Олег?

Объясни рациональность такого поведения.

Только Олег разделался с письмом, как к нему позвонили из приемной генерального директора. Когда он зашел в приемную, секретарь директора передала ему бумагу, на которой размашистым почерком было написано «Командировать О. Веронова». Хотелось или не хотелось Олегу в Волгоград, но именно туда ему было необходимо лететь, причем лететь срочно. Завтра в десять часов утра в офисном центре «Волгоград-Сити» состоится открытие нового филиала фирмы, а Олег на презентации будет представителем офиса головной компании. Сначала туда должен был лететь зам генерального, но погодные проблемы в Калининграде грозили сорвать вылет, и потому, чтобы не рисковать, генеральный решил отправить в Волгоград Олега.

Пятая часть рабочего времени Олега проходила в воздухе, а если учесть ожидания рейсов в аэропортах всего мира, то можно сказать, что четверть своей зарплаты он получал за перелеты. Вот и сейчас сел за компьютер и набрал в поисковой строке название своего любимого сайта для заказа авиабилетов. На экран высыпался столбец ссылок. Олег кликнул по первой из них и попал на страницу со знакомым дизайном. Он сформировал список доступных рейсов. Его несколько смутило то, что список был несколько короче, чем обычно, но, как подумал Олег, Волгоград – не столица мира, чтобы туда летал весь российский авиафлот, потому хватит одной общероссийской любимой воздушной компании. Олег нажал кнопку «оплатить», после чего, в отличие от знакомой страницы перехода на защищенную страницу оплаты, он перешел на другую страницу того же сайта.

Поля оплаты были немного другие: Олегу предлагали заполнить поле с номером карты, cvv кодом карты и ее пин-кодом, и все поля, по заверениям разработчиков сайта, были зашифрованы, а в строке с пин-кодом, якобы, отображались исключительно звездочки. Олег задумался.

Как должен повести себя Олег?

Объясни рациональность такого поведения.

Билет наконец был заказан, и Олег поехал домой за вещами, чтобы ехать в аэропорт. Через два часа он уже был в терминале D аэропорта Шереметьево, быстро прошел регистрацию и досмотр, после чего сел на скамейку с видом на взлетную полосу и открыл ноутбук. Как мы уже написали, пятая часть рабочего времени Олега проходила либо в воздухе, либо в залах аэропорта, поэтому он давно привык работать в любых условиях. Благо wi-fi в большинстве мест, куда он летал, был вполне доступен. Олег включил компьютер. В зоне досягаемости функционировали пять сетей, из которых три – сети близлежащих кафешек, одна – сеть аэропорта Aura, и еще одна – та, которой Олег никогда не пользовался, с благозвучным названием AURA_VIP. У нее был самый сильный сигнал. «Что за VIP? – подумал Олег. – Может, новая сеть, которую создали для пассажиров бизнес-класса и которая в настоящий момент проходит тестирование?» Он подключился к сети. Поскольку до посадки в самолет оставалось 30 минут, Олег решил зайти в свой мобильный банк и перевести оплату за бронь в гостинице.

Как должен повести себя Олег?

Объясни рациональность такого поведения.

Самолет приземлился вовремя. Вздремнув минут 30 в воздухе, Олег чувствовал себя достаточно отдохнувшим. К трапу быстро подогнали автобус, и вскоре вместе со всеми пассажирами Олег уже проходил мимо ленты выдачи багажа к выходу. Где-то в углу девушка радостно кричала о возможности заказать такси до гостиницы, и он решил воспользоваться этим предложением.

– Здравствуйте! – поприветствовал Олег улыбающуюся девушку. – Мне машину до «Х-отеля».

– Конечно, машина уже ожидает Вас на улице у входа – госномер С234ОХ, это ваш автомобиль. Возьмите, пожалуйста, талон, – девушка передала талон Олегу и, кажется, потеряла к нему интерес.

– Оплата наличными или можно картой? – спросил Олег у водителя, когда уже ехал в машине, поскольку вспомнил, что наличных у него нет.

– Наличными. Мы тут картам не доверяем, – усмехнулся водитель.

Олег удивился такому ответу. Машина въехала в поселок, который водитель назвал Городище, и остановилась у банкомата. Банкомат выглядел вполне обычно, но в таком относительно безлюдном месте для Олега снимать наличность было страшновато. Тем не менее он подошел к банкомату.

Как должен повести себя Олег?

Объясни рациональность такого поведения.

И вот, наконец, Олег уже в гостинице. Номер отеля был угловой, и с одной стороны окна выходили на большую площадь с трибунами, по левую сторону от которых стоял театр, судя по трем статуям на фронтоне и афишам по краям. С другой стороны окна выходили на небольшой сквер с высокой стелой посередине и вечным огнем перед ней.

Был вечер, презентация планировалась на следующее утро, а потому Олег решил прогуляться по городу. Он вышел из гостиницы, перешел сквер и подошел к закрытым

дверям универмага. Судя по всему, здание пустовало достаточно долго, поскольку и голые витрины и наглухо закрытые двери свидетельствовали о том, что торговля ушла из этого места безвозвратно.

– Молодой человек! Возьмите листовку! – Олег обернулся. На него смотрела

немолодая взлохмаченная женщина лет 40, довольно помятого вида, в истоптанных туфлях, несвежей блузке. Она сунула ему в руки большой лист дешевой бумаги с растиражированным через ксерокс текстом.

В листовке сообщалось, что только в течение 10 дней потребительский кооператив «Финансовая артель» принимает от населения средства на срок до 3 лет под процентную ставку в размере 31 % годовых. Звонить предлагали до 21 часа вечера. Процент был очень хорошим. Это Олег знал абсолютно точно, поскольку имел несколько вкладов – под 8,5; 12 и 10,1 % годовых. С потребительскими кооперативами Олег дел никогда не имел, а потому не мог доподлинно сказать, почему банковские проценты по ним такие высокие. Он решил позвонить по указанному номеру.

Трубку на том конце взяли почти мгновенно. После просьбы уточнить условия привлечения средств Олегу предложили встретиться, но он отказался: «Я не местный и улетаю буквально завтра. Ответьте на мои вопросы, и я решу, как мне дальше поступить». По словам консультанта, а именно так назвался собеседник, высокий процент объясняется тем, что потребительский кооператив вкладывает свои деньги в самые прибыльные проекты Сколково и других новационных центров России. С другой стороны, потребительский кооператив не тратится на дорогую рекламу, поскольку боится ненадежных и непроверенных клиентов, а кроме того, имеет всего один офис в Волгограде и три по области. Эти преимущества, по словам консультанта, позволяют обеспечивать партнерам высокие проценты. Олег уточнил адрес и время работы. Офис находился совсем недалеко, и потому можно было успеть до закрытия.

Как должен повести себя Олег?

Объясни рациональность такого поведения.

После прогулки Олег решил зайти в одно из кафе на Аллее Героев. Вечер был теплый, но не душный, поэтому он выбрал кафе с открытой верандой. Вдалеке виднелась набережная, залитая теплым светом старых фонарей. Олег выбрал легкий салат, цыпленка и закончил своим любимым капучино. Когда принесли счет, Олег положил карту для оплаты. Девушка взяла ее в руки, поставила на поднос посуду и собралась уходить.

Как должен повести себя Олег?

Объясни рациональность такого поведения

Вечер удался. Олег вошел в гостиничный номер, включил телевизор и лег на кровать. Он достал материалы к завтрашней презентации, сделал несколько звонков сотрудникам, сообщил управляющему офисом, когда он собирается завтра появиться у них перед презентацией. Олег уже готов был заснуть, когда на телефон пришла смс: «Срочно переведи мне на этот номер 1000 руб. Потом объясню. Мама». Номер был незнакомый. Странно, подумал Олег, с чего бы ей писать с другого номера?

Как должен повести себя Олег?

Объясни рациональность такого поведения.

Так прошел день Олега. Он засыпал в уютной кровати номера волгоградского отеля и был абсолютно уверен, что завтра все пройдет хорошо.

Приложение 2

Краткое содержание

отсутствующих фрагментов

Фрагмент 1

Вид мошенничества: нигерийское письмо.

Действия: пометить как спам, не осуществлять никаких финансовых операций.

Фрагмент 2

Вид мошенничества: фишинг/фарминг.

Действия: 1) посмотреть на адресную строку, там должен быть официальный электронный адрес сайта; 2) проверить, запущен ли антивирус, не истек ли срок его лицензии и подавал ли он сигналы о риске фишинга/фар- минга; 3) если в адресной строке информация соответствует действительности, антивирус никаких сведений о фишинговой атаке не подавал и других подозрительных изменений на сайте не обнаружено, то сайтом можно пользоваться. В противном случае от использования сайта необходимо отказаться.

Фрагмент 3

Вид мошенничества: Eviltwin/honeypot.

Действия: 1) узнать у официальных лиц организации наименование ее wi-fi сети и пользоваться только подтвержденными сетями; 2) отключить функцию автоматического подключения к wi-fi сети; 3) не отключать файрволл на компьютере; 4) по возможности не совершать финансовых операций в бесплатных сетях.

Фрагмент 4

Вид мошенничества: скимминг.

Действия: 1) не пользоваться банкоматами в безлюдных местах с низкой проходимостью; 2) проверить отсутствие различных устройств на картоприемнике, за исключением особых антискимминговых устройств, установленных самими банками; 3) проверить устойчивость клавиатуры на банкомате; 4) проверить наличие «пупырышка» на цифре 5 клавиатуры банкомата; 5) проверить отсутствие посторонних лиц за спиной или видеокамер, с которых можно было бы видеть вводимый пин-код.

Фрагмент 5

Вид мошенничества: финансовая пирамида.

Действия: отказаться от предложения.

Фрагмент 6

Вид мошенничества: кража данных финансовых карт (не техническая).

Действия: попросить официантку принести терминал к столу и провести все платежные операции в присутствии клиента. Банковская карта не должна уноситься официанткой.

Фрагмент 7

Вид мошенничества: смс-мошенничества.

Действия: позвонить на телефон родственнику, чтобы узнать о его состоянии. Просьбы, присланные по смс, игнорировать.

5) Практикум, проблемные задания.

Риски и финансовая безопасность: ключевая область финансовой грамотности, включающая возможность определения путей и способов управления финансами с учетом представлений о потенциальных финансовых прибылях или убытках.

Предметные области финансовой грамотности	Компоненты финансовой грамотности	Компетенции финансовой грамотности	
		Базовый уровень	Продвинутый уровень
Риски и финансовая безопасность	Знание и понимание	• Понимать, что такое финансовый риск.	• Знать, что такое финансовые риски, какими они бывают и что все финансовые инструменты связаны с рисками. • Знать о возможностях финансового мошенничества и что нужно делать, чтобы не стать жертвой мошенников
	Умения и поведение	• Уметь защитить личную информацию, в т.ч. в сети Интернет	• Уметь оценивать степень финансового риска продуктов и услуг. • Обладать навыками технологической безопасности, в т.ч. пользования пластиковой картой, банкоматом, платежами через Интернет и др.
	Личные характеристики и установки	• Быть способным реально оценивать свои возможности. • Развивать критическое мышление по отношению к рекламе	Осознание последствий рискованного поведения

Ключевая проблема темы: В нашей жизни часто происходит так, что отдельные события способны нанести вред личным сбережениям. Но, если пытаться их предотвратить, то приведет к еще большим тратам. Можно ли защититься от угроз так, чтобы они не оказывали разрушительного влияния на нашу жизнь?

Для решения ключевой проблемы темы необходим алгоритм, который сведет ее до решения более узких задач: 1. Как управлять бытовыми рисками? 2. Как управлять финансовыми рисками? 3. Как не стать жертвой мошенников?
Задача 1. «Как управлять бытовыми рисками?»
Многим людям негативные события представляются чем-то внезапным и неотвратимым. Можно ли рационально описать неприятные и непредвиденные события, которые происходят в нашей жизни?
Алгоритм задачи 1:
1. Понимать, как оценивается риск и какая информация для этого нужна.
2. Делать предварительную оценку вероятности и ущерба и выявлять существенные риски в своей жизни, учитывая специфику рисков разного происхождения.
3. Корректировать предварительную оценку, учитывая личные особенности.
4. Собирать дополнительную информацию об особенностях наиболее существенных рисков, влияющую на выбор способа реагирования на них.
5. Реалистично оценивать собственные возможности защититься от разных рисков, расставлять приоритеты и выбирать способы реагирования на них.

Практически в любой деятельности люди сталкиваются с нехваткой информации, из-за которой возникают неопределенность и риск. Люди так или иначе оценивают риски на бытовом уровне и выбирают привычный для себя способ реагирования. Однако привычные способы реагирования часто оказываются не соответствующими меняющейся жизненной ситуации. Существенно уменьшить угрозы и потери можно, освоив рациональный подход к управлению рисками разных типов. Однако собрать всю информацию обо всех рисках невозможно, т.к. это требует затрат ресурсов. Поэтому нужно выявлять наиболее существенные риски, изучать их взаимосвязи и подбирать подходящие способы реагирования на риск: избегание, принятие, страхование или финансирование.

Ключевые понятия задачи 1: неопределенность, риск, субъективная оценка риска, статистическая оценка риска, значимость риска, устранение неопределенности, бремя собственника, карта рисков, принятие риска, страхование риска, избегание риска, финансирование риска.

Задача 2: «Как управлять финансовыми рисками?»

В отличие от бытовых рисков, финансовые риски возникают лишь при использовании финансовых инструментов. Но как минимум один из них (деньги) используют все, поэтому с финансовыми рисками сталкивается каждый. Эти риски особенно важны при выборе инвестиционных продуктов и в предпринимательской деятельности, но также имеют значение при выборе потребительских финансовых продуктов (кредитов, страховок, банковских карт и т.д.). Человеку нужно понимать, когда он оказывается в ситуации риска, осознавать его содержание и особенности, и при необходимости собирать дополнительную информацию. Что можно сделать, чтобы использование финансовых инструментов не приводило к неприятным и неожиданным последствиям?

Алгоритм задачи 2:
1. Учитывать наличие у всех финансовых инструментов специфических рыночных рисков.
2. Учитывать социально-экономический контекст, в котором принимаются финансовые решения.
3. Выбирать организации-контрагенты с учетом их рискованности.
4. Корректно трактовать неудачу при принятии финансовых решений.

В управлении финансовыми рисками применяется тот же алгоритм, что и в управлении бытовыми рисками, но у финансовых рисков есть особенности, которые необходимо учесть. Финансовые риски связаны с договорами, сделками и т.п., которые мы заключаем. Управляя всеми финансовыми рисками, человек должен определить, насколько рискованно решение о выборе финансового продукта, насколько оно устойчиво к внешним угрозам (в т.ч. исходящим от социально-экономической ситуации), и насколько надежен контрагент (организация, с которой заключена сделка). Чтобы ответить на эти вопросы, может потребоваться консультация специалиста или платные услуги по сбору информации. Для того, кто не собирается торговать на фондовом рынке, нет никакого практического смысла читать учебники по фондовому рынку. Но если человек использует какой-то финансовый продукт, то он должен быть готов и к появлению рисков, грамотно собирая необходимую для их оценки информацию

Ключевые понятия задачи 2: финансовый риск (в узком смысле), рыночный риск, риск контрагента, неудачное решение, ошибочное решение.

Задача 3: «Как не стать жертвой мошенников?»

Среди рисков с большими финансовыми последствиями и высокой вероятностью особое место занимает мошенничество. Каждый из нас слышал страшные рассказы про кражу денег с кредитных карт, обманутых дольщиков жилья и т.д. Насколько правдивы эти слухи, и можно ли что-то предпринять, чтобы самому не оказаться жертвой мошенников?

Алгоритм задачи 3.
1. Выявлять признаки мошенничества и перепроверять информацию, в достоверности которой есть основания сомневаться.
2. Не допускать «утечки» конфиденциальной информации.
3. Пресекать мошеннические действия, оставаясь в рамках закона.
4. Оказавшись жертвой мошенников, использовать предоставленные законом возможности для получения компенсации.

Приемы мошенников постоянно изменяются, поэтому научиться противодействовать каждому из них невозможно. Вместо этого нужно думать о защите информации, которую могут использовать мошенники, и быстро замечать признаки опасности. Поэтому правильное отношение к мошенничеству подразумевает соблюдение простых правил безопасности, критическое отношение к финансовым предложениям и готовность отстаивать свои интересы в сложной ситуации. Однако полностью защититься от всех возможных угроз невозможно. Поэтому, выбирая, что и как защищать, нужно определять приоритеты и учитывать взаимосвязи рисков мошенничества с другими рисками.

Ключевые понятия задачи 3: мошенничество, персональные данные, конфиденциальность.

Таким образом, решение ключевой проблемы (ключевые выводы) темы «Можно ли защититься от негативных событий так, чтобы они не оказывали разрушительного влияния на нашу жизнь?» состоит в том, чтобы оценивать риски и выбирать среди них наиболее значимые и грамотно управлять ими. Некоторые риски поддаются контролю в большей степени (бытовые риски), другие – в меньшей (форс-мажорные обстоятельства, страновые риски и т.д.). Для разных категорий рисков могут использоваться разные способы реагирования (принятие, страхование, финансирование, избегание). Финансовые риски относятся к управляемым, так как люди самостоятельно принимают решения в этой сфере,

но для этого нужны базовые знания об экономике и обществе. Это же касается и рисков мошенничества: соблюдение правил безопасности позволяет их избегать.

Практикум.

Цели практикума:
1. рассмотреть примеры финансового мошенничества;
2. выявить основные методы финансовых мошенников;
3. выявить «слабые» стороны потерпевших от финансовых мошенников;
4. выявить «зоны риска» встречи с финансовыми мошенниками;
5. создать «Памятку правильного поведения для минимизации рисков от действий финансовых мошенников ».

Подготовительные задания:

1. Вам нужно снять деньги с карты. На противоположной стороне улицы в стену магазина встроен уличный банкомат. Улица плохо освещена, и возле банкомата стоят какие-то люди. Ваши действия?

Решение: Старайтесь пользоваться банкоматами внутри отделений банков. Их чаще проверяют и лучше охраняют. Проверьте банкомат: нет ли на нем посторонних устройств. Клавиатура не должна отличаться по фактуре, а тем более шататься. Когда вводите ПИН-код, всегда прикрывайте клавиатуру свободной рукой, чтобы никто не подсмотрел.
Лучше всего, если на банкомате есть «крылья» для клавиатуры — на них невозможно поставить накладную клавиатуру. Также благодаря им сложнее подсмотреть ваш ПИН-код.

2. Вы хотите продать свой старый телефон через сайт объявлений в интернете. С вами связался заинтересованный покупатель и готов перевести деньги вам на карту. Он просит вас сообщить номер карты, срок действия, имя держателя на английском языке, а также трехзначный код на оборотной стороне карты. Так деньги точно дойдут. Ваши действия?

Решение: Такой подход должен вас насторожить — для перевода денег достаточно знать только номер карты. Если вы передадите основные платежные данные карты, то рискуете остаться без денег. Мошенники смогут расплатиться картой в интернет-магазине.

3. Вам на мобильный телефон звонит человек и, представляясь сотрудником банка, сообщает, что по вашей банковской карте была проведена подозрительная операция, из-за чего банк заблокировал карту. Для разблокировки вам необходимо сейчас сообщить всю важную информацию: ФИО, номер карты, ПИН-код, трехзначный код на оборотной стороне карты.

Решение: Сотрудники банка владеют необходимой информацией для блокировки карты. Им незачем спрашивать ее у вас. Не реагируйте на подобный звонок, в случае сомнений перезвоните в банк по телефону, указанному на оборотной стороне карты.

4. На вашу электронную почту приходит письмо с адреса известной платежной системы: «Мы подвели итоги лотереи держателей карт нашей платежной системы. Поздравляем вас с победой в конкурсе! Перейдите по ссылке для получения приза». Вы перешли по ссылке и видите знакомую вам страницу сайта, правда, немного худшего качества, чем всегда (логотип платежной системы какой-то нечеткий). Перед вами форма для заполнения информации по вашей карте, куда вам перечислят деньги. Ваши действия?

Решение: Мошенники копируют известные сайты, используя похожее название компании и оформление. Например, вы хотите узнать, поступила ли стипендия на вашу карту, вводите

логин и пароль на сайте банка, а попадаете на сайт-клон. Если вы введете на таких сайтах свои данные, они попадут в руки злоумышленников. В данном случае о том, что это сайт-клон, говорит нечеткое изображение логотипа. Если попробуете открыть другие страницы сайта, они могут не открываться.

5. На ваш мобильный телефон пришло сообщение: «Вам поступил платеж 200 рублей». При этом вы не пополняли счет своего телефона. Вы удивлены. Через 10-15 минут приходит новое сообщение: «Извините, ошибочно перевела 200 рублей на ваш счет. Пожалуйста, верните деньги на мой номер х-ххх-ххх-хх-хх. Лиза».

Решение: Такая ситуация больше похожа на мошенническую схему: скорее всего, деньги не приходили, СМС пришло не от вашего банка, а повторное СМС прислал вам злоумышленник. Проверьте состояние вашего счета, закажите выписку в онлайн-банке или позвоните в банк, прежде чем переводить кому-то деньги.

Анализ ситуаций:

1. Тридцатилетний житель Омска потерял 12300 рублей, пытаясь сэкономить на авиабилетах. Молодой человек проанализировал несколько сайтов по поиску билетов на самолет, пока не нашел ресурс с выгодным перелетом. Для покупки билетов необходимо было ввести данные банковской карты, что, в общем-то, обычное дело при таких операциях. Однако после списания денег никаких авиабилетов омичу не прислали. А сайт, где он нашел выгодный перелет, и вовсе закрыли. Как выяснили полицейские, у ресурса не было ни юридического лица, ни собственного офиса, ни даже отзывов клиентов.
2. В полицию обратилась 61-летняя женщина, с банковской карты которой аферисты украли 31 тысячу рублей. Оказалось, что она в интернете подбирала кредит и оставила заявку на сайте одного из московских банков. Позже с ней связался человек, представившийся работником этого самого банка. Он сообщил, что кредит женщине одобрят, если она погасит имеющуюся задолженность по другому займу. Просьба банковского служащего пенсионерку не смутила: она предоставила ему доступ к своему мобильному банку. Мошенники опустошили счет женщины, а ее заверили, что к ней уже выехал курьер с кредитными средствами. Разумеется, никто к пожилой читинке не приехал, а телефонный номер, с которого звонил банковский служащий, оказался недоступен.
3. Трое молодых людей вступили в преступный сговор с целью хищения денежных средств ПАО СК «РОСГОСТРАХ» во Владимирской области путем обмана относительно наступления страхового случая с использованием машины, имеющей механические повреждения кузова. 29 мая 2017 года злоумышленники на участке автодороги Собинка-Лакинск-Ставрово инсценировали дорожно-транспортное происшествие с участием автомобилей Ауди А4 и ВАЗ 21074. Данные о якобы имевшем место ДТП они сообщили сотрудникам государственной инспекции безопасности дорожного движения, которые, не подозревая подвоха, произвели его оформление. 31 мая 2017 года один из участников мнимой аварии предоставил в филиал ПАО СК «РОСГОСТРАХ» по Владимирской области пакет документов, необходимый для страхового возмещения убытков по полису обязательного страхования гражданской ответственности и получил от страховой компании около 190 тыс. рублей. Деньги молодые люди потратили на личные цели.
4. 39-летний мужчина, действуя как физлицо, а также от имени трех подконтрольных юрлиц, размещал в Интернете объявления о продаже сельхозпродукции (пшеница, просо, семена подсолнечника) по ценам ниже рыночных. После заключения договоров с потенциальными покупателями обвиняемый приобретал небольшие

партии якобы продаваемой им продукции, которые для создания видимости исполнения договорных обязательств направлял клиентам. Затем он требовал полную предоплату за крупные партии товаров, после перечисления которой на связь с покупателями больше не выходил. Таким способом злоумышленнику удалось похитить у восьми юридических лиц и четырех индивидуальных предпринимателей более 25 млн рублей.

Примерное содержание «Памятки правильного поведения для минимизации рисков от действий финансовых мошенников»

1. Перед снятием денег в банкомате осмотрите его. На картоприемнике не должно быть посторонних предметов, клавиатура не должна шататься.
2. Старайтесь пользоваться банкоматами, установленными в безопасных местах (например, в отделениях банков).
3. Набирая ПИН-код, прикрывайте клавиатуру рукой. Делайте это даже во время расчетов картой в кафе или магазинах.
4. Если вам приходят СМС с уведомлениями о блокировке карты или якобы совершенных транзакциях, никогда не перезванивайте по номеру, указанному в СМС. Всегда звоните только по номеру колл-центра банка, указанному на официальном сайте, или по номеру телефона, указанному на оборотной стороне карты.
5. Ссылки из сообщений незнакомцев не лучший способ искать заработок в интернете, потому что бесплатный сыр бывает только в мышеловке.
6. Если незнакомцы пишут вам от лица компании или бренда, лучше уточнить информацию на официальном сайте компании или ее странице в социальной сети - крупные компании редко проводят конкурсы, в которых вы можете победить, даже не участвуя, и никогда просто так не запрашивают ваши личные данные, а тем более данные карты.
7. Если вам приходит на почту письмо от незнакомца, например иностранца, или от известной компании, то ничего страшного не произойдет, если вы просто откроете письмо. Но не переходите по ссылкам и не скачивайте вложения из письма - так вы рискуете заразить компьютер вирусом, который позволит мошенникам его контролировать.
8. Думайте о последствиях своего решения.
9. При наличии опасности пострадать от финансового мошенника, не вступайте с ним в контакт; если контакт уже есть, то прервите его.

Знайте о своих слабых сторонах. Помните, что мошенники – прекрасные психологи, поэтому будьте бдительны.

6) Видеоматериалы.

Видео:

https://drive.google.com/file/d/1iqb4pkW0vwokJFHX15Y4bac0-xPaJkcz/view?usp=sharing

Вопросы к видеоматериалу:

1.Как обезопасить себя при работе с банковской картой?

- не пользоваться банкоматами неизвестных банков

-не расплачиваться картой в сомнительных местах, интернет-магазинах

- не отдавать в руки свою банковскую карту, расплачиваться самостоятельно, прикладывая/вставляя карту в терминал для оплаты

- не сообщать никому PIN-код банковской карты

- не верить смс-сообщениям с требованием подтвердить ваш PIN-код обратным сообщением

2. В каких странах опасно расплачиваться банковской картой? Приведите в качестве примера 3-5 стран

- Бразилия

- Мексика

- Сирия

- Иран

- Албания

- Тайланд

- Молдавия

3. Какие действия рекомендуется выполнять для сохранения личных, банковских средств?

- подключить услугу «SMS-оповещение»

- завести 2-3 карты, для возможности экстренной блокировки карты

- установить лимит оплаты и выдачи средств

7) Квизлет.

https://quizlet.com/ru/527874593/Финансовое-мошенничество-flash-cards/?x=1jqU&i=2r42x2