Муниципальное казенное общеобразовательное учреждение

Даниловская средняя школа им. А. С. Макаренко

ИНДИВИДУАЛЬНЫЙ ПРОЕКТ НА ТЕМУ:

**«АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЛИЧНОЙ ФИНАНСОВОЙ БЕЗОПАСНОСТИ»**

Выполнила:

учащаяся 11 класса

Юрова Алиса Сергеевна

Руководитель проекта:

Лукова Наталья Александровна,

учитель математики

СОДЕРЖАНИЕ

|  |  |  |
| --- | --- | --- |
|   | Введение…………………………………………………………………. | 3 |
|  | Теоретическая часть………...………………………………………….. | 4 |
|  | Практическая часть …………………………………………………….. | 12 |
|  | Заключение……………………………………………………...………. | 14 |
|  | Список литературы…………………………………………..…………. | 15 |

ВВЕДЕНИЕ

 Сегодня невозможно представить жизнь современного человека без денег. Они нужны нам для покупки еды, одежды, оплаты транспорта и других услуг. Однако современные деньги подразделяются на наличные и электронные, и все они подвергаются рискам.

 В наше время много мошенников и недобросовестных людей, которые стремятся получить чужие деньги. В последнее время финансовые потери случаются очень часто на всех уровнях, начиная от макроэкономического и затрагивая отдельных граждан. Поэтому значительная часть финансовых махинаций проводится именно в области личных финансов граждан. По статистике к 50-60 годам гражданин России накапливает определённую сумму, которая в последствии становится приманкой для мошенников.

 В мире финансов орудуют множество мошенников, действия которых в большинстве случаев являются законными. Во избежание всех рисков я решила изучить данную тему, чтобы не попасть в различные уловки и защитить свои финансовые накопления. Именно поэтому целью данной работы является: изучение и приобретение знаний о мошенниках и их уловка и способах минимализации рисков.

 Для реализации цели я поставила следующие задачи:

1) Выяснить, что такое личная финансовая безопасность.

2) Изучить виды мошенничества, а также способы распознания мошенников и их уловок.

3) Узнать, что делать, если остались обманутыми.

4) Сделать буклет с рекомендациями по защите банковской карты от мошенников.

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

**1.1. Финансовая безопасность.**

**[Финансовая безопасность** – это такое состояние финансовой системы, при котором относительно устойчиво функционируют все её элементы**.]1**

Личная финансовая безопасность постоянно подвергается угрозам. К угрозам личной финансовой безопасности относится:

1) Бедность населения;

2) Социальное расслоение населения;

3) Высокий уровень безработицы;

4) Неравномерность экономического развития регионов страны.

Для того чтобы минимизировать количество угроз личной финансовой безопасности, государству необходимо проводить политику повышения уровня финансовой грамотности населения. Следовательно, личная финансовая безопасность зависит как от гражданина, так и от государства.

**Финансовое мошенничество**

**[**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».**]2**

**[Финансовое мошенничество** – совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.**]3** Наша жизнь высоко технизирована, поэтому всё чаще случаются случаи мошенничества.

**1.2. Виды мошенничества:**

**Страхование.**

Во всем цивилизованном мире люди обращаются к помощи страховых компаний. Страховые взносы принято считать способом избежать личных рисков. Страховка призвана возместить угон или порчу машины, пожар на даче и т.д. Теоретически за небольшой взнос можно получить серьезную финансовую защиту. К сожалению, на нашем рынке полно фирм, чей настоящий бизнес — собирать деньги и по возможности ничего никому не выплачивать. А если платить, то минимум.

При выборе страховой компании целесообразно провести анализ по нескольким направлениям:

 • Просить любые предложения в письменной форме.

 • Ни на что не соглашаться сразу, внимательно изучать документы.

 • Собирать и анализировать всю информацию о страховой компании.

 • Посмотреть различные рейтинги страховых компаний.

 • Проверить работу и узнать о репутации страховой компании.

**Мошенничества с использованием банковских карт.**

Мошенничеством с банковскими картами по ст. 159.3 считается хищение денежных средств с использованием похищенной или подделанной банковской карты. Как правило, при этом фиксируются факты обмана сотрудников кредитных, торговых или других организаций. Под статью также подпадают аналогичные действия, совершенные группой лиц по предварительной договоренности, которые привели к нанесению финансового ущерба гражданину. Мошенничеством считается также хищение денежных средств одним лицом или группой лиц с использованием служебного положения в крупных и особо крупных размерах.

Основные приемы, которые используют злоумышленники:

1) Скимминг – это установка специальных устройств на банкоматы, с помощью которых преступники получают информацию о карте: накладная клавиатура или миниатюрная камера, которая заснимет процесс ввода ПИН-кода, и устройство для считывания данных карты. Перед пользованием банкоматом внимательно осмотрите его на предмет наличия посторонних предметов.

2) «Магазинные мошенничества». Данные карты могут быть считаны и зафиксированы ручным скиммером. Поэтому не передавайте карту или ее данные посторонним, требуйте проведения операций с картой только в личном присутствии.

3) Траппинг. На банкомат устанавливаются устройства, которые блокирует карту. На помощь человеку приходит мошенник, который подглядывает ПИН-код и после ухода человека достает карту из банкомата. При вводе ПИН-кода закрывайте рукой клавиатуру.

4) Фишинг. Рассылка электронных писем о якобы производимых изменениях в системе безопасности банка. Мошенники просят дать информацию о карте, в том числе указать номер кредитки и ее ПИН-код отправив ответное письмо или заполнив анкету на сайте, похожем на сайт банка-эмитента. Самая сложная задача мошенника — узнать ваш ПИН-код. Никому не сообщайте его.

5) Вишинг (голосовой фишинг). Сбор информации о номерах карт и счетов при помощи моделирования звонка автоинформатора.

Меры безопасности:

• Храните ПИН-код отдельно от карты и не пишите его на карте, не сообщайте никому и не вводите ПИН-код при работе в Интернете.

• Сохраняйте документы до окончания проверки правильности списанных сумм.

• Сообщайте банку актуальные контактные данные.

• Подключите услугу SMS- уведомлений, всегда имейте при себе телефон службы поддержки.

**Интернет – мошенничества.**

Для проведения операций в финансовой сфере сейчас широко используют онлайн-сервисы. Но развитие технологий способствует активизации аферистов в Интернете. Обманывать доверчивых граждан в Сети гораздо проще, чем оффлайн. Существует несколько популярных видов мошенничества:

1) Покупки через интернет. Продавец просит оплатить товар через систему денежных переводов, используя фальшивое или недействительное удостоверение личности. Получая деньги, он исчезает.

2) Письма платежных систем, к которым прилагается вирус, замаскированный под вложение – файл или ссылку. Его задача – собрать данные о ваших аккаунтах в платежных системах и данные банковских карт.

3) Двойники интернет-магазинов. Невероятно дешевые товары и горячие предложения за полцены призваны завлечь ничего не подозревающих онлайн-покупателей. Через поисковые системы пользователи переходят по ссылке, проходят регистрацию и вводят информацию о своем банковском счете для завершения покупки. В итоге продавец получает оплату и пропадает или присылает совершенно иной товар. Нужно всегда проверять адресную строку в браузере. Она должна начинаться с "https" (безопасный протокол передачи данных), это означает, что ресурс имеет защищенное (шифрованное) соединение, хотя и не гарантирует полной безопасности.

4) Взлом аккаунтов и рассылка от друзей с целью наживы. Мошенники пишут на почту или в социальные сети родственникам и знакомым владельца страницы с просьбой срочно перевести деньги, придумывая различные ситуации.

5) Предложения выгодного заработка. Недобросовестные работодатели предлагают удаленную работу. Но предварительно требуют оплатить организационные нужды. Как только человек переводит деньги, выдуманная организация пропадает с радаров.

Способы защиты:

• Не открывайте сайтов платежных систем по ссылке в письмах, проверяйте URL в адресной строке, посмотрите, куда ведет ссылка.

• Совершайте покупки в интернете с помощью отдельной банковской карты и только на проверенных сайтах.

• Не сообщайте ваши пароли, вводите их только на сайтах платежных систем.

• Не храните файлы с секретной информацией на доступных или недостаточно надежных носителях информации, делайте несколько копий таких файлов.

• Не оплачивайте никаких взносов, при трудоустройстве на удаленную работу.

• Предложения в духе «вышлите туда-то небольшую сумму и вскоре вы будете завалены деньгами» как правило от организаторов финансовых пирамид.

• В 99 % случаев платежи, которые вы делаете онлайн, отменить нельзя. Поэтому не торопитесь, подумайте, прежде чем заплатить за товар или услугу.

**Мобильные мошенничества.**

Основой мошеннических схем служит персональная информация, полученная на нелегальном рынке баз данных интернет-магазинов, финансовых учреждений, государственных структур. **[**«Телефонные мошенники похищают со счетов россиян 3,5-5 миллиардов рублей ежемесячно. Средний чек по успешной мошеннической операции находится на уровне 8 тысяч рублей» - говорит Станислав Кузнецов (зампред правления Сбербанка). **]1**

Самые распространённые случаи мобильных мошенничеств:

1) «Вы выиграли приз». Мошенник привлекает жертву дорогим подарком, который он «выиграл», при этом просит прислать подтверждающую СМС, внести регистрационный взнос и т.п. Получив деньги, мошенник исчезает.

2) «Мама, я попал в аварию». Мошенник отправляет СМС или звонит с неприятной новостью, «жертва» в панике забывает проверить достоверность полученной информации и переводит средства на счета мошенников.

3) «Ваша карта заблокирована». На мобильный телефон приходит соответствующая СМС с указанием телефона для разблокировки, по которому мошенник предлагает жертве совершить несколько операций с банкоматом под диктовку. Деньги с карты перейдут на счет мошенников.

4) Вирус. Он помогает злоумышленникам подобраться к банковской карте, привязанной к мобильному телефону, и перевести все деньги на свой счет.

Способы защиты:

• Не отвечайте на СМС и не открывайте ММС от неизвестных абонентов.

• При получении сообщений от банков, мобильных операторов о проблемах со счетом перезвоните по известному вам номеру банка и уточните информацию.

• Не отправляете СМС на короткие номера, заранее не узнав его стоимости.

• Не сообщайте никаких персональных данных. Попросите представиться, назвать ФИО, звание должность, наименование организации… Узнайте телефон этой организации в справочных базах и перезвоните.

• Если вам сообщают, что ваш родственник или знакомый попал в беду и за него нужно внести деньги - позвоните ему напрямую.

• Ценную информацию не храните только в телефоне, дублируйте ее в бумажном блокноте или в компьютере.

**Финансовая пирамида.**

**[Финансовая пирамида** – это такая модель получения дохода, где происходит перераспределение денежных средств от нижестоящих участников пирамиды к вышестоящим. То есть верхушка пирамиды всегда получает больше, чем нижние звенья.

Часто финансовые пирамиды маскируются под инвестиционные фонды и различные коммерческие проекты, которые якобы вкладывают ваши денежные средства в высокодоходные финансовые инструменты или «сверхприбыльные проекты».**]5**

Чаще всего финансовая пирамида работает по следующему принципу: организаторы пирамиды собирают у вкладчиков деньги (продают ценные бумаги пирамиды), но не вкладывают эти деньги в экономику, а оставляют у себя. Они объявляют о росте курса своих ценных бумаг и, когда старые вкладчики хотят снять свои деньги с процентами, с ними расплачиваются деньгами новых вкладчиков.
Пирамиды обычно обещают сверхвысокую доходность: 200—300% в год. Так как поначалу число вкладчиков всё время растёт, организаторы пирамиды могут какое-то время поддерживать её платёжеспособность.
Опасность пирамиды заключается в том, что рано или поздно она рухнет. Слишком много вкладчиков одновременно захотят продать свои ценные бумаги. Организаторы поймут, что расплатиться со всеми не получится, приостановят выплаты, а потом скроются с оставшимися деньгами.

Меры безопасности:

• Не поддавайтесь на агрессивную рекламу и обещания гарантированной доходности выше ставки банковского депозита.

• Обратите внимание на признаки финансовых пирамид: высокая доходность за счет непрозрачных сверхприбыльных проектов в другой стране, сокрытие организаторами информации о себе, отсутствие лицензий, обещание вознаграждения за приведенных друзей.

• Принимайте взвешенные решения, не поддавайтесь эмоциям.

**1.3 Что делать если вас обманули мошенники?**

Если вы подверглись действию мошенников и у вас пропали деньги, то в первую очередь необходимо обращаться в полицию.

Можно оставить заявление о действиях мошенников:

1) по телефону горячей линии МВД 8-800-222-74-47

2) на сайте МВД

3) в отделении полиции по месту жительства

Также можно обратиться в банк. **[**По закону банки обязаны вернуть клиенту незаконно списанные средства, если не докажут, что клиент сам нарушил правила использования карты (п.15 ст. 9 закона «О национальной платёжной системе»)**]6**

Если вложили деньги в финансовую пирамиду:

**[**1) Если компания ещё существует, соберите документы, которые доказывают факт мошенничества, и подайте письменную досудебную претензию;

2) Найдите других пострадавших — например, через социальные сети;

3) Подайте коллективный иск в суд;

4) Обратитесь в Банк России. Он не выплатит пострадавшим деньги, но проведёт собственное расследование и передаст результаты в прокуратуру. Возможно, это поможет найти мошенников быстрее

Если организацию признали пирамидой, деньги могут вернуть — но только те, которые вложили лично вы. Из этой суммы вычтут полученный доход и проценты, если они были. Максимальная сумма к возврату — 35 000 рублей.**]6**

ПРАКТИЧЕСКАЯ ЧАСТЬ

При исследовании данной темы был проведён опрос среди учащихся школы. Цель опроса – выяснить знают ли учащиеся о мошенниках и их уловках, а также о том насколько часто они сталкиваются с теми или иными видами мошенничеств. С помощью диаграмм были проиллюстрированы ответы учащихся.

1. Знаете ли вы, что такое финансовое мошенничество?

2. О каких видах мошенничеств вы знаете?

3. С какими видами мошенничеств вы сталкивались?

В результате можно наглядно наблюдать то, что значительная часть опрошенных знают о мошенничестве и его видах. Среди опрошенных большая часть подвергалась интернет – мошенничествам и мобильным мошенничествам. Из этого следует сделать вывод, о том, что необходимо проводить беседы с учащимися о мошенничестве и рассказывать о действиях, если ты уже стал жертвой мошенников.

ЗАКЛЮЧЕНИЕ

В последнее время всё чаще встречаются случаи мошенничества по отношению к личным финансам граждан, поэтому я решила подробно изучить эту тему.

Цель данной работы заключалась в изучении и приобретении знаний о мошенниках и их уловка и способах минимализации рисков. Эта цель была полностью достигнута.

В ходе выполнения данной работы я выяснила, что такое личная финансовая безопасность и от чего она зависит.

Также я изучила основные виды мошенничества и как правильно защититься от каждого из них.

Был проведён опрос среди учащихся школы, в ходе которого я выяснила что значительная часть опрошенных знают о мошенничестве и его видах. Среди опрошенных большая часть подвергалась интернет – мошенничествам и мобильным мошенничествам. Из этого следует сделать вывод, о том, что необходимо проводить беседы с учащимися о мошенничестве и рассказывать о действиях, если ты уже стал жертвой мошенников.

Кроме этого, я узнала, что необходимо делать, если ты подвергся действию мошенников.

По результатам работы был составлен буклет с рекомендациями по защите банковской карты от мошенников, который может применяться на внеурочных занятиях по финансовой грамотности.

СПИСОК ЛИТЕРАТУРЫ

1. <https://center-yf.ru/data/Yuristu/Finansovoe-moshennichestvo.php>
2. [**center-yf.ru**›data…Finansovoe-moshennichestvo.php](https://center-yf.ru/data/Yuristu/Finansovoe-moshennichestvo.php)
3. [**http://15.rospotrebnadzor.ru**](http://15.rospotrebnadzor.ru/bytag3/-/asset_publisher/5Wso/content/%D0%BB%D0%B8%D1%87%D0%BD%D0%B0%D1%8F-%D1%84%D0%B8%D0%BD%D0%B0%D0%BD%D1%81%D0%BE%D0%B2%D0%B0%D1%8F-%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C)
4. <https://www.mos.ru/otvet-dengi/kak-zaschititsya-ot-finansovyh-moshennikov/>
5. [Осторожно! Финансовые пирамиды!](https://35.xn--b1aew.xn--p1ai/press/consultation/Ostorozhno_Finansovie_piramidi%22%20%5Ct%20%22_blank)
6. [**[gosuslugi.ru](https://35.xn--b1aew.xn--p1ai/press/consultation/Ostorozhno_Finansovie_piramidi%22%20%5Ct%20%22_blank)**[›situation/financial\_fraud/when\_](https://35.xn--b1aew.xn--p1ai/press/consultation/Ostorozhno_Finansovie_piramidi%22%20%5Ct%20%22_blank)](https://www.gosuslugi.ru/situation/financial_fraud/when_deceiving)