Муниципальное бюджетное общеобразовательное учреждение

«Отрадовская средняя общеобразовательная школа»

Исследовательский проект

**«ФИНАНСОВАЯ БЕЗОПАСНОСТЬ»**

Работу выполнила:

ученица 9 класса

Воропаева Яна

Руководитель:

Дудник Е. Г.

с. Отрадовка,

2024

ОГЛАВЛЕНИЕ

|  |  |
| --- | --- |
| ВВЕДЕНИЕ...................................................................................................... | 3 |
| ГЛАВА 1 ФИНАНСОВАЯ БЕЗОПАСНОСТЬ И ВИДЫ МОШЕННИЧЕСТВА....................................................................................... | 5 |
|  1. 1 Финансовая безопасность. Финансовое мошенничество...... | 5 |
|  1. 2 Мошенничество с банковскими картами……......................... | 6 |
|  1.3 Интернет-мошенничество…………………………………….. | 7 |
|  1.4 Мобильное мошенничество…………………………………... | 8 |
| ГЛАВА 2 ПРАКТИЧЕСКАЯ ЧАСТЬ…………………................................. | 13 |
|  2.1 Анкетирование по теме исследования…………..……............. | 13 |
| ЗАКЛЮЧЕНИЕ................................................................................................ | 17 |
| СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ......... | 18 |
| ПРИЛОЖЕНИЕ.............................................................................................. | 19 |

ВВЕДЕНИЕ

Финансовая грамотность заключается в таком способе управления всей совокупностью составляющих личных финансов, при котором молодежь будет двигаться из настоящего навстречу своему желаемому будущему, то есть к собственным финансовым целям, к желаемому образу жизни!

В данном проекте было рассмотрено мошенничество ‒ одно из самых распространенных преступлений в России. Ежегодно возбуждаются тысячи дел по статье 159 УК РФ.

Актуальность работы определяется тем, что в наше время много мошенников и недобросовестных людей, которые ежедневно заполучают чужое нажитое имущество себе. Во избежание этого было принято решение изучить тему финансовой безопасности подробней, дабы не попасть в различные ловушки и уловки, защитив свои финансовые накопления и помочь другим подросткам.

Цель исследовательской работы: изучение видов мошеннических схем, разработка рекомендаций по финансовой безопасности.

Объект исследования: виды мошенничества.

Предмет исследования: личная финансовая безопасность.

Для достижения цели были поставлены следующие задачи:

1. Изучить литературу по данному вопросу.
2. Познакомиться с понятием «финансовая безопасность».
3. Изучить виды мошенничества.
4. Провести анкетирование по теме исследования.
5. Составить рекомендации по финансовой безопасности.
6. Проанализировать и обобщить полученные данные, сделать выводы по результатам исследования.

Мною была выдвинута следующая гипотеза:

Чем больше подростков ознакомятся с информацией о способах распознавания мошеннических схем, тем меньше  будут риски потерь собственных средств.

Методами исследования стали: изучение источников информации (книги, статьи, сайты), анализ, анкетирование, проведение исследования.

 Работа проводилась в три этапа:

1. Поиск и сбор информации.

2. Проведение исследовательской работы.

3. Систематизация материалов, оформление работы.

Работа состоит из введения, двух глав, заключения, списка используемых источников и литературы, а также приложения.

ГЛАВА 1 ФИНАНСОВАЯ БЕЗОПАСНОСТЬ И ВИДЫ МОШЕННИЧЕСТВА

1. 1 Финансовая безопасность. Финансовое мошенничество

Финансовая безопасность – понятие, включающее комплекс мер, методов и средств по защите экономических интересов государства на макроуровне, корпоративных структур, финансовой деятельности хозяйствующих субъектов на микроуровне.

В России существуют разные уровни финансовой безопасности: национальный, региональный, корпоративный (организации), личный.

Любой уровень финансовой безопасности могут нарушить финансовые мошенники. Финансовое мошенничество угрожает финансовой безопасности

личности. Для того, чтобы эффективно противостоять ему, необходимо разобраться с тем, что оно из себя представляет и каким бывает.

Мошенничество по российскому законодательству, согласно ст. 159 УК РФ, представляет собой неправомерное завладение чужими деньгами или имуществом с целью обращения его в свою пользу или в пользу третьих лиц, совершаемое с помощью обмана или злоупотребления доверием. Далеко не все деяния, попадающие под эту статью, имеют характер финансовых. Практика, скорее всего, назовет ими только действия, имеющие два признака:

* преступление совершается в финансовой сфере с использованием ее ресурсов и механизмов, основано на применении опыта добросовестных банков, страховых компаний, инвестиционных фондов;
* преступление носит массовой характер, оно разрабатывается в целях хищения средств у большого числа лиц, не нацелено на одного человека, не имеет индивидуального характера, в его разработке и реализации также участвует группа лиц, иногда имеющая интернациональный характер.

 Для понимания, каким образом мошенники побуждают физических и юридических лиц добровольно расстаться с деньгами, нужно изучить классификацию наиболее часто встречающихся видов финансовых мошенничеств. В любом случае в своей основе они имеют продуманный план, организацию, каждый из участников которой отвечает за свой участок работы, возможность замены участника или метода. Все эти подготовительные меры приводят к хищению средств в большинстве случаев. Среди наиболее распространенных видов мошеннических схем являются: мошенничество с банковскими картами, интернет-мошенничество, мобильное мошенничество.

1. 2 Мошенничество с банковскими картами

Рассмотрим эти виды мошеннических схем подробнее. Для начала мы поговорим о мошенничестве с банковскими картами: скимминг. Самым распространенным способом кражи реквизитов карты при ее использовании в банкомате – это установка на банкомат скиммера. Это специальное устройство, которое копирует данные с магнитной полосы карты. Могут украсть и ПИН-код, установив на банкомат скрытую камеру или накладную клавиатуру. Поддельную клавиатуру ставят прямо поверх оригинальной, и сам банкомат реагирует на нажатия как обычно – вы даже не заметите, что что-то идет не так. Злоумышленники, используя украденные данные, могут изготовить копию вашей карты.

Также существует еще одна мошенническая схема с банковскими картами – траппинг. Траппинг – это разновидность мошенничества с банковскими картами. Его схема заключается в следующем: злоумышленник устанавливает в картридер банкомата надрезанный специальным образом кусок фотоплёнки, пластика или другого материала. Карта, попадая в прорезь картридера, не возвращается держателю, а попадает в «ловушку». Пока гражданин решает вопрос возврата карты, мошенники вытаскивают из картридера свой кусок пластика вместе с картой посетителя.

Необходимо помнить, что главнейшая задача мошенников в отношении вашей банковской карты – это раздобыть ПИН-код от нее. Не сообщайте ее никому и не при каких условиях. Как не стать жертвами скимминга и траппинга:

* Перед снятием денег в банкомате осмотрите его.
* На картоприемнике не должно быть посторонних предметов, клавиатура не должна шататься.
* Набирая ПИН-код, прикрывайте клавиатуру рукой. Делайте это даже во время расчетов картой в кафе.
* Старайтесь пользоваться банкоматами внутри отделений банков. Их чаще проверяют и лучше охраняют.

Если карта все же попала в руки злоумышленников, что делать?

* Позвонить в банк (номер всегда есть на обороте карты), сообщить об
этом и заблокировать карту.
* Запросить выписку по счету и написать заявление о несогласии с
операцией.
* Обратиться с заявлением в отдел полиции по месту жительства или
отправить обращение в управление МВД России.

1.3 Интернет-мошенничество

Следующая схема финансовых мошенников –  интернет-мошенничество: фишинг (сайты двойники). Мошенники копируют известные сайты, используя похожее название компании и оформление. Например, вы хотите узнать, есть ли у вас штрафы в ГИБДД или как оформить кредит онлайн, а попадаете на фишинговый сайт, то есть сайт-клон. Если вы введете на таких сайтах свои данные, они попадут в руки злоумышленников.

  Интернет-мошенничество используют и в виде дорогих подарков. Вам на почту присылают письма с обещанием подарков, денег и кредитов.

Мошенники пытаются заманить вас чем угодно: предлагают работу с большой зарплатой, которую вы не искали. Пишут, что вы выиграли машину, телефон и т.п. Присылают ответ на якобы ваше письмо. Просто хотят «познакомиться поближе», а затем «выжать» из вас некоторую сумму.

Как не попасть на  мошеннический сайт:

* обращайте внимание на адресную строку браузера: на сайте-клоне будет допущена ошибка;
* оплачивайте покупки только через сайты с защищенным соединением и значком платежной системы;
* внимательно изучите и содержание сайта – злоумышленники часто невнимательно относятся к наполнению сайта;
* добавьте в закладки сайты, которыми часто пользуетесь, чтобы
не набирать адрес вручную.

1.4 Мобильное мошенничество

Мобильные телефоны стали для нас одним из самых ценных видов имущества, и киберпреступники об этом знают. Мы всегда носим их с собой и используем для доступа к важнейшей информации. К нашим телефонам привязаны учетные записи от банков, электронная почта и другие конфиденциальные данные, что делает их идеальной мишенью для злоумышленников.

Задача мобильного мошенника – вынудить вас самостоятельно заразить свое устройство или передать ему конфиденциальную информацию.

К самым популярным видам мобильного мошенничества относятся:

1. Сообщения о заражении мобильного телефона вредоносной программой.
2. SMS-фишинг («смишинг»).
3. Мошенничество с помощью телефонных звонков («вишинг»).
4. Сбрасывающиеся звонки.

Сообщения о заражении мобильного телефона вредоносной программой.

При этом виде мошенничества на экране устройства отображается поддельное сообщение об обнаружении вредоносной программы.

Такое могло случаться с вами при просмотре интернет-страниц. В сообщениях обычно говорится, что в ходе сканирования на телефоне было обнаружено вредоносное ПО и вам необходимо принять срочные меры.

Вам будет предложено загрузить «антивирус», который на самом деле является вредоносной или шпионской программой. После того как вредоносный код внедрится в ваш смартфон, злоумышленники смогут получить к нему полный доступ или заразить другие устройства. Самый простой способ защититься от подобных атак – установить на свой телефон защиту, например [антивирус для устройств на Android](https://www.google.com/url?q=https://www.kaspersky.ru/android-security&sa=D&source=editors&ust=1650001581052785&usg=AOvVaw1sc4ocQcKSsE2yGJRzu13-).

Телефонный вишинг

Вишинг – это вид мошенничества, при котором вам звонят, пытаясь побудить вас к какому-либо действию.

Обычно мошенники притворяются реальными людьми или компаниями, чтобы завоевать ваше доверие. Они могут сказать, что работают в реально существующей организации, чтобы убедить вас сообщить им свои личные данные или перевести деньги.

И действий от вас ждут прямо во время телефонного разговора. Мошенники создают ощущение срочности, чтобы вы запаниковали и сделали то, чего они хотят. Вот почему они требуют заплатить или раскрыть данные прямо во время звонка, а не просят выполнить какое-то дополнительное действие позднее (после завершения разговора).

SMS-фишинг

При SMS-фишинге, или «смишинге», злоумышленники будут призывать вас к действию с помощью текстовых сообщений.

В таком сообщении может содержаться [вредоносная ссылка](https://www.google.com/url?q=https://www.kaspersky.ru/resource-center/threats/sms-attacks&sa=D&source=editors&ust=1650001581053521&usg=AOvVaw1amt8P3X8TaMq3f1QF5oMR), перейдя по которой вы загрузите на свое устройство вредоносную или шпионскую программу. Но иногда злоумышленники вынуждают жертву совершить другие действия, например перезвонить на платный номер, оформить подписку или выдать личные данные.

Сбрасывающиеся звонки

Сбрасывающиеся звонки – это вызовы с неизвестного номера, которые длятся [всего пару секунд](https://www.google.com/url?q=https://www.howtogeek.com/449936/what-is-a-wangiri-or-one-ring-phone-scam/&sa=D&source=editors&ust=1650001581053830&usg=AOvVaw38ApecajJ7qepMoZYz7U3a). Это сделано для того, чтобы вынудить вас перезвонить на этот номер. Как правило, такая схема срабатывает, если ваше любопытство перевешивает критическое мышление. Хитрость в том, что обратный звонок на подозрительный номер будет платным. На этом мошенники и зарабатывают. Обычно эти звонки совершаются с международных номеров, за что с вас и снимают деньги. Иногда мошенники оставляют сообщение в голосовой почте – это повышает шанс того, что вы решите перезвонить. Будьте осторожны, принимая звонки или прослушивая голосовую почту с неизвестного номера.

Что делать, чтобы не попасться на мобильное мошенничество?

Лучше всего защититься от мошенников вам поможет сознательное отношение к коммуникации по телефону. Помимо умения распознавать обман вам помогут и некоторые дополнительные меры обеспечения безопасности конфиденциальных данных.

Вот несколько полезных советов для защиты от мобильного мошенничества:

1. При подключении к публичным сетям Wi-Fi используйте виртуальные частные сети (VPN). Шифрование в VPN-сети скроет передаваемую информацию от чужих глаз. Такие сервисы также обеспечивают анонимность, так что вас нельзя будет выследить с помощью IP-адреса или других средств.
2. Установите сложные пароли. Никогда не используйте один и тот же пароль дважды. Лучше всего создавать пароли из случайного набора знаков. Чередуйте регистр и помимо букв используйте цифры и специальные символы. Если ваш пароль – это кодовая фраза, состоящая из нескольких коротких и запоминающихся слов, замените некоторые буквы в ней символами или числами.
3. Используйте длинный ПИН-код. Если ваше устройство позволяет, вместо четырехзначного ПИН-кода установите на экран блокировки ПИН-код из шести знаков. Шестизначный ПИН-код образует больше возможных комбинаций, затрудняя [подбор пароля злоумышленником](https://www.google.com/url?q=https://www.kaspersky.com/resource-center/definitions/brute-force-attack&sa=D&source=editors&ust=1650001581054473&usg=AOvVaw37c-4M7S7qzjg9FAyedWwS), желающим взломать ваш телефон или учетные записи. Никогда не используйте в качестве пароля даты и другие личные данные, так как хакеры, пытаясь подобрать пароль, в первую очередь обращаются к информации, которую можно найти о вас в интернете. Также откажитесь от стандартных числовых комбинаций вроде «0000» или «1234».
4. Храните свои пароли в безопасном онлайн-хранилище. Чтобы не забывать свои пароли и ПИН-коды, воспользуйтесь сервисом наподобие [Kaspersky Password Manager](https://www.google.com/url?q=https://www.kaspersky.ru/password-manager&sa=D&source=editors&ust=1650001581054770&usg=AOvVaw0MOQBOP_ZDWV9cdv5lxqXS) . Никогда не записывайте пароли в блокноте или в заметках на телефоне – это крайне ненадежно. Менеджеры паролей шифруют ваши данные таким образом, что взломщики не смогут их подсмотреть. Вам нужно будет запомнить всего лишь один пароль – от самого хранилища. Конечно, его нужно сделать максимально сложным и надежным, чтобы никто не смог получить туда доступ.
5. В настоящих розыгрышах никто не будет требовать с вас денег. Если кто-то просит вас заплатить за приз, откажитесь от затеи. Скорее всего, вы имеете дело с мошенниками.
6. Установите приложение, блокирующее звонки. Такие приложения защищают ваш телефон от звонков, нелегально выполняемых роботами, и прочих типов телефонного мошенничества. Однако они не всегда работают идеально и могут отправлять в спам реальные номера. К счастью, многие приложения помечают входящие звонки как потенциальный спам, позволяя вам самостоятельно решить, брать трубку или нет.
7. Не вступайте в разговор и положите трубку. Участие в разговоре в любом виде может спровоцировать еще больше звонков. Не нажимайте на кнопки для навигации по автоматизированному меню и не отвечайте живым операторам, если заподозрили неладное. Просто повесьте трубку и поищите в интернете информацию о звонящем, если вас все еще одолевает любопытство.
8. Пользуйтесь только официальными приложениями. Использование сторонних приложений для входа в такие сервисы, как онлайн-банки и социальные сети, делает ваше устройство уязвимым к несанкционированному доступу. Более того, если вы предоставите свои учетные данные сторонней организации, вы можете потерять их, оказавшись жертвой фишинга. Желательно избегать приложений, предназначенных для работы сразу с несколькими сервисами: всегда делайте выбор в пользу официальных программ.
9. Проверяйте телефонные счета. Если вы обнаружили в счете несанкционированные списания, вероятно, вы стали жертвой злоумышленника. Если это произошло, немедленно обратитесь к оператору и требуйте вернуть средства. Даже если причиной такого списания было не мошенничество, вы наконец отключите нежелательные услуги, накопившиеся за годы.
10. Установите защиту на свой телефон. Самый простой способ сохранить конфиденциальность в интернете и данные на своем телефоне – это защитить их. Мы рекомендуем воспользоваться решением [Kaspersky Security Cloud](https://www.google.com/url?q=https://www.kaspersky.ru/security-cloud&sa=D&source=editors&ust=1650001581055623&usg=AOvVaw3gkYVcfjrS6pYhZZhfzUhe) , охватывающим сразу несколько устройств. Подписка Family позволит вам настраивать родительский контроль – так вы защитите себя, своего партнера и детей, если они у вас есть.

ГЛАВА 2 ПРАКТИЧЕСКАЯ ЧАСТЬ

 2.1 Анкетирование по теме исследования

В целях подтверждения или опровержения теоретических положений, указанных выше, было проведено анкетирование, в котором участвовало 40 человек. Гражданам были предложены вопросы, связанные с самыми распространенными видами финансового мошенничества. Анкетирование было анонимным, предлагалось только указать возраст опрашиваемого респондента.

Результаты

1. С какими видами мошенничества вы сталкивались?

Из диаграммы 1 видно, что среди опрошенных всех возрастных категорий самым распространенным видом мошенничества является мошенничество с использованием банковских карт. Пожалуй, эти данные очевидны, т.к. и молодые и возрастные граждане в подавляющем большинстве пользуются банковскими картами и хранят на них свои денежные средства. Среди молодежи, которые значительную часть своего времени проводят в сети Интернет, распространены интернет-мошенничества. В возрасте от 25 до 40 лет люди часто попадаются на уловки мошенников по телефону. Мобильное мошенничестве смело занимает второе место у граждан среднего возраста после незаконных операций с банковскими картами. А в более зрелом возрасте граждане попадаются на удочку мошенников практически регулярно. Примечательно, что участие молодых людей и людей старше 25 лет в финансовых пирамидах незначительно, в то время как граждане старше 40 и пенсионеры, несмотря на негативный опыт 1990-х гг. всё ещё пытаются разбогатеть, вкладывая деньги в такого рода схемы.

2. Сталкивались ли вы со списанием средств с банковской карты?

Если посмотреть на диаграмму 2, то мы увидим, что большинство людей, у которых есть банковская карта, сталкиваются с несанкционированным списанием средств с нее. Данные диаграммы свидетельствуют о том, что люди, близкие к пенсионному возрасту чаще других возрастных категорий становились жертвами мошенников. Довольно сложно сформулировать однозначный вывод по этим сведениям, но можно предположить, что граждане старшего поколения пренебрегали элементарными правилами информационной безопасности, например, осуществляли покупки в интернете на незащищенных сайтах, предоставляли конфиденциальную информацию о банковской карте третьим лицам и др. Гораздо более предусмотрительнее в этом плане ведёт себя молодежь. Результаты опроса показали, что более половины молодых людей в возрасте от 18 до 25 лет не сталкивались со списанием средств с банковской карты. Однако, в целом, данные анкетирования, конечно, неутешительные. Все категории граждан хотя бы раз в жизни подвергались атакам финансовых преступников. Эти данные дают нам повод задуматься над повышением способов защиты своих карт.

3. Страховали ли вы в банке свою банковскую карту?

Данные Диаграммы 1 и Диаграммы 2 позволяют прийти к однозначному выводу: основным видом несанкционированных действий в области финансовой безопасности граждан стало списание с банковских карт граждан денежных средств. Эффективным средством защиты от мошеннических действий становится страхование банковских карт коммерческими банками, которые их выпускают. Иными словами, если не удалось сберечь денежные средства, то их хотя бы вернет страховая компания, правда, в случае, если будет доказан факт мошенничества. Тем не менее, данные Диаграммы 3 свидетельствуют о том, что граждане всех возрастных категорий не спешат обезопасить себя от действий финансовых преступников таким способом. Можно только догадываться о мотивах, лежащих в основе такого поведения, но всё же некоторые причины отказа от страхования можно указать. Для людей старшего поколения банковские услуги ложатся дополнительным бременем на их бюджет, воспринимается как навязывание, не приносящее реальной пользы. Граждане среднего возраста и молодежь, возможно, надеются на традиционный русский авось, думая, что эта проблема их не коснется.

 Из проведенного мной анкетирования можно сделать вывод, что самыми уязвимыми категориями граждан являются люди старшего поколения, они чаще всего попадаются на удочку мошенников. Во избежание неприятных последствий, необходимо проводить работу по финансовому просвещению граждан с целью сократить число жертв финансовых мошенников.

ЗАКЛЮЧЕНИЕ

В эпоху становления и развития в мире информационного сетевого общества, формирования глобального интернет-пространства на повестке дня появляются вопросы связанные с формированием финансовой безопасности личности. Возможности современных цифровых и информационных технологий сделали жизнь человека намного более удобной, мобильной и комфортной. Однако, часто за всеми преимуществами постиндустриальной цивилизации мы не замечаем как уязвима наша жизнь, особенно в сфере кибернетики. Новыми возможностями пользуются, к сожалению, преступники, фактически воруя с глобальной сети наши личные данные, пароли, а порой и денежные средства. Финансовая безопасность граждан во многом зависит от их самих. Огромной проблемой для держателей банковских карт является незаконное списывание денежных средств с них, а попросту говоря, кража. Помимо мер, предпринимаемых финансовыми организациями по защите карт от такого рода действий, граждане должны придерживаться минимальных рекомендаций по обращению с картами. Но если данный вид мошенничества относится к таким видам, когда от действий владельца карты порой ничего не зависит, то потеря денег через скимминг, фишинг, траппинг является результатом банальной доверчивости, жадности, а порой и глупости. Важно помнить, что все финансовые операции, будь то выплата выигрыша или перевод средств, имеют сложную процедуру и не могут осуществляться одним нажатием кнопки мобильного телефона.

 В заключение хочется сказать, что наша финансовая безопасность зависит только от нас самих и от принимаемых нами решений. Для того чтобы избежать неприятных финансовых потерь следует придерживать определенных правил, которые не гарантируют, что вы не станете жертвой мошенников, но повысят ваши шансы на то, чтобы сохранить денежные средства и оставить финансовых преступников ни с чем.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

* 1. Гладкий Алексей Мошенничество в Интернете. Методы удаленного выманивания денег, и как не стать жертвой злоумышленников / Алексей Гладкий. - М.: АВТОР, 2019. - 899 c.
	2. Даниил Алексеевич Зыков Компьютерное мошенничество: / Даниил Алексеевич Зыков. - М.: LAP Lambert Academic Publishing, 2018. - 188 c.
	3. Липсиц И.В., Рязанова О.И.: Финансовая грамотность: материалы для учащихся 8-9 классов - М.: ВАКО, 2020. – 207 с.
	4. Яновская Оксана Анатомия обмана. Энциклопедия мошенничества / Оксана Яновская. - М.: Питер Пресс, 2018. - 192 c.
	5. Виды мошенничества и способы защиты/URL:https://утурфо.мвд.рф/informacia/info\_dlya\_grajdan/виды-мошенничества-и-способы-защиты (дата обращения: 17.01.2024).
	6. Елизарова В.В. Финансовая безопасность: понятие, роль и основные пути обеспечения/URL: http://ucom.ru/doc/conf.2014.11.15.pdf (дата обращения: 05.12.2023).
	7. Риски и финансовая безопасность // Материалы VВсероссийской недели финансовой грамотности для детей и молодежи/ URL:
	http://fingram.rkomi.ru/uploads/documents/lichnaya\_finansovaya\_bezopasn
	ost\_pdf\_2019-06-09\_08-29-38.pdf (дата обращения: 29.12.2023).

ПРИЛОЖЕНИЕ

**Вопросы**

***1. С какими видами мошенничества вы сталкивались?***

а) Мошенничество с использованием банковских карт

б) Интернет-мошенничества

в) Мобильные мошенничества

г) Финансовые пирамиды

***2. Сталкивались ли вы со списанием средств с банковской карты?***

а) Да

б) Нет

***3. Страховали ли вы в банке свою банковскую карту?***

а) Да

б) Нет