**Федеральное государственное автономное образовательное**

**учреждение высшего образования   
“Национальный исследовательский университет   
“Высшая школа экономики”**

Факультет экономики, менеджмента и бизнес-информатики

Кафедра физического воспитания

Дисциплина «Безопасность жизнедеятельности»

**Контрольная работа на тему:**

**Современная социальная среда и проблемы предупреждения и борьбы с мошенничеством**

**Выполнил:** студент Чепоков Е.С.,

уч. гр. ПИ-18-2

**Проверил:** кандидат социологических наук,

доцент кафедры физ.

воспитания

Лобанов Сергей Васильевич

Пермь, 2018

**СОДЕРЖАНИЕ**

1. Введение…………………………………………………………………..с.3
2. Что же такое «мошенничество»?..............................................................с.5
3. Методы, применяемые мошенниками......................................................с.7
4. Общая защита от мошеннических действий..........................................с.12
5. Заключение……………………………………………………………....с.14
6. Библиография……………………………………………………………с.15
7. Приложение………………………………………………………….......с.16

**ВВЕДЕНИЕ**

Жизнь человека, а точнее его здоровье и психическое состояние сильно зависят от огромного количества факторов. Например, от таких как: уровень жизни в стране, материальное и духовное состояние, окружение, защищённость от угроз для жизни. Совокупностью всех этих условий и является социальная среда.

Вне зависимости от развития человечества, всегда оставались факторы, которые могли навредить жизни человека. Современный человек, как и человек, живший много тысяч лет назад, вынужден остерегаться огромного количества опасностей.

Опасности делят на:

* Естественные (климатические и природные явления, возникающие при изменении погодных условий, например: наводнения, землетрясения, ураганы и пр.)
* Техногенные (создаются элементами техно сферы – машинами, сооружениями и тп.)
* Антропогенные (возникают в результате ошибочных или несанкционированных действий человека или групп людей)
* Социальные (опасности, распространённые в обществе и угрожающие жизни и здоровью людей, сюда входит и мошенничество)

Таким образом на жизнь и развитие человека, как личности влияет не только общество, но и природа создающие неблагоприятные условия социальной среды.

Среди социальных опасностей выделяется группа, связанная с психическим воздействием на человека. К ней относятся: интернет, СМИ, пропаганда сцен насилия, шантаж, воровство и мошенничество, именно о нем и будет идти речь далее в тексте.

Мошенничество занимает 10,7% в рейтинге по количеству преступлений в год, что ровняется 142709 зарегистрированных преступлений и 40908 раскрытых (примерно 4000 случаев в Пермском крае за январь-август 2018 года).

За последние 20 лет, в связи с появлением банковских карт и удалённых способов оплаты, количество преступлений по ст. 159 УК РФ – мошенничество, увеличилось в 9 раз. Из-за этого следует предупреждать общество о возможных путях мошенничества и борьбы с ним.

Целью данной работы является: исследование мошенничества как условия социальной среды и создание сборника методических рекомендаций по защите от угрозы мошенничества.

Задачи, выполнение которых необходимо для достижения цели этой работы:

* Исследовать понятие «мошенничество»;
* Выделить виды мошенничества, которые могут встретиться студентам НИУ ВШЭ Пермь;
* Классифицировать виды и приемы, применяемые мошенниками;
* Разработать технологию защиты против мошенников;
* Скомпоновать полученные данные в сборник методических указаний.

Методы исследования, использованные в данной работе:

1. Изучение соответствующей литературы по заданной теме;
2. Опрос среди жителей Перми и студентов НИУ ВШЭ - Пермь;
3. Изучение статистических данных, связанных с мошенничеством в России и Пермском крае;

**2. Что же такое «мошенничество»?**

Мошенничество – хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием, наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, исправительными работами на срок до одного года, ограничением свободы на срок до двух лет, принудительными работами на срок до двух лет, арестом на срок до четырех месяцев, лишением свободы на срок до двух лет. (в ред. Федерального закона от 07.12.2011 N 420-ФЗ). Лица, занимающиеся мошенничеством, называют мошенниками.

Целью любых мошеннических действий является создание иллюзии законности перехода имущества от владельца к мошеннику.





*Историческая справка.*

Изначально слово «мошенничество» (по Соборному уложению) означало «обманное, ловкое хищение чужого имущества». Первое законодательное определение мошенничества, близкое к современному, было дано в Указе Екатерины II от 3 апреля 1781 года «О разных видах воровства и какие за них наказания чинит»: «*Будь кто на торгу… из кармана что вынет… или внезапно что отымет, или обманом или вымыслом продаст, или весом обвесит, или мерою обмерит, или что подобное обманом или вымыслом себе ему не принадлежащее, без воли и согласия того, чьё оно*».

Форма мошеннических обманов очень разнообразна. Обман может совершаться в виде устного или письменного сообщения, либо заключаться в совершении каких-либо действий.

Мошенники – своего рода [элита](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B8%D1%82%D0%B0) преступного мира. Это обычно люди, обладающие высоким интеллектом и определенными познаниями в психологии. Они обладают умением вступать в контакт, располагать к себе. Они также часто являются специалистами в экономике, информационных технологиях и тому подобное, для более углубленного взаимодействия с окружением.

Поэтому, не стоит забывать, что мошенники зачастую умные люди, что играет им на руку, не стоит медлить и давать им себя обмануть.

Образ мошенника и их уловки «наяву», можно увидеть с помощью литературы или художественных фильмов.

Например, герой романа «Двенадцать стульев», Остап Бендер является образом мошенника СССР 20 века. Но для полного представления лучше, посмотреть художественный фильм «Поймай меня если сможешь», где представлен один из самых известных мошенников Фрэнк Уильям Абигейл-младший. Который на столько мастерски владел своим делом, что не только смог скрываться от преследования 9 лет, но и после поимки его приняли к сотрудничеству в Академии ФБР, где уже он выявлял подделки.

На основе вышесказанного можно сделать некоторые выводы:

1. Мошенник зачастую это умный человек;
2. Они являются никой «элитой» среди преступников;
3. Мошенники умеют общаться с «жертвой» и поэтому невозможно сразу распознать их замысел;
4. Образ мошенника описан в литературе и в художественных фильмах;

**3. Методы, применяемые мошенниками**

Методы, применяемые этими незаурядными представителями криминального общества разнообразны и порой поражают своей гениальностью и изощрённостью. Мошенники часто используют следующие психологические приёмы:

* предлагают совершить какую-либо сделку на условиях, которые значительно выгоднее обычных;
* заставляют жертву совершать какие-либо действия в спешке, мотивируя это различным образом;
* выдают себя за очень богатых, влиятельных и преуспевающих людей.

Видов мошенничества огромное множество, поэтому в рамках данной работы были выделены лишь наиболее значимые разновидности, наиболее часто встречающиеся в современном мире и актуальные для студентов НИУ ВШЭ Пермь.

**Мошенничество посредством**[**мобильной связи**](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B1%D0%B8%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%80%D0%B0%D0%B4%D0%B8%D0%BE%D1%81%D0%B2%D1%8F%D0%B7%D1%8C)

* Мошенничество с подпиской на услугу (см. Приложение рис.1)

Вид мошенничества заключается в том, что пользователя обманным путём убеждают перейти по ссылке, служащей для подписки на платные услуги. Для реализации схемы мошенникам нужен номер мобильного телефона пользователя. Часто подобные ссылки рассылаются в SMS под видом ссылок на поздравительные открытки или важные сообщения.

* Фрод

вид [мошенничества](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%BE) в области информационных технологий, в частности, несанкционированные действия и неправомочное пользование ресурсами и услугами в сетях связи. Фрод используется для воровства средств с мобильных телефонов.

* Вишинг

Один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определенных действий со своим карточным счетом. (Пример: звонит якобы оператор сбербанка и просит предоставить данные карты)

* Как бороться со злоумышленниками?

НИКОГДА не открывайте SMS от подозрительных номеров, а лучше сразу удаляйте эти сообщения. Так же не переходите по ссылкам рекламы на неизвестных сайтах и тем более ничего не скачивайте, помните, что 80% этой рекламы является платной подпиской или фродом.

Если на Ваш телефон пришло сообщение о том, что Ваша банковская карта заблокирована и для разблокировки надо отправить SMS на короткий номер – не делайте этого, а лучше обратитесь в ближайший банк.

Не стоит доверять сообщениям об различных выигрышах в конкурсе и просьбах оплатить доставку приза – организатор всегда берёт на себя все расходы при доставке.

**Мошенничество в**[**Интернете**](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82)

* Мошенничество с надомной работой

Мошенник предлагает возможность работать, не выходя из дома, делая лёгкую работу, и получать максимум денег за минимум потраченного времени. Цель преступника – вымогательство денег за обучение или продукты по завышенной цене.

* Фишинг и фарминг (см. Приложение рис.2)

Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с переходом на другой сайт. После того, как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

* Кликфрод

Обманный маневр в сфере поисковой рекламы, когда оплата зависит от количества кликов по ссылкам. При таком виде мошенничества на сайт переходят посторонние люди, например, вебмастер или конкуренты рекламодателя, чтобы получить прибыль от проставленных ссылок или заставить рекламодателя влезть в долги.

Так же может осуществляться с помощью автоматизированных скриптов или программ, имитирующих клик пользователя по рекламным объявлениям.

* Мошенничество с помощью служб знакомств

Ряд различных мошеннических действий, использующих сайты знакомств просто как площадку для поиска жертв. Представившись ищущему романтических отношений человеку потенциальным партнёром, злоумышленник сначала входит к нему в доверие, а затем под вымышленными предлогами просит его добровольно посылать деньги, номера банковских счетов, кредитных карт

* Мошенничество с обещанием лёгкого заработка в Интернете (бинарные опционы, Интернет-казино, пирамиды, лже-коучинг).
* Как бороться со злоумышленниками?

Обращайте внимание на URL-адрес сайта, на котором вы находитесь, если он запрашивает ввод каких-то данных. Его можно увидеть сверху в отдельной строке браузера. Название сайта не должно быть искажено. Так же, как и в SMS, не стоит доверять сообщениям об различных выигрышах в конкурсе и просьбах оплатить доставку приза – организатор всегда берёт на себя все расходы при доставке.

Так же, нужно помнить, что легких денег не бывает, а на неизвестных сайтах тем более.

При скачивании на непроверенных сайтах пользуйтесь правилом – чем больше и ярче кнопка, тем меньше вероятность того, что именно она приведёт к запуску процесса скачивания нужного вам ПО.

Будьте осторожнее со знакомствами в соцсетях и службах знакомств. Если вы заметили, что ваш собеседник часто просит о материальной помощи, то стоит прекратить общение.

**Мошенничество с**[**банковскими картами**](https://ru.wikipedia.org/wiki/%D0%9F%D0%BB%D0%B0%D1%81%D1%82%D0%B8%D0%BA%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BA%D0%B0%D1%80%D1%82%D0%B0)

* Кардинг

Вид мошенничества, при котором производится операция с использованием платежной карты или её реквизитов, не инициированная или не подтвержденная её держателем. Частным случаем является скимминг (см. Приложение рис. 3) – снятие данных магнитной ленты на банковской карте с помощью специального устройства – скиммера.

* Считывание NFC чипов (см. Приложение рис. 4)

Вид мошенничества появившийся не так давно, мошенники ходят по общественным местам с аппаратом для оплаты, с заранее вбитой суммой денег, и прикладывают к карманам людей. После прикладывания у жертвы списываются деньги с карты, а мошенник ищет новую жертву.

* Как бороться со злоумышленниками?

Будьте внимательными при использовании банкомата. Перед проведением необходимых операций проверьте его на наличие скиммера. Лучше использовать проверенный банкомат недалеко от дома, чтобы наверняка знать были ли изменения.

Подключите услугу SMS оповещения, чтобы всегда знать о взаимодействиях со счётом.

Не носите карту в боковых карманах, а лучше уберите в кошелёк и в сумку.

Перейти с банковской карты на оплату телефоном.

Таким образом, можно сделать следующие выводы:

Зная основные методы и принципы работы мошеннических схем, несложно подобрать меры по борьбе с ними;

Всегда нужно быть начеку и не открывать то, что выглядит подозрительно.

**4. Общая защита от мошеннических действий**

Мной был проведён опрос среди 40 учащихся ВУЗа НИУ ВШЭ – Пермь и 28 жителей города Перми. Опрос был проведён в целях сбора данных о том насколько люди проинформированы об опасности мошенничества и узнать, нужен ли сборник методических указаний.

1. Становились ли Вы жертвой мошенничества? (да/нет)
2. Какие виды мошенничества вы знаете? (выбрать из предложенных)
3. Нужен ли сборник методических указаний по предупреждению и борьбе с мошенничеством? (нужен/не нужен)

Опрос прошли 68 участников:

* 42 (62%) участника ответили, что были жертвами мошенничества (см. Диаграмма 1 в приложении);
* 40 студентов выбрали ответ с пирамидами, в опросе можно было выбирать несколько вариантов, поэтому процентное соотношение трудно представить (см. Диаграмма 2 в приложении);
* 42 (62%) участника ответили, что сборник с указаниями не нужен. (см. Диаграмма 3 в приложении).

По результатам опроса видно, что большинство участников знают об опасности мошенничества и знают, как ей противостоять. Участники ответили, что сборник не нужен ссылаясь на наличие интернета.

Общие правила защиты от мошенничества:

1. Не совершайте поспешных действий;
2. Не доверяйте всему и всем;
3. Не переходите по подозрительным ссылкам, сообщениям или контактам;
4. Будьте всегда начеку и не теряйте бдительность при совершении каких-либо денежных операций.
5. При скачивании чего-либо из интернета проверяйте на наличие вирусов и сторонних ПО;
6. При покупке чего-либо из интернета удостоверьтесь в честности продавца, почитайте отзывы о нём.

**ЗАКЛЮЧЕНИЕ**

Цель и задачи, поставленные в контрольной работе, выполнены. Исследовано понятие «мошенничество» как условия социальной среды, создан сборник методических рекомендаций по защите от угрозы мошенничества – глава 4, выделены и описаны виды мошенничества, которые могут встретиться студентам НИУ ВШЭ – Пермь и к каждой разобраны и написаны технологии борьбы.

Мошенники всегда были и будут самыми гениальными преступниками и в будущем явно появятся новые способы мошенничества, для которых тоже нужно будет искать методы борьбы.

При создании сборника методических указаний все виды мошенничества были поделены на группы для большего удобства и лучшей наглядности и так же приведены примеры борьбы с ними.

В сборник методических указаний не попали:

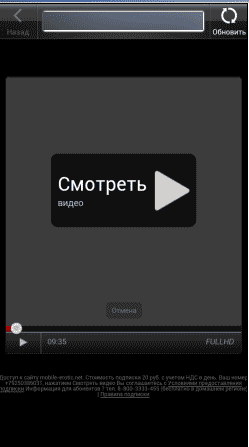
1. Мошенничество с куплей/продажей имущества (ввиду не актуальности для студентов);
2. Перехват трафика данных (специализированный тип);
3. Гадания, экстрасенсы, игра в напёрстки (ввиду не актуальности для студентов);
4. Автоподставы;
5. Обвес, обсчёт и проч. (ввиду исчезновения данного вида мошенничества в нынешних магазинах);
6. Мошенничество с материнским капиталом (ввиду не актуальности для студентов);
7. Мошенничество с «куклой» - обычная бумага посередине крупной пачки денег;
8. «Высотка на шести сотках» - строительство многоквартирных домов на участках, выделенных под садоводство (ввиду не актуальности для студентов)

**6. Библиография**

1. Уголовный кодекс Российской Федерации. Официальный текст: текст Кодекса приводится по состоянию на 1 августа 2018 г.— М.: Эксмо, 2017.
2. Абрамов В.В. Безопасность жизнедеятельности: учебное пособие для вузов/ В.В. Абрамов – 2-е изд. перераб. и доп. - М.: 2013. - 365 с.
3. Волженкин Б.В. «Мошенничество». — СПб., 1998. — (серия «Современные стандарты в уголовном праве и уголовном процессе»).
4. Кочои С. М. «Ответственность за корыстные преступления против собственности.»- 2-е изд., доп. и перераб. - М.: АНТЭЯ 2000; Профобразование, 2000. - 288 с.
5. Сунчалиева Л. Э. «Мошенничество (уголовно-правовой и криминологический аспект).» Дисс. канд. юрид. наук. — Ставрополь, 2004.
6. Интернет-мошенничество: памятка для граждан [Электронный ресурс]. – Режим доступа: <https://мвд.рф/>;
7. Yudhijit Bhattacharjee. http://content.time.com/time/magazine/article/0,9171,2041113,00.html, TIME (Jan. 17, 2011)
8. Рождественский И. В России на четверть увеличилось число дел по статье «Мошенничество» [Электронный ресурс] / И. Рожденственский// РБК: медиахолдинг – 14.07.2016.— № 1. –.
9. Фадеев, П. Пермь криминальная — 2016 [Электронный ресурс] / П. Фадеев// Новый компаньон: полит. газета. – 2016. — № 1.
10. https://properm.ru/news/finmoshenniki/ «Мошенничество в Перми» [Электронный ресурс]
11. Куликов Н.И. , Сизов А.А. Анализ схем правонарушений в области использования пластиковых карт // Научный журнал НИУ ИТМО. Серия "Экономика и экологический менеджмент". — 2015.

**7. Приложение**

Рис. 1



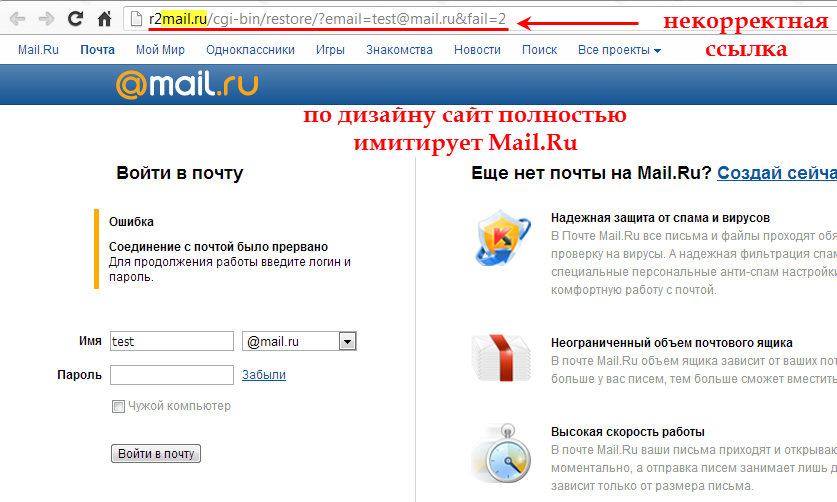
Рис. 2

Рис. 3

Рис. 4

Диаграмма 1

Диаграмма 2

Диаграмма 3