

Министерство здравоохранения Ростовской области
государственное бюджетное профессиональное образовательное учреждение
Ростовской области
«Таганрогский медицинский колледж»

Ветрова Е.Н.

**«Как не стать жертвой.
Мошенничество с банковскими картами»**

Методическая разработка
воспитательного мероприятия
для студентов 1-4 курсов
специальности:
34.02.01 Сестринское дело

2025 г.

СОДЕРЖАНИЕ

стр.:

Пояснительная записка	3
Введение	4
Сценарий	7
Список использованных интернет- ресурсов:	13
Приложение	14

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

В методической разработке раскрывается методика проведения информационной беседы на тему: **«Как не стать жертвой. Мошенничество с банковскими картами».**

Предназначена для кураторов, использующих активные инновационные формы проведения внеаудиторных мероприятий с использованием информационно-коммуникативных технологий.

Информационная беседа рассматривает виды, способы мошенничества с банковскими картами, а также меры, которые может предпринять человек, чтобы не стать жертвой мошенничества.

Куратор имеет возможность донести информацию и провести дискуссию о том, что на сегодняшний день существуют десятки способов обмана людей и кражи денег с банковских карт, начиная от банального подглядывания из-за плеча во время использования клиентом банкомата и последующим хищением его карты, заканчивая хакерскими атаками на программное обеспечение пользователя. При этом злоумышленники постоянно придумывают новые способы хищения денежных средств.

Акцент при проведении беседы необходимо сделать на актуальность данной темы и формирования постоянного самоконтроля студентов в их дальнейшей самостоятельной деятельности.

ВВЕДЕНИЕ

*Нажить много денег - храбрость;
сохранить их - мудрость,
умело расходовать – искусство»
Бертольд Авербах*

Актуальность данной темы обусловлена самой жизнью. Большое количество людей ежедневно становятся жертвами мошенников.

Цель: формирование у студентов сознательного, ответственного отношения к вопросам личной безопасности при использовании банковской карты.

Задачи:

- 1) обучать студентов находить выход из экстремальных ситуаций, предвидеть их и по возможности избегать;
- 2) сформировать у студентов понятие о разновидностях банковских карт;
- 3) рассмотреть некоторые виды мошенничества;
- 4) изучить способы защиты денежных средств на банковской карте от мошенников.
- 5) развивать умение видеть опасности и суметь быстро отреагировать на них; воспитывать самоконтроль, самообладание в трудных жизненных ситуациях.

Проблемный вопрос:

Какие правила необходимо соблюдать, чтобы не попасться на уловки мошенников с банковскими картами?

Участники (выбрать ведущих 1,2):

1.студенты группы 4-2: (23 чел.)

2. куратор группы: Ветрова Е.Н.

Контингент: студенты 1-4 курсов

Специальность: 34.02.01 Сестринское дело

Форма проведения: информационная беседа с элементами обсуждения

Место проведения: аудитория № 205

Дата проведения:

20 г.

Продолжительность:

30 мин.

Оборудование: ноутбук, экран, проектор

Оформление: презентация

Раздаточный материал: памятка

Подготовительная работа

1. Куратор предлагает студентам тему мероприятия и форму его проведения.
2. Формирует рабочую группу из актива самоуправления.
3. Раздаёт задания:

- подобрать иллюстрации;
- оформить, презентацию,
- провести поиск информации о мошенничестве;
- подготовить предложения для сценария, используя различные источники;
- изготовить памятку.

4. Формирует микрогруппы и назначает ответственных.

5. Проводит групповой анализ поставленных задач и целей.

Оформление:

- предварительное объявление (в группе кураторов);
- презентация;
- памятки.

Ход мероприятия:

1. Вступление.
2. Основное содержание
3. Обсуждение вопросов, относящихся к теме:

- Понятие банковская карта
- История возникновения
- Виды банковских карт
- Виды мошенничества
- Как защитить карту от мошенников
- Куда обратиться, если похитили деньги с карты

3. Подведение итогов
4. Рефлексия
5. Планируемые результаты:

Предметные:

- сформулировать понятие мошенничество;
- научиться извлекать нужную информацию, проводить обобщение и на основе этого делать соответствующие выводы.

Межпредметные:

- научиться планировать свои действия в соответствии с поставленной задачей;
- научиться учитывать разные интересы, мнения и обосновывать свою позицию.

Личностные:

- осознающий себя гражданином и защитником великой страны;
- проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном

самоуправлении, в том числе на условиях добровольчества. Продуктивно взаимодействующий и участвующий в деятельности общественных организаций;

- осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельность.

СЦЕНАРИЙ

На экране тема информационной беседы:

«Как не стать жертвой. Мошенничество с банковскими картами»

(слайд 1)

Вступление

Куратор:

Здравствуйте!

Тема нашей информационной беседы:

«Как не стать жертвой. Мошенничество с банковскими картами»
(слайд 2 фото с названием темы, целей, задач, актуальности
мероприятия)

Куратор:

Горе приходит к людям внезапно. Попасться на уловки ушлых преступников можно кому угодно, где угодно и когда угодно. Это может произойти, когда вы снимаете деньги в банкомате либо расплачиваешься пластиковыми картами при покупке различных товаров. К вам могут подойти на улице и попросите телефон, чтобы совершить срочный звонок, так как недостаточно средств на счёте. И, наконец, жертвой преступников вы можете стать в собственной квартире. В ситуации, когда вопрос жизни и смерти решают в буквальном смысле секунды, минуты, мы должны уметь помочь себе сами.

Сегодня мы поговорим с вами о том, кто такие мошенники и как уберечь себя от их воздействия **(слайд 3)**

Ведущий №1:

Слово «мошенник» является производным от существительного «мошна», означающего «сума, кошелек» **(слайд 4)**

По происхождению слово «мошенник» славянское и используется в русском языке с XVI в., мошенником называют «жулика», «нечестного человека». **Мошенник** – это тот, кто обманывает других в корыстных целях. Обычно это довольно образованный человек, который, будучи отличным психологом, является знатоком человеческой натуры и способов отъёма денежных накоплений **(слайд 5)**

Как правило обман строится на выстраивании доверительных отношений, умении убедить, и на жадности граждан, которые часто забывают, что «бесплатный сыр бывает только в мышеловке». Мошенники были, есть и будут во все времена, от этого не уйти. **(слайд 6)**

Куратор задаёт вопрос студентам:

Сталкивался ли кто-нибудь из присутствующих (или их родные/знакомые) с мошенниками?

Студенты делятся информацией (слайд 7)

2. Основное содержание

Ведущий 2: Банковские карточки стали привычным способом хранения денег. Казалось бы, финансы надежно защищены, ведь карта всегда под рукой, а получить наличность или рассчитаться в магазине можно, только зная пин-код. Вначале давайте разберёмся, что же это такое банковская карта (слайд 8).

Ведущий 1: Это пластиковая карта, используется для оплаты товаров и услуг, в том числе через интернет, а также снятия наличных банков и в банкоматах, и полностью замещает использование бумажных денежных знаков.

Первая банковская карта была создана в США во времена «торгового бума» (1940—1950-е годы). В большинстве своём она заменила чековые книжки. В процессе своего развития происходила техническая модернизация карт. (слайд 9)

Ведущий 2: Сначала это был просто кусочек картона, затем на карте появилось эмбоссирование номера - процесс механического выдавливание на лицевой стороне имени владельца и она стала работать по принципу перфокарты, в начале 1970-х была разработана магнитная полоса, а в конце 1990-х в кредитные карты стали интегрироваться чипы (слайд 10)

Ведущий 1: Первой платежной картой, пришедшей в Россию (тогда еще в Советский Союз) следует считать карту международной платежной системы Diners Club. Именно эти карты начали приниматься в системе магазинов «Березка» в 1969 г. И лишь после начала развития в России системы коммерческих банков (точкой отсчета этого можно считать принятие в 1990 г. Закона «О банках и банковской деятельности») у банковских пластиковых карт как платежного инструмента, ориентированного на держателей — частных лиц, появилось в России большое будущее. (слайд 11)

Куратор задаёт вопросы студентам:

Ребята, какие виды карт вы знаете? (слайд 12)

Существуют два вида карт дебетовые и кредитовые

Дебетовые карты используются для распоряжения собственными деньгами, находящимися на расчетном счете в банке. (слайд 13)

Они имеют дополнительные возможности такие как: Бонусные баллы, Мобильный банк, Онлайн банк (слайды 14,15)

Кредитная карта предназначенная для совершения операций, расчёты по которым осуществляются исключительно за счёт денежных средств, предоставленных банком клиенту в пределах установленного лимита в соответствии с условиями кредитного договора. (слайд 16)

Мошенничество – хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием.

Мошенничество с банковскими картами набирает обороты, поскольку мошенники каждый раз придумывают новые схемы и махинации, целью которых является снятие денег с карточного счета. Для того чтобы не стать жертвой воров и защитить собственные сбережения, нужно знать всевозможные методы кражи данных и варианты защиты от них (слайд 17)

Куратор задаёт вопрос: Ребята, о чём предостерегают СМИ? Расскажите (слайд 18)

Рассмотрим основные виды мошенничества с банковскими картами.

Ведущий 1: Через мобильный банк (слайд19)

создатели программы специально заражают ее вирусом, который начинает работать на мошенников.

Суть: Он заменяет окно мобильного банка поддельным. Владелец телефона вводит туда свои данные. Вирус отправляет их аферистам, которые затем незаконно получают доступ к карточному счету клиента.

Программа может получать доступ к смс- оповещениям клиента при работе в программе. С их помощью воры под видом владельца дебетовой карты они могут входить в банки и совершать кражу денег. Вирусы блокируют сообщения о снятии наличных и переводе денег, которые должны поступать на телефон.

Меры борьбы: (слайд 20)

1.необходимо устанавливать лишь лицензионные программы (в том числе и антивирусные)

2.регулярно проверять счёт

Ведущий 2: По телефону (слайд 21)

При краже/утере телефона или сим-карты, преступники получают доступ в интернет-банк и спокойно переводят все деньги с кредитки (Если к телефонному номеру была привязана банковская карточка).

Злоумышленники могут взломать сайт мобильного оператора. После этого они устанавливают переадресацию всех смс- сообщений пользователя и используют их для доступа к мобильному или интернет банку (социальным сетям)

Меры борьбы:

1.блокировать карту

Ведущий 1: СМС мошенничество (слайд 22)

Суть: Владельцу карты приходит сообщение на сотовый, что карта заблокирована. Для ее разблокировки предлагается сделать обратный звонок оператору финансового учреждения по указанному в смс номеру. При телефонном звонке мошенник представляется сотрудником банка и просит дать секретную информацию: номер с пластика, кодовое слово и цифры пин-кода, якобы необходимых для разблокировки.

Меры борьбы:

1. позвонить в банк по номеру, указанному на обратной стороне карты и узнать всю нужную информацию
2. сотрудники банка не обзванивают владельцев карт по поводу их блокировки

Ведущий 2: Через интернет (слайд 23)

Покупка товаров через интернет очень популярна, поскольку помогает существенно сэкономить .

Куратор задаёт вопрос:

Ребята, вы осуществляли покупки товаров через интернет с использованием банковской карты? (слайд 24)

Ведущий 2:

Суть: Мошенники могут перехватывать данные прямо во время проведения оплаты, а потом применять реквизиты банковской карточки для дальнейшего вывода денег.

Меры борьбы: (слайд 25)

1. не делать покупки на большие суммы через всемирную паутину;
2. использовать для оплаты виртуальную карту;
3. установить лимит по разовой оплате;
4. использовать для совершения покупок только проверенные сайты;
5. подключить услугу Secure Code.

Ведущий 1: Кража пластиковой карты (слайд 26)

Если такое обнаружено, необходимо срочно связаться с оператором и заблокировать карту или сделать это самостоятельно через мобильное или интернет- приложение.

Снять деньги без пин-кода с него не представляется возможным, однако расплачиваться в магазине не составит труда.

Карточками с чипом или с бесконтактной оплатой воспользоваться сложнее, потому что для любых операций понадобиться ввести номер секретного пароля.

Ведущий 2; С помощью поддельных банкоматов (слайд 27)

Суть: Вставив карту в устройство, человек видит информацию об отсутствии наличности либо неисправности системы. Мошенники завладевают всей необходимой им информацией для вывода денег. Фальшивый банкомат может возвратить карточку, а может оставить ее у себя. В этом случае снять деньги будет еще проще, ведь есть оригинал и известен пин-код.

Ведущий 1: При платежах по терминалу (слайд 28)

Суть: При покупках в магазине стоит внимательно следить за кассирами, которые берут пластик в свои руки для оплаты по терминалу. Если сотрудник магазина проводит банковской карточкой два раза по терминалу, то в первый раз он делает это, чтобы списать деньги, а второй – для снятия информации с пластика, чтобы потом увести деньги. Кроме этого, он может запомнить cvv код и данных на лицевой стороне, при помощи которых легко проводить покупки в интернете

Ведущий 2: Бесконтактные считающие устройства с технологией Paypass (слайд 29)

Суть: Использование платежной карточки с технологией бесконтактной оплаты PayPass разрешает производить оплату на сумму не более 1000 рублей без ввода пин-кода. Для осуществления операции нужно лишь приложить переносной терминал к сумке или одежде, где находится карта. Осуществляется в местах с большим скоплением народа

Ведущий 1: Получение личных данных с карты (слайд 30)

Суть: установка специального устройства скиммера на место карто приемника банкомата. Клиент банка вставляет банковскую карту , а злоумышленники копируют всю нужную информацию с магнитной полосы карты для изготовления дубликата. Пин-код добывается двумя способами – при помощи установки специальной накладки на клавиатуру банкомата или путем монтажа миниатюрной видеокамеры.

Ведущий 2: Меры борьбы: (слайд 31)

1. не снимать деньги в банкоматах, расположенных в отдаленных и слабоосвещенных местах;
2. Перед тем как вставлять пластик в банкомат, нужно убедиться, что на поверхности отсутствуют подозрительные накладки – как правило, они отличаются цветом и видом.
3. торговых точках желательно оплачивать картой самостоятельно.

Куратор задаёт вопрос:

Ребята, как всё-таки защитить банковскую карту от мошенников ваше мнение?

(слайд 32) Обсуждение.

Ведущий 1: Итак давайте подведём итог (слайд 33)

1. перед тем как вставлять банковскую карту в банкомат, нужно убедиться, что на поверхности отсутствуют подозрительные накладки (они отличаются цветом и видом).
2. с бесконтактным способом оплаты рекомендуется установить минимальный кредитный лимит при оплате без пин-кода или вовсе его отменить.
3. поместите карту в радиэкранированный кошелек (для этого нужно лишь положить внутрь его фольгу), металлическую коробочку или фольгированный пакет.

4. нельзя отдавать свою кредитку в руки третьим лицам, а тем более сообщать пин-код, ведь это секретная информация, которая доступна только владельцу карты, даже сотрудникам банка она неизвестна, потому что формируется автоматически.
5. не стоит производить оплату в ответ на смс - сообщение и электронные письма, пришедшие из неизвестных источников.
6. в случае несанкционированного списания средств с баланса, нужно звонить в банк и осуществлять блокировку.

Ведущий 2: Куда обращаться, если похитили деньги с карты (слайд 34)

- 1.если списаны деньги без ведома владельца, это позвонить в банковское учреждение по номеру, указанному на обратной стороне пластика
- 2.прийти в ближайшее отделение полиции и написать заявление. Можно ли вернуть деньги
- 3.написать заявление в банк на возврат денег.

- 4.если банк отказывает, можно смело обращаться в суд.

Ведущий 1: Вернуть исчезнувшие средства крайне сложно, особенно если для проведения транзакций необходим ввод пин-кода, но такие случаи известны. Проще возвратить деньги, если зафиксирована хакерская атака на банк или пострадало большое количество граждан

Правовая ответственность за мошенничество (слайд 35)

Уголовный кодекс (статья 159) признает мошенничество с банковскими картами преступлением, за которое виновные несут ответственность в соответствие с законодательством.

Ведущий 2: Виды наказания: (слайд 36)

штраф, арест, исправительные работы или ограничение свободы. Штраф в размере *до 1.000.000 рублей или до 100% от заработной платы (иного дохода)* преступника за период до 10 лет; Обязательные работы *до 480 часов, исправительные работы на срок до 2 лет*, арест до 4 месяцев или же лишение свободы сроком до 10 лет .

Куратор: Рефлексия (слайд 37)

Давайте закрепим наши знания. Чтобы не попасться на удочку мошенников, надо выполнять простые правила, которые, помогут нам защитить денежные средства на наших банковских картах (раздаются памятки)

Обсуждение общих советов, по защите от мошенников

Куратор предлагает студентам поднять стикеры (в зависимости от достигнутой цели занятия) соответствующего цвета:

зеленый стикер - знаю общие сведения о мошенничестве;

желтый стикер - в основном уверен в том, что меня не обманут мошенники;

*красный стикер - уверен в своих знаниях и в себе, меня не обмануть
Ребята, вам понравилась информационная беседа? (слайд 38)*

Но самое главное, помните, что честных и хороших людей на свете

всё-таки гораздо больше!

СПАСИБО ЗА ВНИМАНИЕ! (слайд 39)

СПИСОК ИСПОЛЬЗОВАННЫХ ИНТЕРНЕТ-РЕСУРСОВ:

1. Если вы не хотите стать жертвой мошенников / Советы гражданам [Электронный ресурс]. – Режим доступа: <http://uvd-uzao.ru/page75.htm>
2. Как не стать жертвой мошенников [Электронный ресурс]. – Режим доступа: <https://ratk61.ru/wp-content/uploads/Kolesnikova-MR-Kak-ne-stat-zhertvoj-moshennikov.pdf?ysclid=m5nn12hfbf907737237>
3. Статистика мошенничества [Электронный ресурс]. – Режим доступа: <http://www.ubep44.ru/index.php?page=statistika-moshennichestva>

ПАМЯТКА

БУДЬТЕ БДИТЕЛЬНЫ!

Действительно, сегодня мы всё меньше используем наличные деньги, потому как рассчитываться при помощи пластиковых карт очень удобно и они очень просты в обращении (не надо носить с собой деньги, мелочь). Наибольшее распространение махинации с пластиковыми картами получили в последние годы.

Вот их основные виды:

- 1 Использование потерянных либо украденных карт, когда банк вовремя не блокирует счёт пропавшей карточки, и мошенник его обнуляет.
- 2 Подделка карт, когда полученная незаконным путём информация о чужой карте передается на пластик (белый пластик) или записывается на магнитную полосу подделки или подлинной карты.
- 3 Заказ по почте, телефону, интернету различных товаров и услуг с использованием данных платёжной карточки человеком, не являющимся владельцем этой карты.
- 4 Интернет-мошенничество – использование реквизитов карты, полученных незаконным путём, для транзакций в виртуальной среде.

Номер карты мошенники получают различными путями, включая кражу из компьютерной системы торговой точки в сети Интернет, не имеющей необходимых средств безопасности для предотвращения несанкционированного доступа. Необходимо отметить, что самое трудное для мошенников – получить пин-код карточки.

И поэтому способы обезопасить свои сбережения, очень просты.

Не стесняйтесь закрывать от посторонних клавиатуру банкомата, особо любопытных попросите отойти; лучше всего одной рукой закройте сверху клавиатуру (так как мошенники могут установить микрокамеру на банкомате), а другой введите пин-код.

Снимать деньги лучше стараться в банкоматах, которые расположены либо в офисах Банка, либо рядом с офисами банков (эта территория

просматривается видеокамерами служб безопасности банков и мошенники стараются туда не соваться).

В банке, который выдал вам карту, подключить услугу «смс - информирование». По любой операции по вашей карте из банка будет приходит смс- сообщение на ваш мобильный телефон, это позволит вам контролировать операции в онлайне. Такую услугу предоставляют, все крупные банки.

Будьте внимательны и осторожны!