Прокуратура Новосибирского района НОВОСИБИРСКОЙ ОБЛАСТИ

МОШЕННИЧЕСТВО. ИНТЕРНЕТ-МОШЕННИЧЕСТВО

Самые распространенные способы обмана

ВНИМАНИЕ, МОШЕННИКИ!

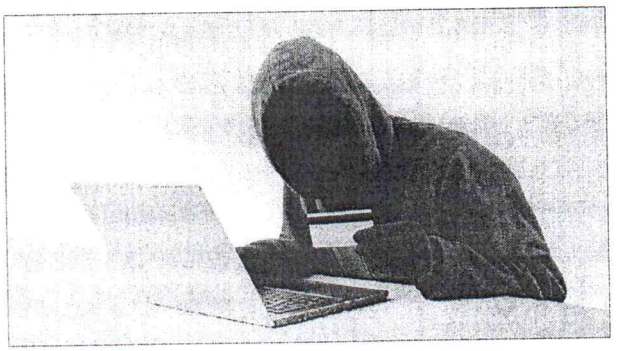
ПРОФИЛАКТИКА ПРАВОНАРУШЕНИЙ

ЧТО ТАКОЕ ИНТЕРНЕТ-МОШЕННИЧЕСТВО

ЧТО ГОВОРИТ ЗАКОН?

Любое мошенничество – это уголовное преступление, отвечать за которое придется по статьям Уголовного Кодекса Российской Федерации.

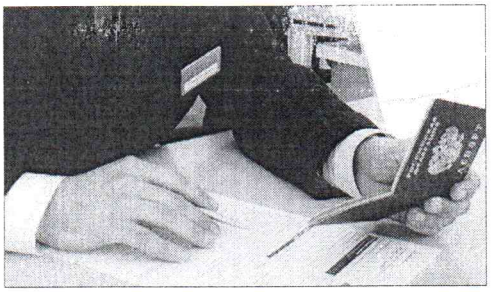
Закон определяет мошенничество, как хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием, дифференцируя некоторые его виды в зависимости от сферы совершения: кредитование, страхование, электронные средства платежа и т. д.



Если вы пользуетесь хотя бы электронной почтой и смартфоном, вы уже в зоне риска.

Мошенничество отличается от кражи тем, что жертву обманывают и она добровольно отдает свое имущество или передает права на него.

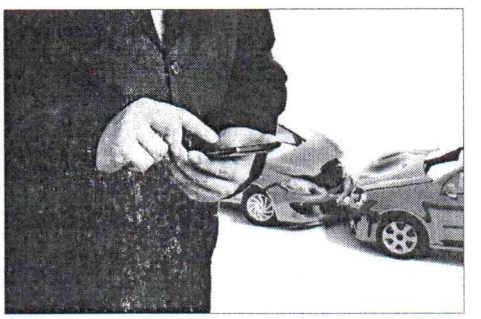
Несмотря на добровольность передачи, отвечать перед законом мошеннику все равно придется. Вот за что предусмотрена уголовная ответственность.



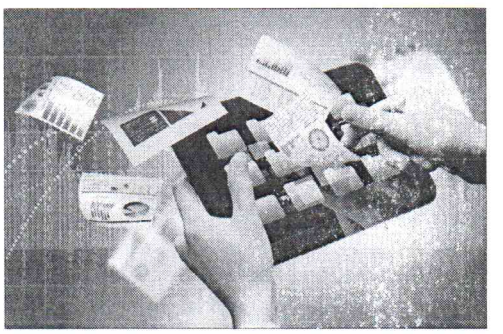
Мошенничество с электронными платежами, когда преступники используют банковские карты, виртуальные кошельки, электронные переводы или криптовалюту для отмывания денег.

Жульничество со страховками, когда врут о наступлении страхового случая или размере ущерба, чтобы получить выплату по страховке.

Примерно 90 % страховых мошенничеств сосредоточено в автостраховании.



Махинации с хранением, обработкой, изменением или передачей данных в электронном виде.



В этом случае обычно крадут или изменяют электронные данные, чтобы получить права на имущество.

МОШЕННИЧЕСТВО ПРИ ПОМОЩИ МЕССЕНДЖЕРОВ ИЛИ СМС

Одной из наиболее известных схем мошенничества является СМС сообщения с просьбой перевести деньги родственнику, якобы оказавшемуся в беде.

Но мошенники все чаще стали прибегать к разводам именно через популярные мессенджеры. Один из самых популярных, в котором промышляют данные элементы, как ни странно, viber.

Текст сообщения подбирается таким образом, чтобы значительная часть получателей могла принять такое сообщение за отправленное кем-либо из близких людей. Большинство граждан уже не верят безликим сообщениям с просьбой перевести деньги, однако, мошенники становятся все более изощренными и заставляют абонентов перечислять им деньги, представляясь, к примеру, сотрудниками сотовой компании и предлагая дополнительные услуги или сообщая о ложной блокировке телефона.

Также получила распространение другая схема, при которой на телефон приходит уведомление о пополнении счёта и счёт действительно пополняется, затем приходит СМС с текстом «Случайно перевёл Вам 100 руб. Можете вернуть?». Как только Вы переводите 100 руб. и «ошибочно переведённые» 100 руб. также исчезают с Вашего счета.

Наиболее известный способ мошенничества, это информирование о блокировке банковской карты, о совершенном переводе средств или другая информация, после прочтения которой гражданин перезванивает на указанный в СМС номер телефона для уточнения информации. Перезвонившему мошенники представляются сотрудниками службы безопасности банка, специалистами службы технической поддержки или контактного центра и в убедительной форме предлагают срочно провести действия по разблокировке карты, по отмене перевода и т. п. в зависимости от содержания

СМС. Для этого предлагается подойти к ближайшему банкомату и еще раз перезвонить на указанный в СМС номер телефона. Далее, слепо следуя получаемым по телефону инструкциям, люди сами переводят средства на электронные кошельки, банковские карты, телефоны мошенников или подключают свои банковские карты к услуге Мобильный банк на телефон, указанный мошенником, что позволяет ему самому перевести деньги с карты.

Чтобы не стать жертвой СМС мошенников необходимо четко знать номера телефонов, с которых могут поступать уведомления, если полученное СМС сообщение вызывает сомнение, необходимо позвонить в Контактный центр банка по официальным телефонам, которые указаны на оборотной стороне карт для уточнения полученной информации.Нужно помнить, что представители банков никогда не звонят клиентам, не запрашивают у клиентов секретные данные, к которым относится срок действия карты и CVV2-код.

Если Вы все таки стали жертвой мошенников необходимо незамедлительно обратиться в Контактный центр банка и заблокировать карту, реквизиты которой были сообщены мошенникам и по которой были совершены мошеннические операции, либо обратится к оператору мобильной связи, в адрес которого переведены средства, с заявлением о мошенничестве и возврате средств, а также подать заявление в любое подразделение полиции о совершенном мошенничестве.

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКА

ЕСТЬ ПРОСТЫЕ ПРАВИЛА.

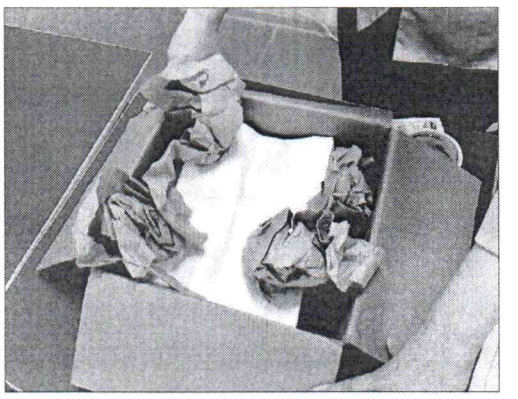
Средняя доходность по рублевым вкладам в России – около 8 %, в долларах и евро – не более 4 %. Если вы получили предложение с доходностью на порядок выше, есть повод задуматься. А если предлагают доходность больше 300 % годовых- очевидно, без печатного станка для денег тут не обойтись. Смело отказывайтесь. Ориентируйтесь на базовый уровень доходности вкладов по данным Центробанка Российской Федерации.

МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ НА ПРОДАЖЕ ТОВАРОВ

«ПРЕДОПЛАТА»

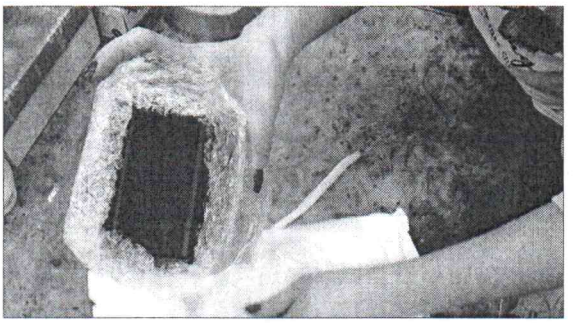
Мошенник сначала взламывает сайт настоящего известного интернет-магазина. Затем выставляет какие-нибудь ходовые товары, установив низкую, привлекательную цену. «Продавец» сразу обговаривает необходимость частичной или 100 % оплаты. Получив деньги, он мгновенно исчезает.

ПОСЫЛКА «КУКЛЫ»



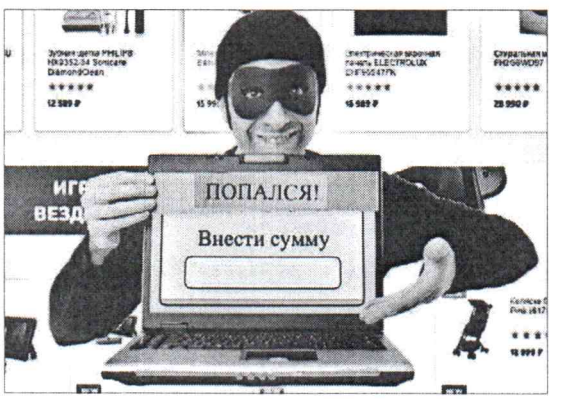
Аферист не только будет выдавать себя за представителя какого-нибудь интернет-магазина, он оформит сделку и даже вышлет посылку. Только вместо товара внутри будет нечто другое похожего веса. Покупка придет, и, осмотрев ее снаружи, покупатель уверится, что все серьезно. Оплатит стоимость и все. Только дома он сможет распознать обман.

БРАК



Некоторые магазины предлагают людям платить позже, когда посылка уже фактически пришла. Однако на почте, как правило, людей много, и необходимого времени на тщательный осмотр нет. Покупатель берет посылку, вскрывает и бегло оглядывает, убеждаясь, что внутри действительно заказанная вещь. Лишь дома он, досконально осмотрев заказ, сможет определить брак или низкое качество (подделка).

ОШИБОЧНАЯ ЦЕНА



Изначально покупатель видел одну цену, а когда посылка уже фактически пришла, ему нужно либо платить больше, либо вернуть посылку. Многие платят, не желая еще 2–3 недели провести, ожидая другой товар.

ФАЛЬШИВЫЕ ХАРАКТЕРИСТИКИ

Иногда продавец, желая приукрасить товар, дополняет его характеристики описанием другой, более качественной продукции. Если покупатель еще не видел вблизи заказываемую вещь или не сравнивал написанное там с данными от других сайтов, продающих такие же предметы, ему будет сложно определять, где реальность.

Осторожнее с предоплатой за товар. Пресс-служба Роскачества рекомендует изучать интернет-профиль продавца перед покупкой товара на онлайн-сервисе.

ПЕРЕД ОФОРМЛЕНИЕМ ЗАКАЗА НЕОБХОДИМО:

– Проявить дополнительную бдительность при взаимодействии с продавцом, который зарегистрировал аккаунт всего несколько дней назад, или, если это его первый товар.

– Обратить внимание на систему рейтингов и отзывов. Чем выше рейтинг – тем меньше шанс обмана, при этом, это все равно не гарантирует положительный результат.

– Покупателю не рекомендуется соглашаться на предоплату.

– Цены, установленные намного ниже рыночных, могут быть признаком мошенничества.

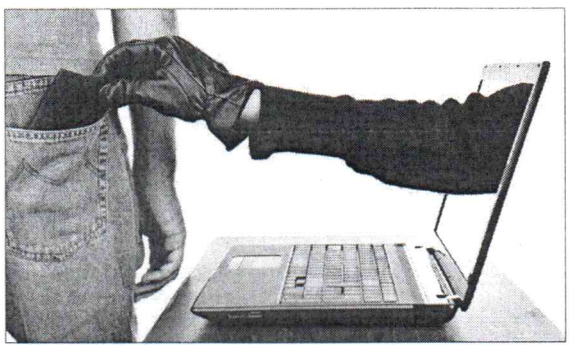
– Прежде, чем оплатить товар, его необходимо тщательно проверить.

НАСТОРОЖИТЕСЬ, ЕСЛИ ВАМ ПРЕДЛАГАЮТ ДЛЯ РАСЧЕТОВ КОШЕЛЕК «КИВИ»

Особенность этой платежной системы – проводить платежи на небольшие суммы без идентификации получателя. Если мошенник получит деньги, найти его потом будет сложно.

НЕ ОТПРАВЛЯЙТЕ ДЕНЬГИ БЛИЗКИМ, ЕСЛИ ОНИ ОБ ЭТОМ ПРОСЯТ В СОЦСЕТЯХ ИЛИ С НЕЗНАКОМЫХ НОМЕРОВ

Лучше позвоните и все узнайте; аккаунт могли взломать.



Никому не сообщайте реквизиты банковской карты

В России 68 % мошеннических операций совершается с помощью реквизитов. Мошеннику нужны только цифры, которые написаны прямо на карте – и он уже сможет вас ограбить.

Реквизиты – это всё, что написано на карте: номер из 16 цифр (иногда 18), имя и фамилия владельца, срок действия и CVC-код – трехзначный код безопасности на обратной стороне. Отнесем к реквизитам и смс-код, который присылает вам банк, когда вы платите в интернете или переводите деньги.

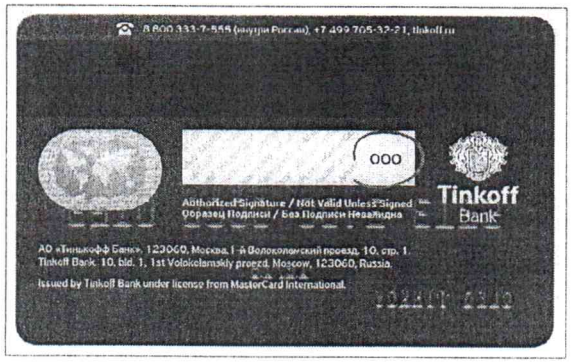
По правилам платежных систем реквизиты нельзя сообщать посторонним. Если банк узнает, что ваши реквизиты попали в чужие руки, то сразу заблокирует карту.

Однако кое-что сообщать все-таки можно. Если кратко, дела обстоят так: (пример-карта банка Tinkoff)

Номер карты из 16 цифр; **можно пересылать, диктовать друзьям и знакомым.**

Имя и фамилия латиницей; **тоже можно.**

Срок действия; **никому не сообщайте и не пересылайте.**



Трехзначный код безопасности на обратной стороне; **никому не сообщайте и не пересылайте.**

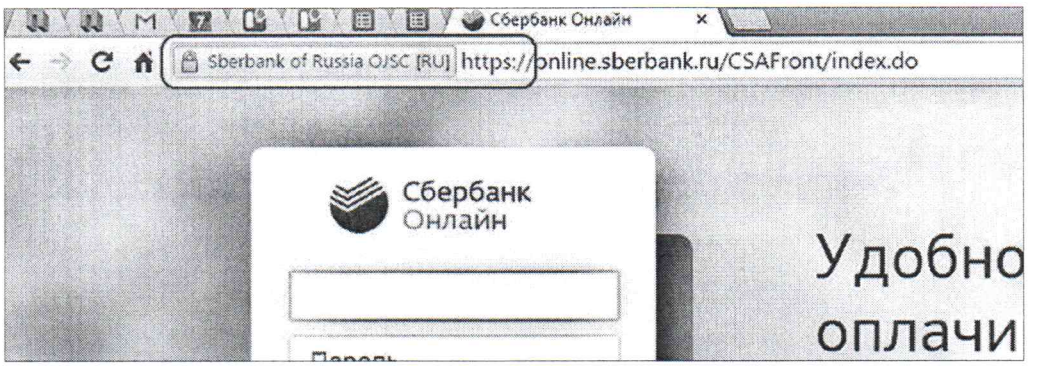
Код из смс; **ни в коем случае, никому и не при каких обстоятельствах не сообщайте.**

КАК ОБМАНЫВАЮТ ЧЕРЕЗ БАНКИ?

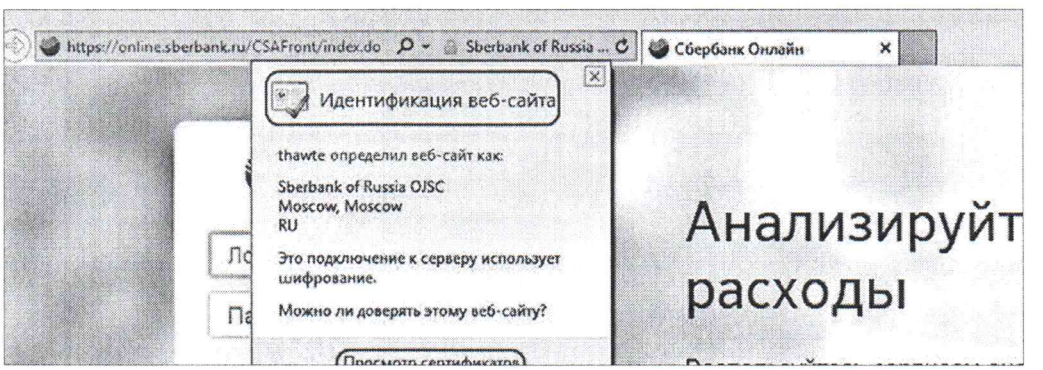
Мошенники создают специальные обманные страницы. Внешне они действительно напоминают реальное приложение.

Например, «Сбербанк онлайн». Сравним настоящий сайт «Сбербанк-Онлайн» и поддельный.

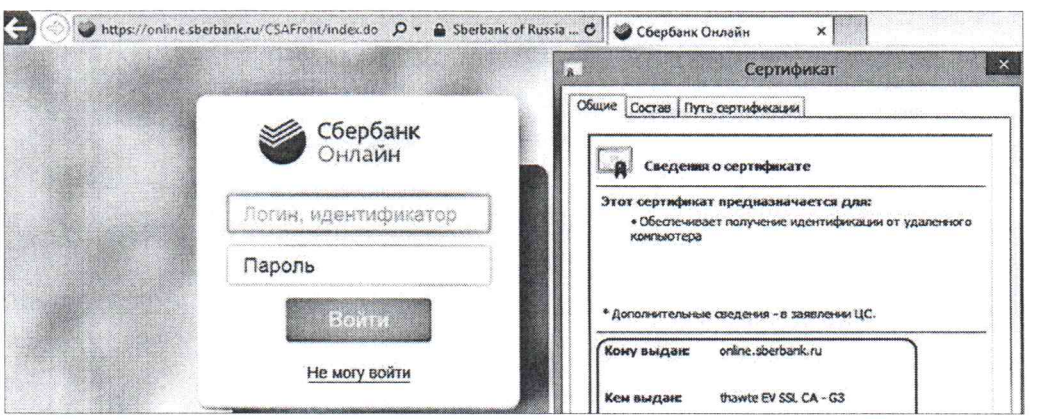
Настоящая страница «Сбербанк-Онлайн» выглядит так, а красным выделены места, на которые, в первую очередь, нужно обращать внимание.



1. Адрес в адресной строке начинается с https;
2. В адресной строке есть надпись Sberbank of Russia OJSC [RU];
3. В зависимости от браузера вся адресная строка или только надпись будут подсвечены зеленым цветом.

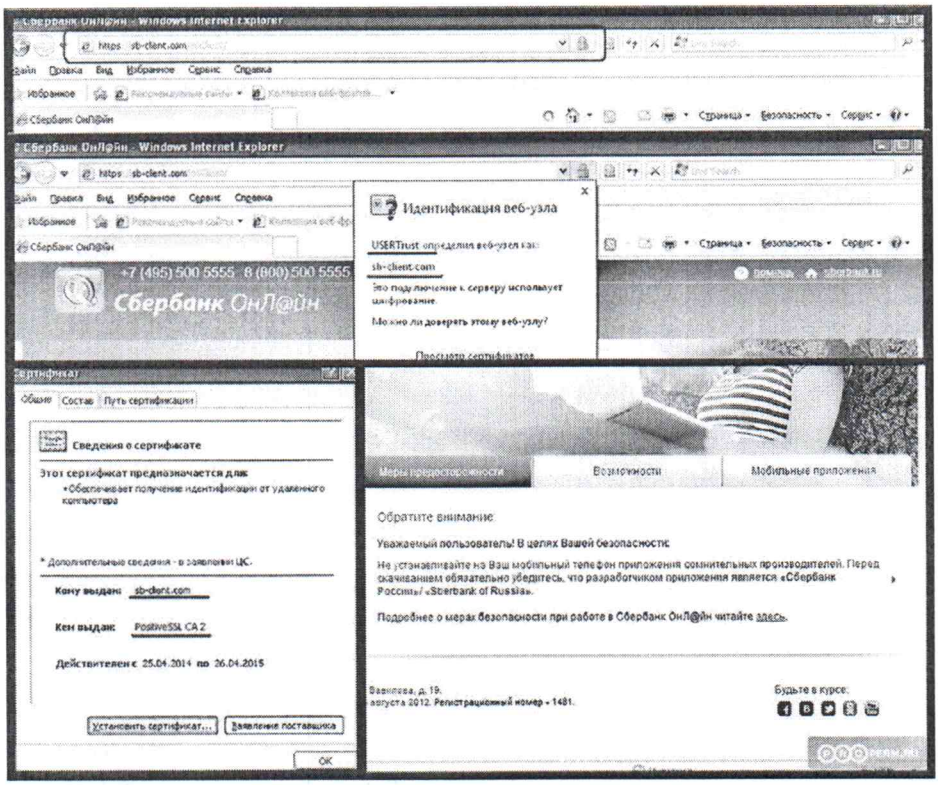


Кликнув мышью на надпись в адресной строке, вы сможете увидеть данные сертификата.



А нажав на плашку «Просмотр сертификата», увидеть подробные сведения о том, кому и кем выдан сертификат, а также срок его действия.

А вот так выглядит поддельный сайт:



Согласитесь, очень похоже на настоящий.

Теперь вы знаете, что мошенничество в интернете имеет много обличий. Защитить от него может только рассудительность и внимательность.

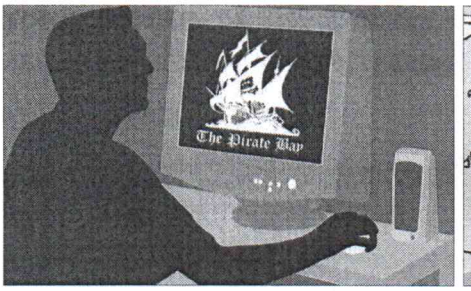
ЗАЩИТИТЕ СВОЙ ДОСТУП В ИНТЕРНЕТ

Для защиты хороши все средства: VPN, антивирусы, приложения для шифрования данных и хранения паролей.

Не экономьте на безопасности и покупайте лицензионные программы.

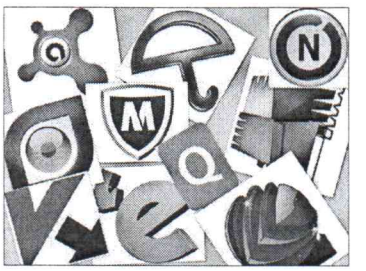
VPN защищают вас от хакеров, вредоносного ПО и других угроз Интернета.

Не используйте пиратские программы.



Мошенники научились красть с их помощью пароли и доступ к вашим финансовым программам.

Доверяйте своей антивирусной программе



Если она советует не заходить на какой-то сайт, или не советует скачивать приложение – не отключайте антивирус.

Придумывайте надежные пароли и храните их в надежном месте.

Если не можете придумать сами – используйте специальные программы-генераторы.

Если же вас обманули, то обязательно обратитесь в правоохранительные органы. В структуре МВД России есть специальный отдел «К», который занимается преступлениями в интернете.

ТЕЛЕФОНЫ ЭКСТРЕННОГО РЕАГИРОВАНИЯ

ЕДИНЫЙ ТЕЛЕФОН ВЫЗОВА ЭКСТРЕННЫХ СЛУЖБ

112

ГУВД МВД России по Новосибирской области,

г.Новосибирск, ул.Октябрьская 78

232-70-00 дежурная часть

МО МВД России «Новосибирский», г. Новосибирск, ул. Объединения 9

232-20-38 дежурная часть