Финансовая грамотность

2022

Управление Роспотребнадзора по Саратовской области

Финансовая безопасность

Наша финансовая безопасность напрямую зависит от принимаемых нами ежедневно решений. Непродуманный выбор поставщика финансовых услуг, невнимательное чтение условия договоров, отсутствие финансовой дисциплины и - как следствие - неисполнение своих обязательств и неприятная финансовая ситуация.

Финансовое мошенничество — совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.

- **Мошенничества с использованием банковских карт**
- **Интернет-мошенничества**
- **Мобильные мошенничества**
- **Финансовые пирамиды**
- **Кредит в продаже медицинских услуг**

Мошенничества с использованиям банковских карт

КАРТА

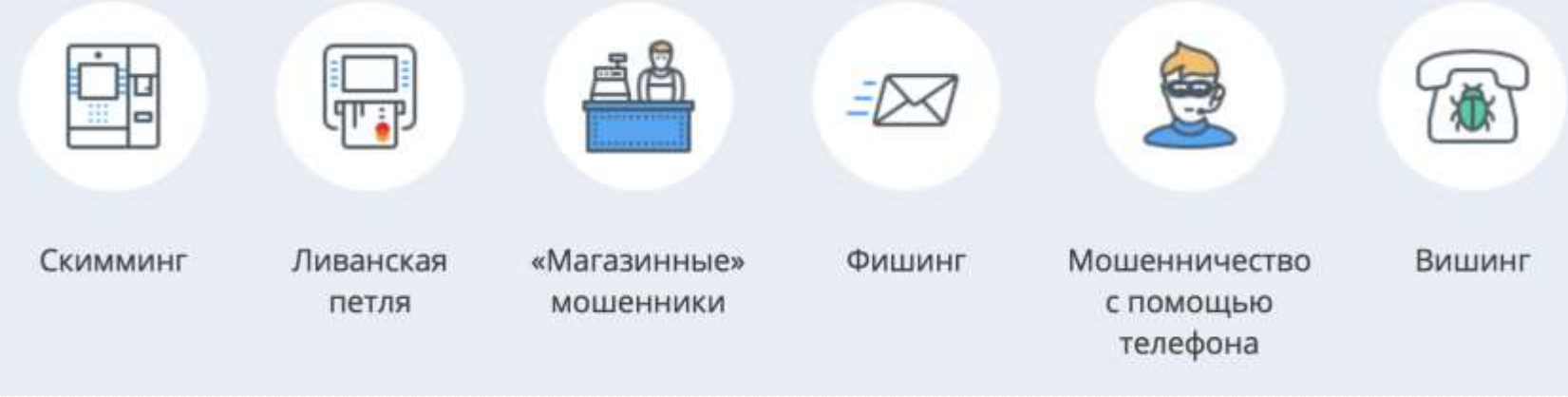
Банковская карта – удобный инструмент повседневных расчетов.

Наиболее распространены:

- **Дебетовые - инструмент управления банковским счетом, на котором размещены собственные средства держателя карты.**

- **Кредитные - это банковская пластиковая карта, позволяющая на основании заключенного с банком договора брать в долг у банка определенные суммы денег в пределах установленного кредитного лимита.**

СХЕМЫ МОШЕННИЧЕСТВ С КАРТАМИ



Способы обмана людей и кражи денег с их банковских карт разнообразны: от подглядывания из-за плеча во время операций с банкоматом и последующего хищения карты до хакерских атак на программное обеспечение. При этом преступники постоянно придумывают новые способы хищения денежных средств, по мере того как старые перестают работать. Именно поэтому важно быть в курсе основных приемов, которые используют злоумышленники, и соблюдать базовые правила безопасности.

СКИММИНГ

Предполагает установку специальных устройств на банкоматы, с помощью которых преступники получают информацию о карте.

Таковыми выступают накладная клавиатура (очень похожая на настоящую) и устройство для считывания данных карты, которое устанавливается на к

Вместо клавиатуры может быть установлена миниатюрная камера, которая заснимет процесс ввода ПИН-кода.

При использовании банкомата осмотрите поверхность над ПИН-клавиатурой и устройство для приема карты на предмет нахождения посторонних предметов.

ТРАППИНГ (ЛИВАНСКАЯ ПЕТЛЯ)

или помощь прохожего. Суть этого вида мошенничества заключается в установке на банкомат устройства, которое блокирует карту и не выдает ее обратно.

Отрезок фотопленки (складывается пополам, края загибаются под углом в 90 градусов) вставляется в банкомат. На нижней стороне фотопленки вырезан небольшой лепесток, отогнутый вверх по ходу карты. Пленка располагается в картридере так, чтобы не мешать проведению транзакции. Отогнувшийся лепесток не позволяет банкомату выдать пластиковую карту обратно.

На помощь человеку приходит «добрый» мошенник, раздавая различные советы. В процессе «помощи» растерянный человек обычно соглашается на введение ПИН-кода, который и запоминает преступник. После чего мошенник «уходит», советуя обратиться в банк. Растерянный человек оставляет карту в банкомате, а мошенник спокойно ее достает и использует по своему усмотрению.

Закрывайте рукой клавиатуру при вводе ПИН-кода

МАГАЗИННЫЕ МОШЕННИЧЕСТВА

От недобросовестных сотрудников в организациях не застрахован никто. Данные карты могут быть считаны и зафиксированы ручным скиммером, а впоследствии использованы для хищения денег

- **Не передавайте карту посторонним: ее реквизиты (номер карты, срок действия, имя владельца, CVV/ CVC-код) могут быть использованы для чужих покупок**
- **Требуйте проведения операций с картой только в личном присутствии, не позволяя уносить карту из поля зрения (например, официантам или кассирам)**

ФИШИНГ

Цель фишинга — получить данные о пластиковой карте от самого пользователя. В этом случае злоумышленники рассылают пользователям электронные письма, в которых от имени банка сообщают об изменениях, якобы производимых в системе его безопасности.

При этом мошенники просят доверчивых пользователей возобновить информацию о карте, в том числе указать номер кредитки и ее ПИН-код. Сделать это предлагается несколькими способами: либо отправив ответное письмо, либо пройдя на сайт банка-эмитента и заполнив соответствующую анкету. Однако ссылка, прикрепленная к письму, ведет не на ресурс банка, а на поддельный сайт, имитирующий работу настоящего.

Самая сложная задача мошенника — узнать ваш ПИН-код. Никому не сообщайте свой ПИН-код.

МОШЕННИЧЕСТВО С ПОМОЩЬЮ ТЕЛЕФОНА

Разновидностью фишинга являются звонки на сотовые телефоны граждан от «представителей» банка с просьбой погасить задолженность по кредиту.

Когда гражданин сообщает, что кредит он не брал, ему предлагается уточнить данные его пластиковой карты.

В дальнейшем указанная информация используется для инициирования несанкционированных денежных переводов с карточного счета пользователя.

Банки и платежные системы никогда не присылают писем и не звонят на телефоны своих клиентов с просьбой предоставить им данные счетов. Если такая ситуация произойдет, вас попросят приехать в банк лично.

ВИШИНГ (ГОЛОСОВОЙ ФИШИНГ)

вид мошенничества, использующий технологию, позволяющую автоматически собирать информацию, такую, как номера карт и счетов.

Мошенники моделируют звонок автоинформатора, получив который держатель получает следующую информацию:

- Автоответчик предупреждает потребителя, что с его картой производятся мошеннические действия, и дает инструкции — перезвонить по определенному номеру. Злоумышленник, принимающий звонки по указанному автоответчиком номеру, представляется вымышленным именем от лица финансовой организации.
- Когда по этому номеру перезванивают, на другом конце провода отвечает типичный компьютерный голос, сообщающий, что человек должен пройти сверку данных и ввести 16-значный номер карты с клавиатуры телефона.
- Затем, используя этот звонок, можно собрать и дополнительную информацию, такую, как CVV-код, срок действия карты, дата рождения, номер банковского счета и т. п.

МЕРЫ БЕЗОПАСНОСТИ

Несмотря на все системы информационной безопасности банка в результате мошеннических операций с картами существует отличная от нуля вероятность хищения средств с вашей карты. Чтобы избежать исчезновения денег, **соблюдайте правила, затрудняющие неправомерные операции с вашими финансами:**

- **Храните ПИН-код отдельно от карты и не пишите его на карте, не сообщайте никому и не вводите ПИН-код при работе в Интернете. При его потере или краже -заблокируйте карту**
- **Сохраняйте все документы до окончания проверки правильности списанных сумм**
- **Сообщайте банку актуальные контактные данные**
- **Подключите услугу SMS- уведомлений, всегда имейте при себе телефон службы поддержки**

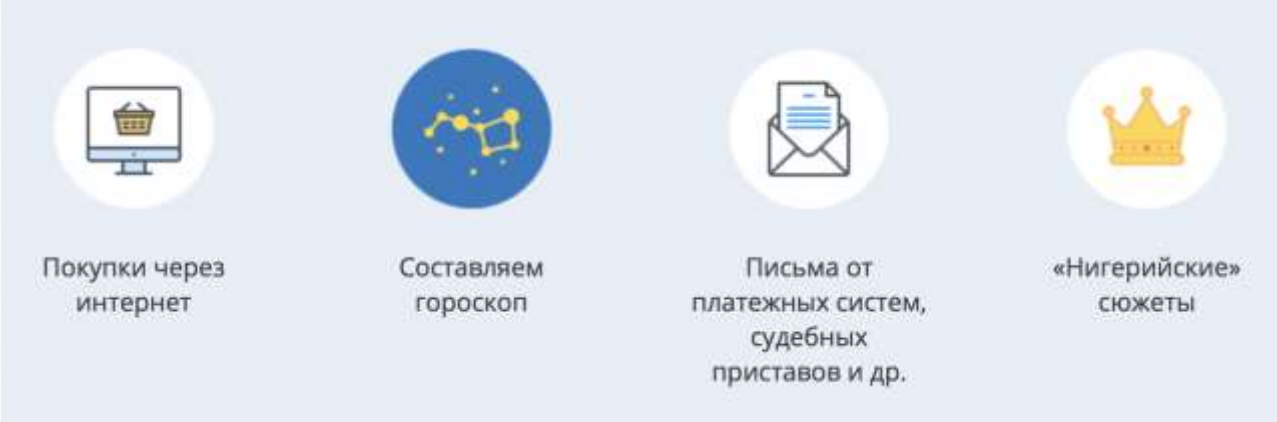
В случае мошеннической или ошибочной операции по карте уведомите банк до конца следующего дня, чтобы сумма этой операции была полностью возмещена банком, иначе вернуть деньги будет гораздо сложнее.

ПРИ РАСЧЕТЕ КАРТАМИ

- **Не превышайте лимит кредитования – это может приводить к блокированию карты, штрафам и комиссиям**
- **Своевременно оплачивайте кредит – это обеспечит отличную кредитную историю и убережет от штрафов**
- **Не допускайте потери карты, поломки, блокировки - перевыпуск карты может стоить дополнительных средств**
- **Не снимайте с карты деньги полностью – оставьте сумму для оплаты комиссий или автоматических платежей. В случае отсутствия суммы и если карта предусматривает овердрафт, банк совершит данный платеж за счет заемных средств.**
- **Если сменили место работы уточните актуальные для вас тарифы по зарплатной карте**
- **При использовании карты зарубежом, помните о курсовой разнице. Если карта привязана к рублевому счету, то при расчетах за границей банкоматы и платежные терминалы будут использовать один курс, а российский банк спишет деньги со счета, применяя другой, и может возникнуть нежелательный «технический овердрафт».**

Интернет-мошенничества

ВИДЫ ИНТЕРНЕТ-МОШЕННИЧЕСТВ



Мошенничество в интернете включает в себя все существующие виды обмана, придуманные человечеством за всю историю его существования. Этот перечень обширен, поскольку мошенники по максимуму используют все преимущества интернет-коммуникаций: массовый охват, возможность выбора целевой группы, оперативность.

ПОКУПКИ ЧЕРЕЗ ИНТЕРНЕТ

Покупатель (жертва) соглашается купить у продавца (мошенника) товар через интернет. Продавец просит оплатить товар через систему денежных переводов и получает деньги, используя зачастую фальшивое или недействительное удостоверение личности. Обещанный товар не доставляется покупателю.

Такая схема мошенничества обычно имеет один или несколько явных признаков — например, предлагаемый товар продается по удивительно низкой цене.

СОСТАВЛЕНИЕ ГОРОСКОПА

Объявлений, предлагающих заказать персональный гороскоп, очень много во всемирной паутине. Авторы обещают выслать его быстро и бесплатно. Пользователю предлагается заполнить стандартную анкету (имя, фамилия, дата рождения), оставить свой электронный адрес.

Любитель астрологии указывает все эти данные, но вместо гороскопа в его ящик попадает письмо с еще одним условием: чтобы получить заказ, надо отправить по указанному номеру СМС-сообщение с набором тех или иных цифр. При этом забывают добавить, что стоимость этого сообщения может составлять **несколько сотен рублей**. В лучшем случае ему, действительно, пришлют гороскоп. Причем сразу же, что уже вызывает сомнения в его уникальности. В худшем — ничего не пришлют.

ПИСЬМА ПЛАТЕЖНЫХ СИСТЕМ

Вы можете обнаружить в своем почтовом ящике письмо от администрации платежной системы (e-gold, Moneybookers, Paypal), судебных приставов и других… В послании, например, говорится, что у вас есть долг по кредиту и вам нужно срочно сверить данные в файле. К письму прилагается вложение — файл, который нужно скачать и открыть. Или же в письме есть ссылка, по которой нужно перейти «для скачивания программы».

На самом деле часто вас поджидает **вирус**, задача которого - собрать данные о ваших аккаунтах в платежных системах, **данные банковской карты**, которые вы вводите на своем компьютере.

«НИГЕРИЙСКИЕ» СЮЖЕТЫ

Суть этой мошеннической схемы сводится к тому, что некто представляется получателю письма действующим или бывшим министром или представителем знатной нигерийской (зимбабвийской, кенийской...) семьи, попавшей в немилость на родине. К адресату обращаются с просьбой оказать содействие в выводе из охваченной гражданской войной страны крупной суммы, которая будет переведена на счет адресата. Ему за помощь «в спасении средств» обещают солидный процент. Когда клиент «заглатывает наживку», его просят перечислить незначительную сумму, необходимую для оформления перевода, дачи взятки или оплаты услуг юриста. Затем появляется еще одна причина перечислить «незначительную» сумму, потом другая... Деньги тянут из доверчивого клиента до тех пор, пока он не осознает, что его обманули.

По результатам специальных исследований, примерно один процент пользователей интернета, то есть **каждый сотый**, получивших по e-mail «нигерийские письма», оказываются вовлеченными в эту аферу. В арсенале мошенников как правило всего несколько уловок, которые могут сочетаться в одном письме.

СПОСОБЫ ЗАЩИТЫ

- Старайтесь не открывать сайты платежных систем по ссылке (например, в письмах). Обязательно проверяйте, какой URL стоит в адресной строке, или посмотрите в свойствах ссылки, куда она ведет. Вы можете попасть на сайт-обманку, внешне очень похожий, практически неотличимый от настоящего сайта платежной системы. Расчет в этом случае на то, что вы введете на таком сайте свои данные и они станут известны мошенникам.
- Совершайте покупки в интернете с помощью отдельной банковской карты и только на проверенных сайтах
- Никогда никому не сообщайте ваши пароли. Вводить пароли можно и нужно только на самих сайтах платежных процессоров, но никак не на других ресурсах.
- Не храните файлы с секретной информацией на доступных или недостаточно надежных носителях информации. Всегда делайте несколько копий таких файлов на разных носителях.

СПОСОБЫ ЗАЩИТЫ

- Если вам предлагают удаленную работу и при этом просят оплатить регистрационный взнос в качестве гарантии за пересылку данных и т. п., не попадайтесь на эту ловушку. Настоящие работодатели никогда не просят денег с соискателей, они сами платят за работу!
- Предложения в духе «вышлите туда-то небольшую сумму и вскоре вы будете завалены деньгами» — это предложения от участников финансовых пирамид. Не верьте таким предложениям, в пирамидах выигрывают только их создатели.
- Письма о проблемах с вашим счетом в какой-либо платежной системе, требующие перехода на сайт и каких-либо действий от вас, отправляйте в корзину, не открывая. Техническая поддержка платежных систем никогда не рассылает таких писем.
- В 99 % случаев платежи, которые вы делаете онлайн, отменить нельзя. Поэтому не торопитесь, подумайте, прежде чем заплатить за товар или услугу.

Мобильные мошенничества

ВИДЫ МОБИЛЬНЫХ МОШЕННИЧЕСТВ

Основных видов мобильного мошенничества немного, но их вариаций достаточно много, причем все они выгодны для мошенников и приносят им огромные суммы денег. Даже при небольших финансовых потерях конкретного человека (15-150 рублей) срабатывает эффект масштаба, когда жертвами становятся тысячи людей.

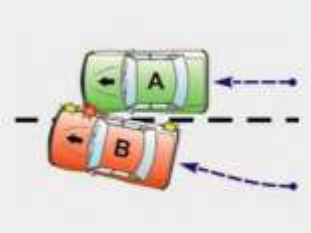
По данным международной статистики, совокупные потери операторов связи и абонентов от мобильного мошенничества ежегодно составляют **примерно 25 млрд долларов**.

«ВЫ ВЫИГРАЛИ ПРИЗ…»

Мошенник привлекает «жертву» дорогим подарком, который выиграл абонент, но при этом просит прислать подтверждающую СМС, внести «регистрационный взнос» через интернет-кошелек, купить карточку предоплаты и перезвонить, назвав код.

Получив «взнос», мошенник исчезает, а обещанный приз тоже растворяется.

«МАМА, Я ПОПАЛ В АВАРИЮ…»



Эта схема направлена на воздействие на психику человека. Мошенник отправляет СМС или звонит с неприятной новостью, «жертва» в панике забывает проверить достоверность полученной информации и переводит средства на счета мошенников.

«ВАША КАРТА ЗАБЛОКИРОВАНА»

На мобильный телефон приходит СМС «Ваша банковская карта заблокирована. По вопросам разблокировки обращайтесь по телефону…». «Жертва» перезванивает по указанному номеру и «сотрудник банка», которым является мошенник, предлагает пройти к банкомату и совершить несколько операций под диктовку. Результат не заставит себя долго ждать - деньги с карты перейдут на счет мошенников.

ВИРУС

Он помогает злоумышленникам подобраться к банковской карте, привязанно к мобильному телефону, и перевести все деньги на свой счет.

СПОСОБЫ ЗАЩИТЫ

- Не отвечайте на СМС и не открывайте ММС от неизвестных абонентов, в том числе поздравительные сообщения и открытки. С вашего счета могут списать деньги.
- При получении сообщений от банков, мобильных операторов о проблемах со счетом перезвоните по известному вам номеру банка и уточните информацию. Банк никогда не сообщает подобным образом информацию.
- Не отправляете СМС на короткие номера, заранее не узнав стоимости подобного сообщения. Это можно сделать на сайте своего оператора мобильной связи.

Дружи с финансами
НАЦИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ ФИНАНСОВОЙ ГРАМОТНОСТИ ГРАЖДАН
вашифинансы.рф

СПОСОБЫ ЗАЩИТЫ

- Никогда не сообщайте никаких персональных данных (дату рождения, ФИО, данные о родственниках и т. д.), даже если вам звонят и представляются сотрудником банка, полиции, мобильных операторов и т. д. Попросите представиться, назвать ФИО, звание-должность, поинтересуйтесь, какой адрес у отделения, офиса, уточните наименование организации. Затем узнайте телефон этой организации в справочных базах и перезвоните. Помните: мошенники могут использовать ваши персональные данные в разнообразных преступных схемах, вплоть до открытия на ваше имя фирмы.
- Вам могут позвонить и сообщить, что ваш родственник или знакомый попал в аварию, за решетку, в больницу и за него нужно внести залог, штраф, взятку — откупиться. Не верьте! Позвоните вашему родственнику.
- Ценную информацию никогда не храните только в телефоне, дублируйте ее в бумажном блокноте или в компьютере.

Как не стать жертвой финансовой Пирамиды

ФИНАНСОВАЯ ПИРАМИДА

Если говорить о деньгах, то нами движут два основных чувства: страх потерять заработанное и желание максимально преумножить то, что уже есть. К сожалению, часто именно второе чувство притупляет осторожность и приводит к плачевным финансовым результатам.

Финансовая пирамида – схема инвестиционного мошенничества, в которой доход по привлеченным денежным средствам образуется не за счет вложения их в прибыльные активы, а за счет поступления денежных средств от привлечения новых инвесторов.

ПРИНЦИП РАБОТЫ

Инвесторов побуждают вкладывать денежные средства обещанием получения высокой гарантированной доходности. Поскольку нет возможности обеспечить в течение длительного времени постоянный приток денежных средств новых инвесторов, ресурсы финансовой пирамиды начинают сокращаться, а финансовые обязательства растут. Возможность возврата вложенных средств с течением времени становится всё меньше.

Закономерным итогом такой ситуации становится крах финансовой пирамиды, в результате которого инвесторы теряют вложенные средства.

ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ ПИРАМИДЫ

Во-первых, не поддавайтесь на агрессивную рекламу «легких и быстрых денег», гарантированная доходность выше ставки банковского депозита – повод задуматься о целесообразности таких вложений.

Во-вторых, обратите внимание на следующие признаки, которые могут характеризовать организацию как «финансовую пирамиду»:

- Вам объясняют высокую доходность непрозрачными сверхприбыльными проектами, при этом не раскрывают информацию о потенциальных рисках. Проекты, как правило, находятся в другой стране, что затрудняет выяснение текущего положения дел.
- Организаторы скрывают информацию о себе, о наличии лицензий на ведение соответствующей деятельности и действуют через посредников. Часто компания зарегистрирована не в России.
- Вам обещают высокое вознаграждения за приведенных друзей, знакомых или родственников. Предлагают построить систему привлечения клиентов и зарабатывать на ней. Агрессивно рекламируют свои услуги

В-третьих, старайтесь принимать взвешенные финансовые решения, не поддавайтесь эмоциям, повышайте свои знания в области финансовой грамотности.

ПРИЗНАКИ ПИРАМИДЫ

Не поддавайтесь на агрессивную рекламу «лёгких и быстрых денег». Прежде чем принять решение о вложении денег, проверьте поступившее вам предложение на **признаки финансовой пирамиды**:

- Призыв не раздумывать и вкладывать быстро
- Обещание сверхвысокой доходности больше 20% годовых
- Объяснение такой доходности непрозрачными сверхприбыльными проектами
- Обещание вознаграждения за приведенных клиентов
- Анонимность организаторов и отсутствие защиты прав вкладчика в договоре
- Отсутствие информации о возможны рисках
- Требование , например, оплатить «вступительный взнос», «обучение», «участие в семинаре»
- Отсутствие лицензии/ указание номера чужой лицензии, или собственной, но не позволяющей работать с денежными средствами

ЧТО ДЕЛАТЬ

Перед тем, как отдать деньги:

- Проверьте наличие лицензии Центрального банка на ведение деятельности (банковская, страховая, инвестиционная).
- Внимательно изучите договор на предмет условий инвестирования и возврата средств.
- Найдите в Интернете информацию о данной организации, ее историю, отзывы клиентов, рейтинги в соответствующей отрасли.

Если деньги уже вложены в сомнительные проекты, постарайтесь максимально оперативно изъять не только полученную прибыль, но и основные вложения. Не ждите, когда пирамида развалится, и не старайтесь компенсировать убытки, вкладывая новые средства.

РЕЗЮМЕ

- **Проявляйте бдительность и внимательность к своим ежедневным финансовым операциям.**
- **Никогда никому не сообщайте ваши пароли, ПИН-код, CVV.**
- **Используйте антивирусное программное обеспечение.**
- **При совершении платежей в интернете обязательно проверяйте, какой URL стоит в адресной строке**
- **Не передавайте банковскую карту третьим лицам.**
- **Обязательно установите пароль для разблокировки телефона, особенно если на нем установлено банковское мобильное приложение.**
- **Гарантирование доходности по инвестициям, в несколько раз превышающей рыночный уровень, является признаком финансовой пирамиды.**
- **При получении сомнительных СМС от банков или лиц, представившихся родственниками, позвоните в банк или родственникам, уточните информацию. Не отвечайте на сомнительные СМС.**
- **Если Вы стали жертвой финансовых мошенников, сообщите в полицию.**

СПАСИБО ЗА ВНИМАНИЕ!

ДО СВИДАНИЯ!