

Татьяна Алёхина

**Коротко
о
финансовой
безопасности**

Татьяна Алёхина

Коротко о финансовой безопасности

<https://litres.ru/74437482>

SelfPub; 2026

Аннотация

Финансовая безопасность — это фундамент, на котором строится благополучие каждого человека и государства в целом. В современном мире, где экономические процессы развиваются стремительными темпами, а финансовые инструменты становятся всё более сложными, умение защитить свои средства и грамотно управлять ими — это не просто привилегия, а необходимость.

Эта книга — ваш путеводитель в мире финансовой безопасности. Она научит распознавать финансовые риски и эффективно противостоять им.

Мы живём в эпоху, когда финансовая грамотность становится важнейшим навыком. Эта книга поможет вам:

Понять основы финансовой безопасности

Научиться защищать свои деньги

Обеспечить финансовую стабильность своей семьи

Независимо от вашего уровня дохода и опыта в финансовой сфере, эта книга станет вашим надёжным помощником на пути к финансовой безопасности. Помните: защищённые финансы —

это уверенность в завтрашнем дне и возможность реализовать свои мечты.

Вперёд к финансовому благополучию!

Автор

Содержание

Глава 1. Финансовая безопасность	5
Статья 1.1 Финансовая безопасность	5
Статья 1.2 Проверка участника финансового рынка	11
Статья 1.3 Обязанность банков возвращать клиентам средства, ранее переведенные мошенникам	13
Статья 1.4 Как правильно давать или брать деньги в долг	15
Статья 1.5 Безопасность сделки при строительстве частного дома	18
Статья 1.6 Предупреждение кражи номера телефона, sim-карты, подмены сим-карты	20
Статья 1.7 Финансовая подушка безопасности	25
Статья 1.8 Не попадайтесь на дипфейк	26
Статья 1.9 Не попадайтесь на фишинг	28
Статья 1.10 Не допускайте виртуального клона Вашей банковской карты	30
Конец ознакомительного фрагмента.	31

Татьяна Алёхина

Коротко о финансовой безопасности

Глава 1. Финансовая безопасность

Статья 1.1 Финансовая безопасность

В современном мире в век цифровых технологий, нейросетей, искусственного интеллекта и роста мошенничества важно владеть навыками финансовой безопасности:

1. Никогда и никому не говорите, сколько у вас денег.
2. Никогда и никому не говорите, какой ваш доход
3. Планируйте свой бюджет
4. Формируйте подушку безопасности!
5. Диверсифицируйте свои деньги!
6. Замечательная русская пословица «Не держите яйца в одной корзине»
7. Избегайте кредитов и долгов!
8. Надёжно храните пароли и личные данные!
9. Будьте внимательными при онлайн оплате!
10. Часто злоумышленники используют подменные стра-

ницы сайтов и подменные приложения для оплаты популярных товаров или услуг.

11. В разговоре с мошенниками лучше не произносить слова «да» и «нет». Это может быть использовано мошенниками в дальнейшем для голосового подтверждения действий от имени аккаунта жертвы. Альтернативный вариант: «слушаю», «не имею возможности», «отрицаю», завершайте разговор быстро.

12. Блокируйте мошенников в телефоне.

13. Не держите в одном банке больше 1 млн. 400 рублей.

14. Оплачивать все счета и налоги вовремя!

15. Принимайте финансовое решение самостоятельно!

16. Не изучив финансовый инструмент, не пользуйтесь.

17. Придется идти на опережение мошенников, изучайте не спеша схемы мошенников, зная схемы мошенников, можно предупредить нежелательную ситуацию и операцию.

18. Не переходите по незнакомым ссылкам, тем более которые невзначай просят Ваши личные данные и данные вашей банковской карты.

19. Чтобы посторонние не могли использовать деньги с вашей карты, нельзя говорить им: срок действия, CVC-код, ПИН-код, код из СМС для подтверждения оплаты, если вы ее не совершали. Если вы сами оплачиваете покупки в интернете, не вводите данные банковской карты на подозрительных сайтах, мошенники могут похитить их.

20. Не держите в одном кошельке банковскую карту и

ПИН-код к ней. ПИН-код должен быть отдельно от банковской карты.

21. Не держите на одной банковской карте все деньги. В случае утери карты мошенники смогут воспользоваться лимитом карты. Банки имеют право сами устанавливать верхний порог покупок без ПИН-кода, однако он не должен превышать максимум, установленный платежной системой. Для «Мира» этот лимит составляет 3 тыс. рублей. Некоторые банки установили 5 тыс. рублей.

22. Возможно автоматизировать пополнение банковской карты ежедневно в пределах суммы Ваших ежедневных покупок.

23. Никогда не носите деньги в финансовую пирамиду.

24. Наличные носите во внутреннем кармане. Внутренний карман сумки или верхней одежды – наилучший вариант для транспортировки наличных денег. Меньше соблазнов для вора. И еще совет – не пересчитывайте свои деньги при посторонних (особенно в транспорте).

25. При дальней поездке распределите деньги:
наличные в разных сумках
безналичные на разных карточках.

26. Прежде, чем ответить на незнакомый звонок, проверьте его на отзывы. Ничего, если Вы перезвоните.

27. Не сообщайте никому логин и пароль от гос.услуг

28. В случае проживания в зоне обстрела распределите денежные средства:

В наличке

В безналичке

В недвижимости

В движимом имуществе

Да хоть вогороде

29. Не вкладывайте свои сбережения и тем более заёмные средства в схемы получения дохода, суть которых не понимаете и которые обещают сверхприбыль

30. При оформлении микрозаймов Вы должны понимать, что микрофинансовые организации выдают займы быстро с минимальным пакетом документов, но под высокие проценты (максимальная ставка составляет 0,8% в день). При просрочке сумма к возврату значительная.

31. В случае звонка якобы от сотрудника банка, работника Центробанка, следователя, служащего отдела безопасности, менеджера ВК, Дзен, телеграммканала, ватцап, Одноклассников спросите должность и Ф.И.О., место работы, Ф.И.О. и должность руководителя отдела и скажите: «Перезвоню»

32. Не записывайте логины и пароли для входа в личные кабинеты на сайтах банков, Госуслугах и других сервисах в блокнотах и бумажниках, которые берете с собой в общественные места

33. Не спешите помогать попавшим в беду родственникам! Если Вам звонят и рассказывают о несчастном случае, который якобы произошел с Вашим близким, что срочно требуется помощь, не торопитесь её оказывать. Не отправ-

ляйте и не передавайте деньги по такой просьбе. Успокойтесь и самостоятельно позвоните тому, с кем случилась якобы беда. Уточните у близкого, всё ли с ним хорошо. В большинстве случаев это не более, чем выдумка мошенников с целью заполучить Ваши деньги.

34. Старайтесь меньше информации о себе выкладывать в соц.сети. После опубликования объявления о продаже, например, после сделки просите админа удалять объявление. Хотя после удаления инфы все равно надолго в интернете.

35. Если Вы инвестируете денежные средства в фондовом рынке, при коррекции фондового рынка сохраняйте часть портфеля в деньгах, чем больше коррекция и больше снижение цен акций, тем больше увеличивайте % портфеля в деньгах. Точку входа находите, когда рынок не лихорадит.

36. Заведите отдельную сим-карту для банков.

37. Если Вы не пользуетесь сим-картой какого-то мобильного оператора, то обязательно вспомните и проверьте еще раз, не привязывали ли к этой симке и этому номеру телефона банковскую карту банка, которой тоже возможно уже не пользуетесь. Если Ваш номер мобильного телефона заблокирован по причине того, что Вы не пользуетесь ей и не платите мобильному оператору, а Вы забыли или не посчитали нужным в банке снять привязку к заблокированному номеру телефона, то злоумышленники могут воспользоваться этой возможностью и взять на Вас кредит! Тем более, если не установлен самозапрет на выдачу кредита!

Поскольку мобильные операторы к сожалению практикуют выдачу мобильного номера через время второму владельцу, если первый владелец долго не пользуется, то тоже вероятность взять на Вас кредит на бывший номер телефона растет. Код придет по смс на телефон, который привязан к Вашей карте.....

38. При строительстве дома используйте счета эскроу.

39. Не попадайтесь на дипфейк.

40. Не попадайтесь на фишинг.

Статья 1.2 Проверка участника финансового рынка

Банк России разработал новый веб-сервис (API), предоставляющий информацию об участниках финансового рынка

<https://cbr.ru/finorg/>

Веб-сервис позволяет автоматизировать получение актуальной информации об участниках финансового рынка, в том числе наличии права (лицензии) на осуществление деятельности на финансовом рынке, а также о подразделениях кредитных организаций.

Сведения могут быть получены по регистрационным данным участника рынка, типу/виду деятельности, субъекту Российской Федерации, наличию права (лицензии) на конкретную дату и за период времени.

В результате автоматизированной обработки запроса веб-сервис предоставляет информацию, аналогичную публикуемой в сервисе «Проверить участника финансового рынка».

Все организации, которые предоставляют финансовые услуги, — банки, небанковские кредитные организации (НКО), негосударственные пенсионные фонды (НПФ), страховые организации (СО), управляющие компании (УК), профессиональные участники рынка ценных бумаг (ПУРЦБ)

(в том числе брокеры, дилеры, инвестиционные советники), операторы финансовых платформ (ОФП) и другие операторы финансовых услуг, микрофинансовые организации (МФО), кооперативы (ЖНК, КПК, СКПК), ломбарды, бюро кредитных историй (БКИ), актуарии и другие — должны получить разрешение Банка России о допуске на финансовый рынок. В зависимости от вида организации это может быть как лицензия, так и включение сведений в реестр или аккредитация.

Для того чтобы проверить легальность работы финансовой организации на рынке (имеющиеся лицензии, виды деятельности), укажите в поисковой строке ее название, адрес, ИНН или ОГРН, регистрационный номер (для кредитных организаций и страховых компаний) или лицензию и нажмите «искать».

Если в справочнике по введенным реквизитам вы не смогли проверить информацию о наличии у организации лицензии, аккредитации или сведений о ее включении в реестр, то высока вероятность, что компания ведет свою деятельность без необходимого разрешения Банка России. Сотрудничество с ней может повлечь за собой нарушение ваших прав.

Статья 1.3 Обязанность банков возвращать клиентам средства, ранее переведенные мошенникам

С 25 июля 2024 года вступил в силу № 369-ФЗ, согласно которому клиенты банков будут защищены от мошеннических действий, связанных с переводами безналичных средств неизвестным.

Федеральный закон от 24.07.2023 № 369-ФЗ "О внесении изменений в Федеральный закон "О национальной платежной системе"

По заявлению клиента банк, разрешивший подозрительную транзакцию, обязан вернуть перечисленные злоумышленнику средства в полном размере и сделать это в течение 30 дней после получения заявления.

Но деньги подлежат возврату только в том случае, если: банк одобрил перечисление средств на счет мошенников, который находится в специальной базе Банка России «О случаях и попытках осуществления перевода денежных средств без согласия клиента»;

банк не уведомил клиента об осуществлении перевода без его согласия;

карта клиента была утеряна или ею воспользовались без ведома владельца, а клиент заранее предупредил об этом

банк.

Во всех остальных случаях финансовая организация имеет право не возвращать деньги.

Статья 1.4 Как правильно давать или брать деньги в долг

Прежде всего помните, что заём необходимо оформить юридическим образом.

Лучше всего это сделать через нотариуса.

Устные договоренности мало что значат в юридическом плане.

Обычный договор тоже не дает особых гарантий: его несложно признать недействительным.

В договоре необходимо четко прописать условия по процентам. Ставка может повышаться, если заемщик несвоевременно исполняет свои обязательства.

Важно помнить, что полученные проценты считаются материальной выгодой и с этой суммы нужно заплатить НДФЛ.

Если стороны договорились о беспроцентном займе, это стоит обязательно зафиксировать. Так как в определенных случаях, если в договоре займа ничего об этом не сказано, должен взиматься процент по ставке Центробанка.

Также в договоре необходимо прописать способ и порядок возврата основного долга и процентов — по частям или полной суммой.

Стоит уделить особое внимание ответственности заемщика на случай, если он не вернет деньги в оговоренные сроки.

То есть прописать штрафы, пени, неустойки.

Если человек, давший деньги займы, решит простить заемщику долг, это можно сделать через договор дарения.

Также долг можно закрыть соглашением о передаче имущества в качестве отступного.

Обязательства по договору займа можно заменить на обязательства по другому договору. Проще говоря, отработать долг, если у должника золотые руки.

Нужен и договор займа и расписка.

В договоре указывается сумма, срок, способ возврата долга и иные существенные условия, но сам по себе он, как правило, не подтверждает, что деньги фактически были переданы заемщику. А пока этого не произошло, договор, по сути, не действует.

Факт получения денег, особенно если это наличные, подтверждается распиской. При этом одной только расписки также недостаточно, поскольку зачастую в ней не указывается, на каких условиях деньги одалживаются.

Алгоритм:

1. Удостоверить договор займа,
2. Передать деньги,
3. Взять расписку об их получении.

Нотариус может засвидетельствовать подлинность подписи заемщика на расписке.

Лучше всего переводить деньги в безналичной форме, чтобы было видно движение средств. И взять выписку со сче-

та как дополнительный аргумент. Лучше сразу, так как, если заем выдается на длительный срок, банк может не сохранить первичные документы к тому моменту, когда они вам потребуются. Обычно в приложении банков выписку и чек можно сформировать за 3 прошедших года.

Статья 1.5 Безопасность сделки при строительстве частного дома

Утверждены новые условия кредитования по «Семейной ипотеке» при строительстве частного дома

Воспользоваться льготным кредитом при строительстве частного дома можно только при условии использования счетов эскроу.

Частные дома будут строить с эскроу.

Механизм эскроу-счетов распространяется на индивидуальное жилищное строительство (ИЖС) по договорам подряда.

Сегодня эскроу-счета широко применяются на рынке новостроек. Далее этот механизм был распространен на коттеджные поселки (малоэтажные жилые комплексы), которые состоят из индивидуальных жилых домов и возводятся девелоперской компанией.

С одной стороны, он дает финансовые гарантии гражданину — участнику строительства, с другой — открывает возможности проектного финансирования застройщику.

Строительство частных жилых домов должно будет осуществляться с использованием домокомплектов или типового проекта. Это позволит защитить средства граждан, поскольку использоваться будут счета эскроу, а значит, подряд-

чик получит оплату своей работы только после завершения.

Статья 1.6 Предупреждение кражи номера телефона, sim-карты, подмены сим-карты

Смартфоны прочно вошли в нашу жизнь: они не только обеспечивают нас сотовой связью, но и позволяют авторизоваться в интернет-сервисах. Наш номер мобильного телефона — это ключ доступа следующим системам:

Мессенджерам, электронной почте и социальным сетям
Криптокошелькам, онлайн-банку и системам управления активами (ценными бумагами)

Государственным системам (Госуслуги, ФНС)

Маркетплейсам, онлайн-магазинам и платформам объявлений.

Каждый владелец телефона или смартфона может оказаться жертвой атаки SIM Swapping — кражи номера телефона. Атаки на eSIM - мошенники перевыпускают их через взломанный личный кабинет оператора сотовой связи. Атака SIM-своперов наносит финансовый ущерб.

Большинство из перечисленных систем используют для авторизации или подтверждения операций SMS-коды, которые приходят на зарегистрированный в сервисе телефонный номер. Если перевыпустить SIM-карту с вашим номером телефона, то мошенники получают доступ к СМС и смогут по-

менять пароли от ваших аккаунтов в различных сервисах.

Как и любая мошенническая схема, подмена SIM-карты преследует определённые цели:

Хищение денежных средств

Лишение жертвы услуг связи - человек не сможет получать СМС и звонки от банков, операторов связи, полиции, родственников и друзей.

Получение конфиденциальной информации о жертве

Несанкционированный доступ на портал Госуслуг, в личный кабинет на сайте оператора связи, к электронной почте, мессенджерам и социальным сетям.

Требование выкупа за доступ к аккаунту.

Как предупредить кражи номера телефона, sim-карты, подмены сим-карты, защититься:

Меньше публичной информации о себе

Используя поддельные документы, участник преступной группы в офисе оператора связи меняет SIM-карту жертвы на новую, физическую либо eSIM (последнюю также можно оформить удалённо).

Мошенники собирают информацию об используемых Вами телефонных номерах и банковских счетах. После чего приобретаются поддельные документы на имя выбранного человека.

На заключительном этапе происходит несанкционированный доступ SIM-своперов к различным аккаунтам жертвы и хищение денег. Средства выводятся через дроп-сервисы или

покупку дорогостоящих товаров.

Замена SIM-карты — это обычная услуга оператора связи. Отличия только в том, как злоумышленники её осуществляют: либо самостоятельно, используя поддельные документы жертвы, либо вовлекают в преступную деятельность сотрудников оператора связи, либо применяют методы социальной инженерии в отношении самого абонента.

Надо отметить, что мобильные операторы внимательно отслеживают подозрительную активность по перевыпуску SIM-карт, а также мониторят действия своих сотрудников.

Помните:

Использование двухфакторной аутентификации через SMS-сообщения не является 100%защитой от мошенников. Ведь после перевыпуска SIM-карты с номером жертвы у неё отключаются все услуги связи.

ОнЛайн PUSH-уведомления: они привязаны не к SIM-карте, а к мобильному устройству.

Какие признаки могут указывать на то, что вашу SIM-карту «угнали»

От оператора связи приходит SMS-сообщение о смене SIM-карты;

Телефон теряет сеть, и никакие манипуляции не помогают;

На электронную почту поступают письма о смене паролей в различных сервисах;

Неожиданно вы узнаете, что разлогинились в основных

аккаунтах, таких как Google, Apple ID, Yandex, Mail.ru.

Неожиданное SMS-сообщение о смене условий вашего тарифного плана, заказе детализации звонков, подключении переадресации, появление посторонних устройств в используемых вами мессенджерах.

Как минимизировать риски...

Если вы всё же стали жертвой атаки SIM-своперов, то знайте, что в первые 24 часа после перевыпуска SIM-карты операторы связи блокируют или ограничивают услуги отправки и получения SMS-сообщений, в том числе в кредитно-финансовые организации.

Поэтому некоторые сервисы будут недоступными.

И у вас есть ровно сутки, чтобы восстановить доступ к своей SIM-карте без серьёзных последствий. Сделать это поможет личный визит в офис оператора связи либо звонок на горячую линию.

Полностью защититься от этой мошеннической схемы, к сожалению, невозможно. Но есть несколько простых правил, которые помогут свести риски к минимуму:

Постоянно помните про цифровую гигиену. Не выкладывайте в публичный доступ (даже в облачные сервисы) сканы своих документов — это должно быть аксиомой.

Оформите у оператора связи услугу запрета действий по нотариальной доверенности.

Не будут лишними использование биометрических данных для доступа к устройству, а также установка PIN-кода

к SIM-карте.

Не игнорируйте сервисные сообщения от оператора связи.

Хорошим способом защиты будет выпуск отдельной SIM-карты для регистрации и использования банковских приложений и государственных сервисов. Конечно, о её существовании никто не должен знать.

По возможности откажитесь от SMS-аутентификации.

Используйте PUSH-уведомления или отдельные приложения-аутентификаторы.

Статья 1.7 Финансовая подушка безопасности

Жить без финансовой подушки опрометчиво.

Финансовая подушка безопасности — это резерв денег для разных непредвиденных ситуаций.

Создать подушку безопасности не сложно

1. Определите свой расход в месяц (ежемесячные траты)
2. Поставьте цель создать подушку безопасности на несколько месяцев (3,6,12 месяцев). Чем больше подушка, тем больше Вы в безопасности перед определенными непредвиденными трудностями. Подушки на 3 месяца может хватить, чтобы перейти на другую хорошую работу. Подушки на 6 месяцев, чтобы оправиться после болезни и дорогого лечения.
3. Рассчитайте нужную сумму своей финансовой подушки безопасности = количество месяцев*сумму ежемесячных трат.
4. Начните откладывать на финансовую подушки безопасности.

На 100% никто не уверен, что будет завтра.

Статья 1.8 Не попадайтесь на дипфейк

Дипфейк - цифровая копия реального человека

Мошенники взламывают аккаунт, берут из него фото, видео- и аудиозаписи человека и загружают их в нейросеть. Далее искусственный интеллект (ИИ) создает дипфейк — цифровой образ, максимально похожий на свой прототип. Преступники записывают ролик с виртуальным двойником. Он говорит, что оказался в беде и просит помочь ему деньгами. Это ложное видео мошенники рассылают родным, друзьям и коллегам человека и добавляют свои реквизиты для перевода денег.

Что нужно знать, чтобы не попасть на дипфейк-технологическое чудо:

Подделку можно распознать по некоторым признакам: монотонному голосу, несвойственной человеку мимике или интонациям, дефектам звука и изображения.

Но даже если видео не вызывает у Вас сомнений, стоит настороженно относиться к просьбам о деньгах и помнить, что аккаунт могли взломать.

Прежде чем переводить какие-то суммы, лучше позвонить знакомому и убедиться, что ему действительно нужна

помощь. Если нет возможности поговорить по телефону или лично, в сообщении задайте человеку вопрос, ответ на который знает только он!

Глава Минцифры М. Шадяев предложил создать в России приложения, которые будут распознавать дипфейки в режиме реального времени. По его словам, использование технологии дипфейк при совершении преступления может статьотягчающим обстоятельством. Об этом заявлено на форуме «Кибербезопасность в финансах»

С коллегами из правоохранительных органов Минцифры обсуждает вопрос того, что использование дипфейков станет отягчающим обстоятельством при совершении преступлений.

Но это планы. А сегодня Ваша безопасность в Ваших руках.

Статья 1.9 Не попадайтесь на фишинг

До Нового года или до 8 марта меньше 50 дней?

Количество распродаж растет.

Мошенники стали активнее!

Лучше предупредить!

Фишинг (phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.

Как это происходит: мошенники от имени организаций или конкретных людей рассылают пользователям сообщения по электронной почте, в социальных сетях и мессенджерах. В письмах содержится ссылка на фишинговый сайт, где расположена форма, в которую предлагается внести личные данные. Если пользователь сделает это, его данные попадут в руки мошенников.

В сезон распродаж самый популярный способ обмана — фишинг. Злоумышленники создают сайты, похожие на популярные бренды. Жертв они призывают ввести пользовательские данные — и таким образом мошенники получают имена учетных записей, пароли, номера кредитных карт или другие личные данные.

Советы по безопасности в канун распродаж:

Актуализируйте информацию в личном кабинете маркетплейсов и интернет-магазинов, удалите старые аккаунты.

Не забудьте установить двухфакторную аутентификацию.

Прежде чем вводить конфиденциальные данные, убедитесь, что вы находитесь на официальных площадках. Проверьте адреса страниц.

Устанавливайте приложения только из проверенных источников.

Не доверяйте подозрительным сообщениям из рассылок и не переходите по незнакомым ссылкам.

Статья 1.10 Не допускайте виртуального клона Вашей банковской карты

Виртуальный клон Вашей банковской карты – новое у мошенников!

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.