



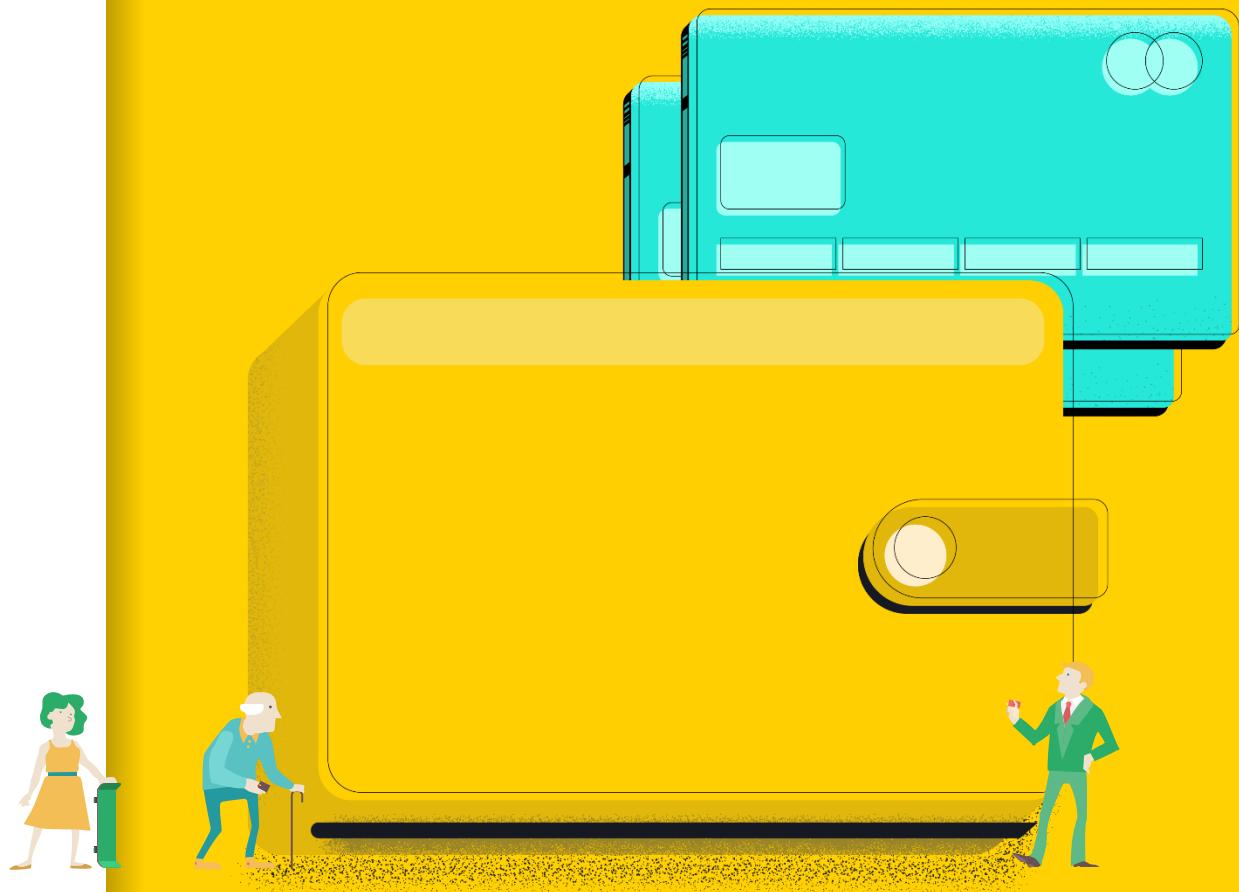
ДЕПАРТАМЕНТ
ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ
ГОРОДА МОСКВЫ



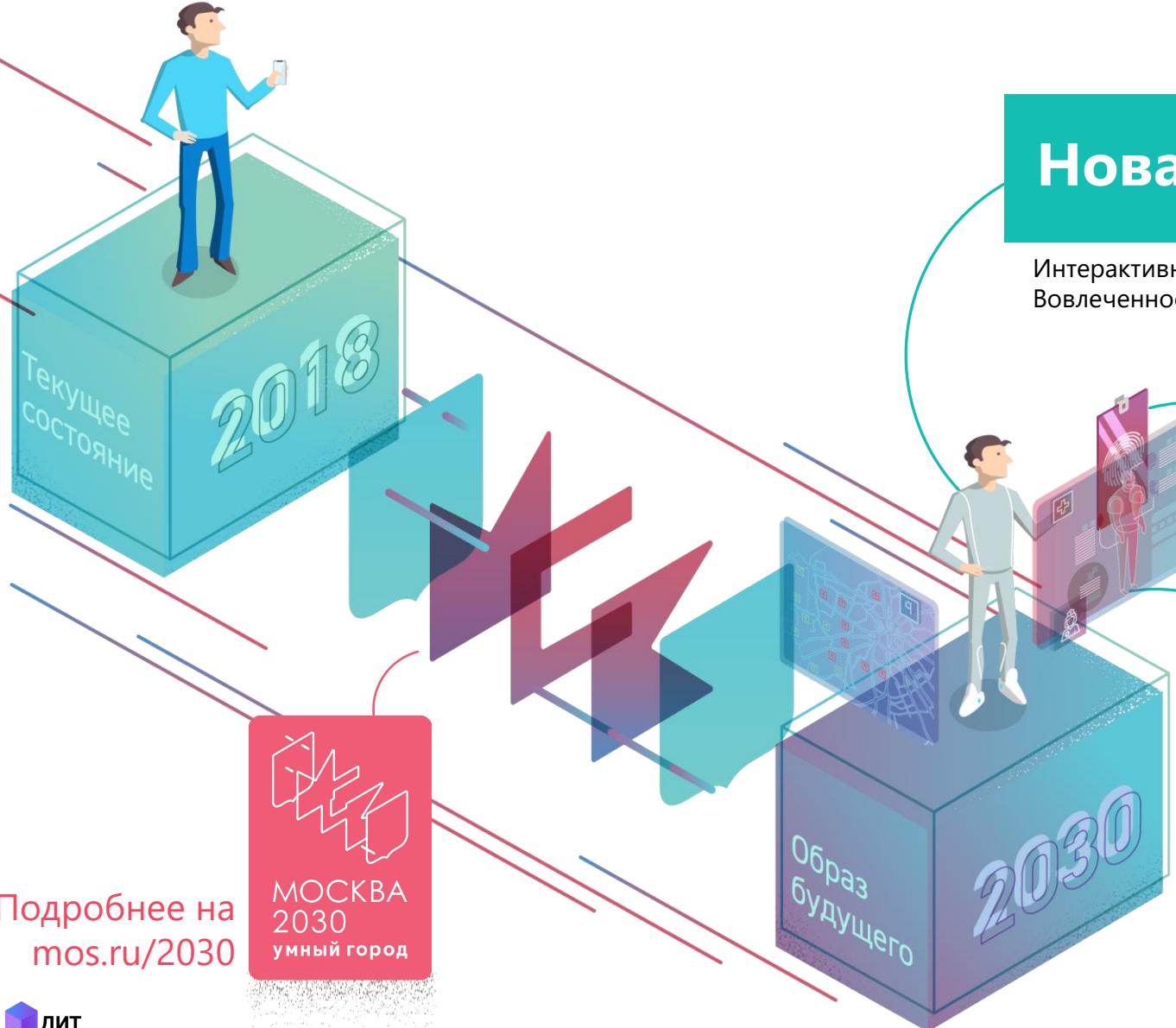
«Использование электронных платежных сервисов в Москве»

Ноябрь 2018

Яндекс Деньги



Умный город для жителей



Подробнее на
mos.ru/2030

Новая модель потребления

Интерактивное потребление **Any Time, Any Place, Any Device**
Вовлеченность в создание продуктов и услуг, управление городом

Новое поведение жителей

Жители будут инвестировать в себя – здоровье, образование, общение, семья т.д.

**24 часа не меняются,
меняется их наполнение**

Экосистемы онлайн-платежей

10 лет назад

50 минут в месяц



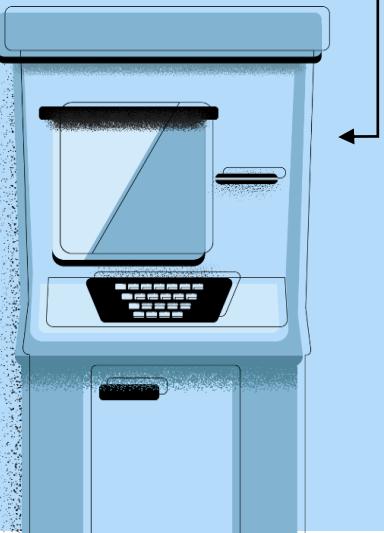
Банк

Салон связи

Терминал оплаты
в магазинах
Связь, ЖКХ

ЖКХ, квитанции,
штрафы, переводы

Связь



Сейчас

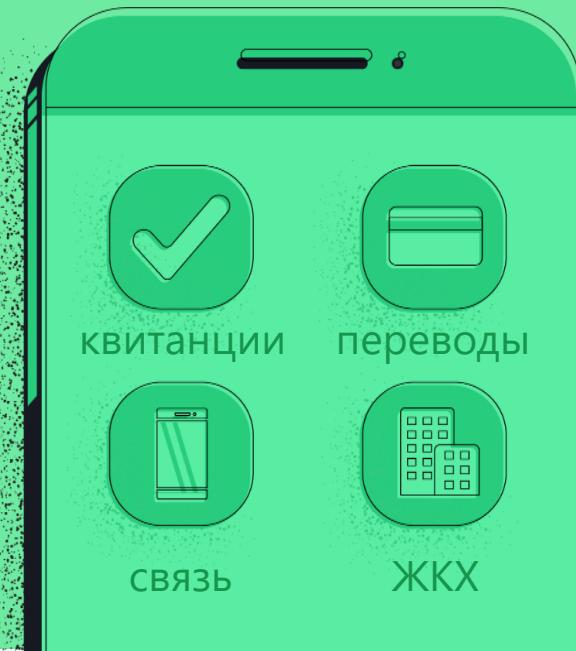
3 минуты в месяц



На работе

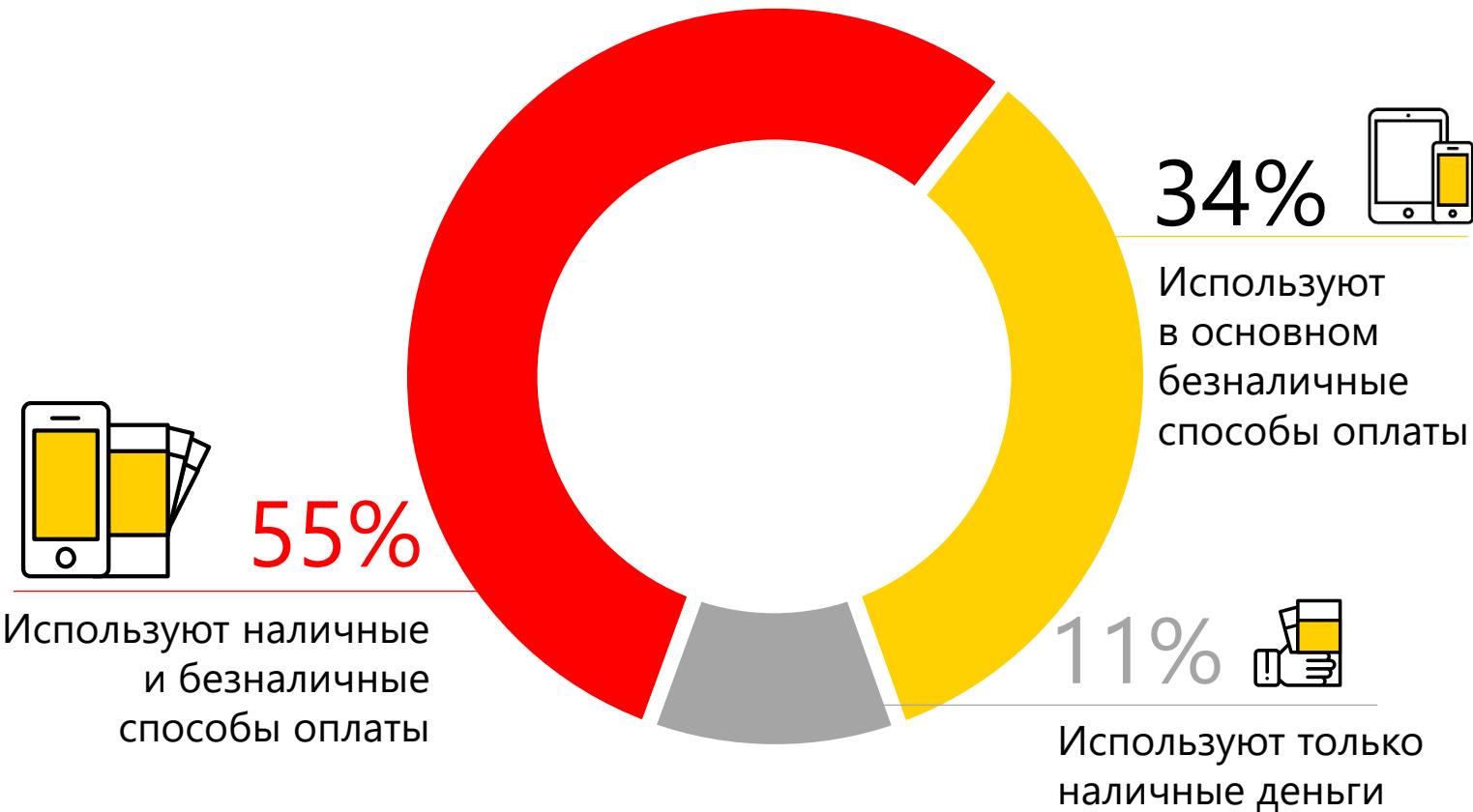
В метро

Дома

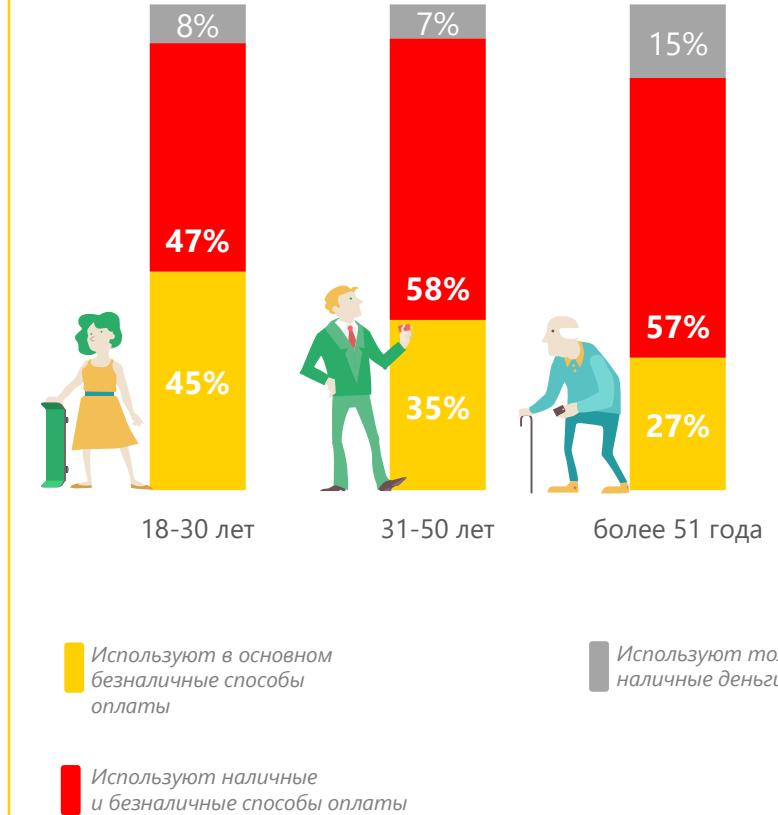


Популярность способов оплаты товаров и услуг среди жителей Москвы

Использование наличных и безналичных способов оплаты

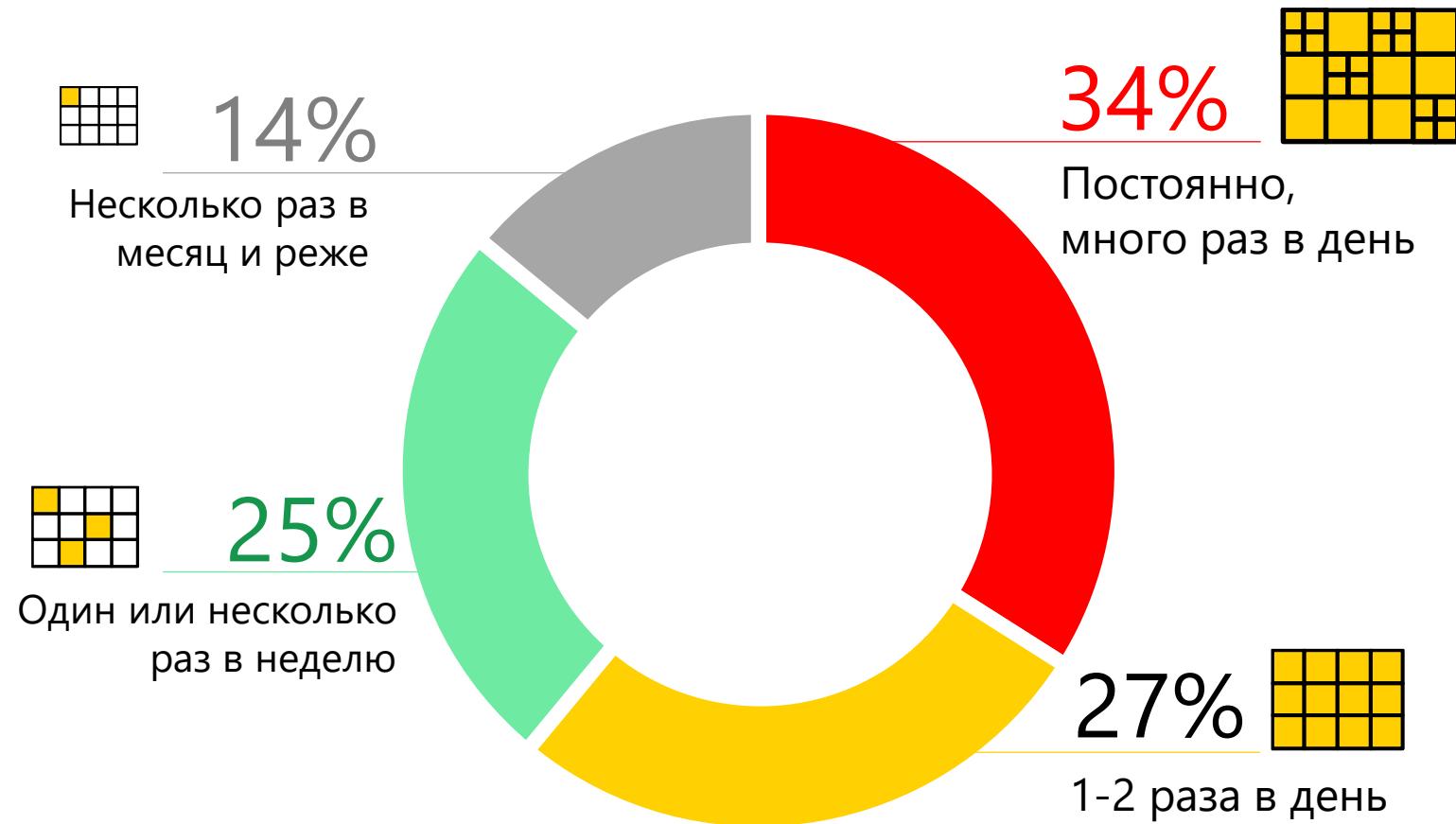


По возрастным сегментам:

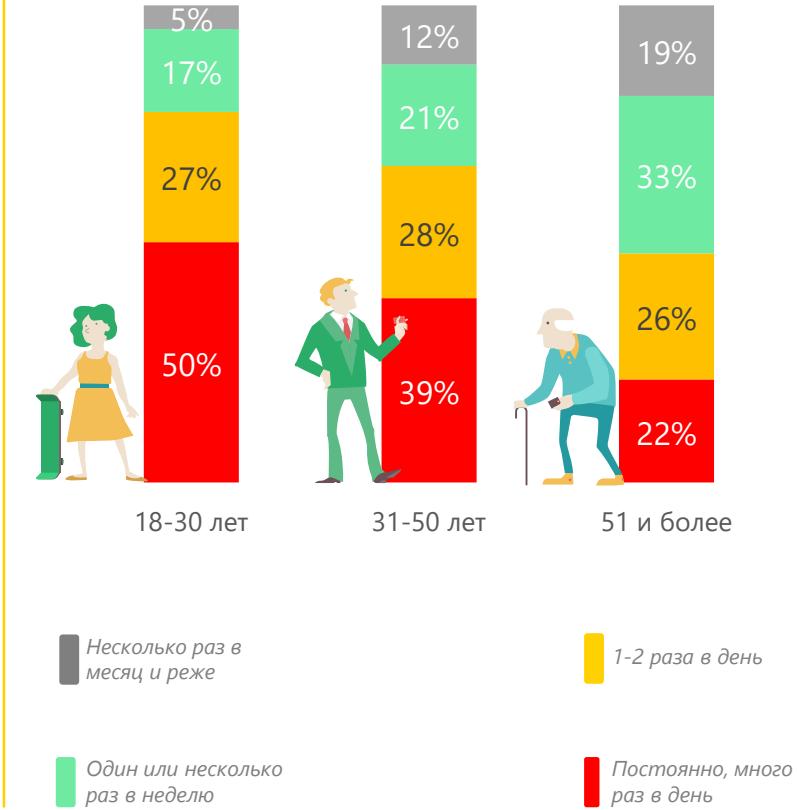


Частота использования безналичных способов оплаты

Частота совершения безналичных платежей среди жителей
Москвы, использующих данный способ оплаты

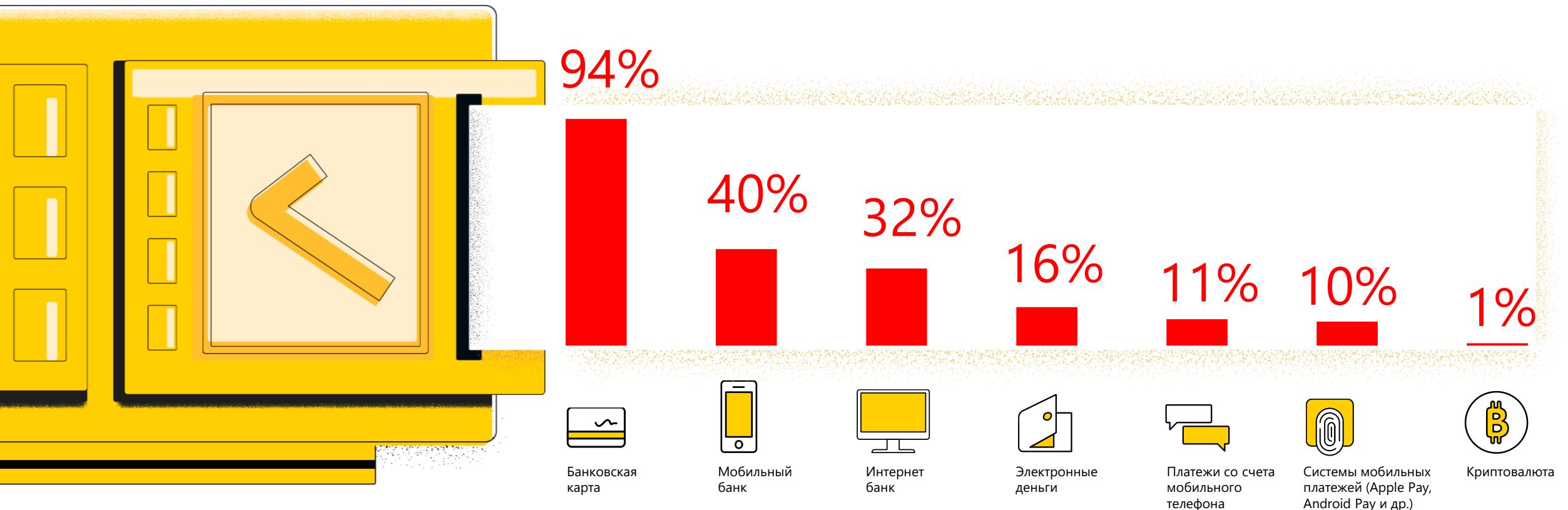


По возрастным сегментам:



Способы безналичной оплаты товаров и услуг¹

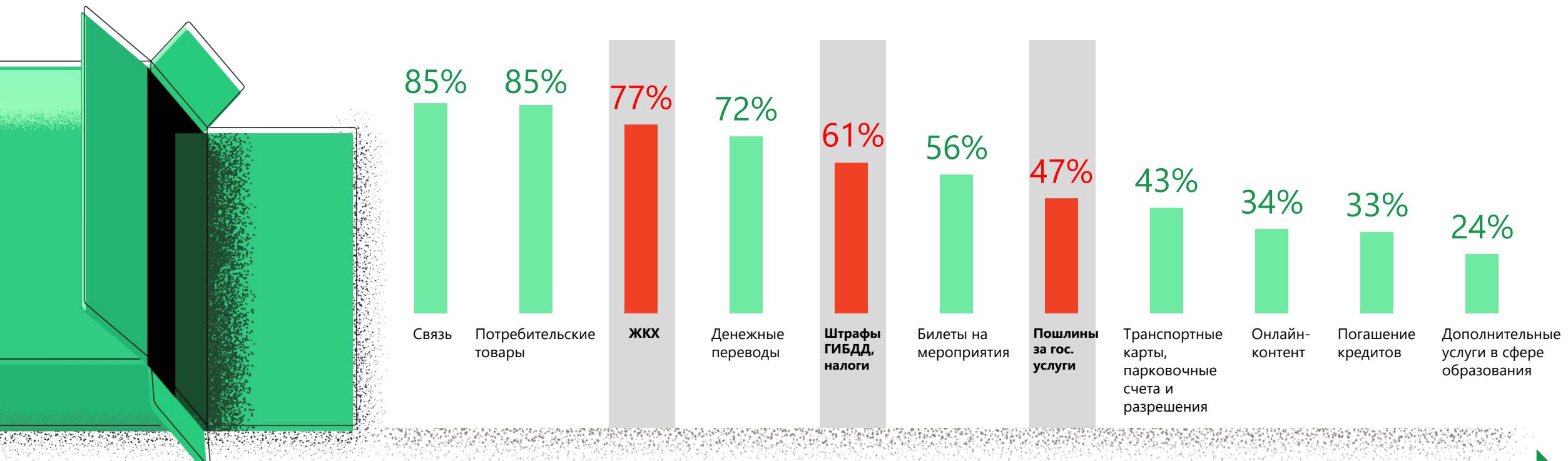
Использование безналичных способов оплаты, %



¹ Среди москвичей использующих безналичные способы оплаты

Товары и услуги для покупки которых москвичи используют безналичные способы оплаты

Категории оплаты товаров и услуг, %



Госуслуги –
одни из самых популярных для безналичной оплаты типов услуг

Городские платежи москвичей. Как вырос объем онлайн-платежей по сравнению с 2015 годом

Рост объема платежей, совершенных в течение первых 9 месяцев 2015 и 2018 гг. жителями Москвы с кошелька или карт Яндекс.Денег на любых городских онлайн-ресурсах, а также любым другим способом — на сайте Яндекс.Денег



¹ оплата по счету от любого юр. лица или ИП, у которого есть счет в банке (например, оплата капремонта, секций, кружков, детсадов)

² оплата штрафов ГИБДД, налогов, квитанций в пользу бюджетных учреждений

В целом объем онлайн-платежей вырос на 25% по всем направлениям городских платежей.

Электронные деньги

(проверка и оплата штрафов ГИБДД, налогов, ЖКУ, а также другие городские платежи; пополнение транспортных карт, оплата квитанций, выдача и погашение кредитов, займов, денежные переводы людям и организациям, выставление счетов, инструменты краудфандинга, скидки и офферы, покупка контента, инвестиции)

Онлайн- и мобильные банки

(оплата штрафов, налогов, ЖКУ и других бытовых услуг, пополнение транспортных карт, оплата квитанций, выдача, И погашение кредитов, денежные переводы людям и организациям, обмен валют, выставление счетов, покупка контента, инвестиции)

Экосистемы онлайн-платежей

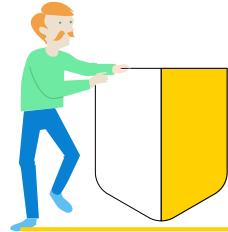
Государственные сервисы приема платежей

(проверка и оплата штрафов, ЖКУ, выдачи документов, госпошлины, школьные карты «проход и питание», оплата квитанций за детские кружки и секции, сотовая связь)

Соцсети и мессенджеры

(экосистемы онлайн-платежей только формируются)

Возможности электронных денег



Безопасность

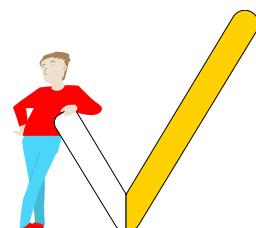
Привязка карты другого банка для безопасной оплаты в интернете

Система защиты с использованием искусственного интеллекта

Двухфакторная авторизация

Одноразовые пароли в смс и подтверждение оплаты через пуш-уведомления

Авторизация по отпечатку пальца



Удобство платежей

Бесшовная оплата товаров и услуг на сайтах — без ввода платежных данных

Выпуск банковской карты

Бесконтактные платежи

Денежные переводы

Платежи по QR-коду: оплата квитанций и товаров

Напоминания и автоплатежи



Дополнительная выгода

Инструменты для сбора денег: формы, кнопки, готовые страницы yasobe.ru

Мгновенный кэшбэк за каждую покупку онлайн и офлайн

Специальные офферы: ежедневные и дополнительные за каждый платеж,

подобранные под каждого конкретного пользователя

Инвестиции: сервис [Yammī](#) на базе технологий робоэдвайзинга



Экономия времени

Открытие счета и выпуск карты без визитов в отделение

Мгновенный выпуск виртуальной карты для онлайн- и офлайн-оплаты

Широкий набор методов идентификации, в том числе онлайн

Технологии и дополнительные услуги сервисов безналичной оплаты

Услуги и технологии при использовании безналичного способа оплаты среди москвичей, %



Доля москвичей, использующих технологии и дополнительные услуги сервисов безналичной оплаты по возрастным группам и полу, %

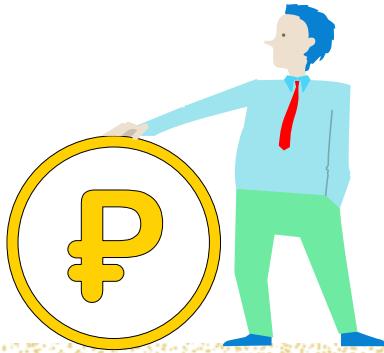


Безналичные способы оплаты: почему используют и какие проблемы возникают



70% москвичей, использующих безналичные способы оплаты, не сталкивались с проблемами при оплате товаров и услуг.

Дополнительные выгоды безналичной оплаты: опыт Яндекс.Денег

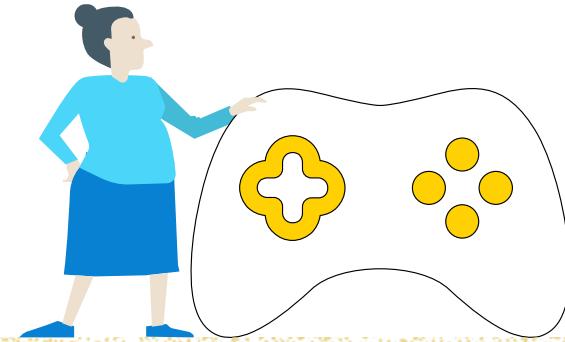


Кэшбэк

Каждый участник программы лояльности Яндекс.Денег получает часть денег, которые заплатил за определенные товары и услуги.

В среднем один клиент получает кэшбэк:

- 7 раз за оплату в категории «Супермаркеты»;
- 5 раз в категории «Кафе, рестораны».



Выгоды геймификации

Клиенты получают дополнительные бонусы за целевые действия, такие как выпуск карты, идентификация счета, приглашение друзей.

80% всех выпущенных в рамках геймификации карт и пройденных идентификаций приходится на клиентов, которые давно с сервисом.



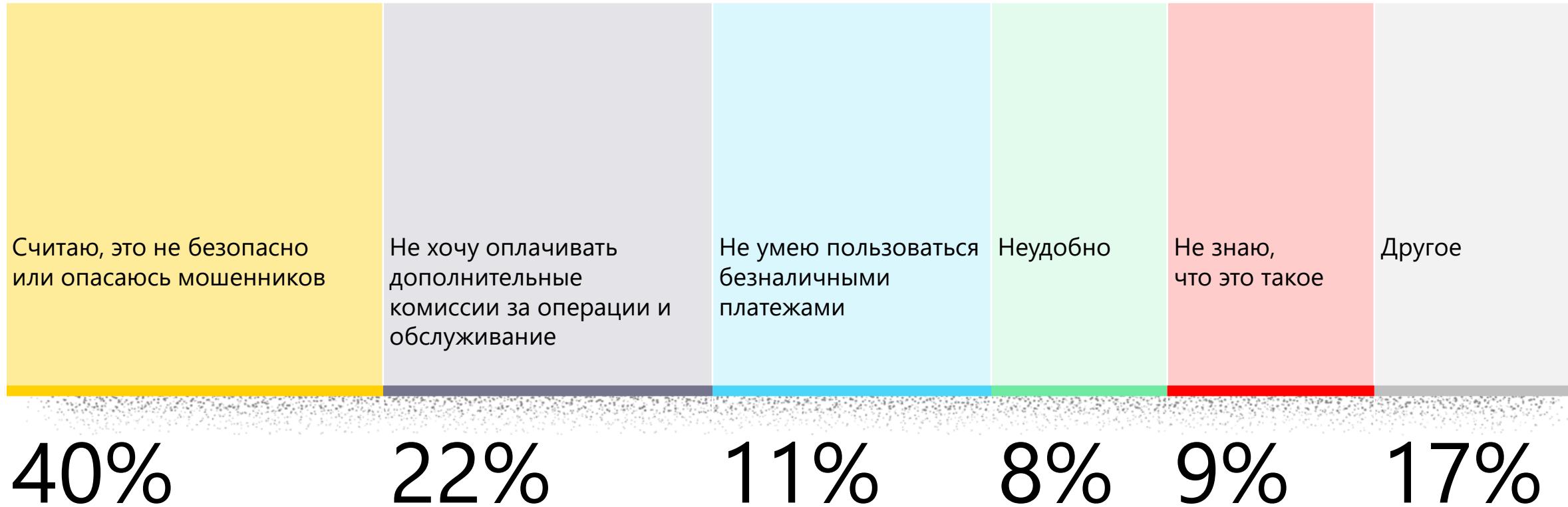
Специальные офферы

Персональные скидки и бонусы в интернет-магазинах, подобранные сервисом с использованием методов машинного обучения.

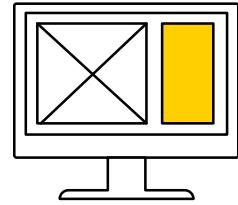
В среднем 6% увиденных предложений пользователи принимают и начинают платить чаще, чем остальные, а их средний чек вырастает примерно на 4%.

Опасения использования безналичных платежей

Почему Вы не пользуетесь безналичными платежами
(стараетесь всегда платить наличными)?

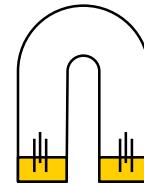


По данным ЦБ РФ, около 90% всех случаев мошенничества с электронными платежами связаны с двумя причинами: воздействие вредоносного кода (вируса) или злоупотребление доверием



Фишинговые сайты, а также компрометация счета

Поддельные сайты, похожие на интернет-магазины, популярные финансовые или другие онлайн-сервисы, в том числе почтовые. Злоумышленники через них собирают данные о платежных средствах, либо персональные и авторизационные данные, либо перенаправляя платежи в свою пользу



Социальная инженерия, в том числе покупки у недобросовестных физических лиц

При злоупотреблении доверием используются не компьютерные, а социальные технологии. Мошенник делает ставку на доверчивость или неопытность жертвы.



Вирусы на компьютерах и Android-устройствах

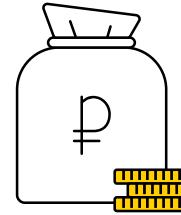
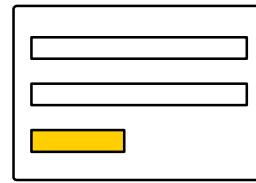
Вредоносные ссылки в SMS
Установка зараженных приложений

РЕШЕНИЕ

Если платите на неизвестном сайте, обращайте внимание на адекватность ресурса (заполненность, наличие контактов, работающие телефоны), так как сайт может быть копией настоящего.

В онлайн-расчетах требуется такая же осмотрительность, как в обычной жизни. Информация о ваших платежных средствах, пинкоды и смс-пароли — секретны. Настоящий сотрудник банка никогда ее не спросит

Антивирус не только на компьютере, но и на мобильных устройствах



Миф 1: платежи без пароля опасны

Необходимость вводить пароль устанавливается банком, выпустившим карту или электронное средство платежа, — технология 3DS. Операции, не требующие 3DS, не менее безопасны, так как пользователь вправе оспорить такую транзакцию. 3DS может не участвовать в операции, если от этого отказалась торговая точка (а значит она принимает риски мошенничества на себя) или банк-эквайер.

Миф 2: бесконтактные платежи можно перехватить

Самый устойчивый миф — о мошеннике со специальным терминалом, который списывает в метро деньги с наших карт и телефонов, в которых настроены мобильные бесконтактные сервисы X-Pay. Почему это миф:

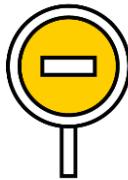
Когда мы подносим карту или смартфон к терминалу, задействуются зашифрованные динамические коды безопасности: они новые в каждой транзакции и должны быть подтверждены принимающим карту устройством или эмитентом в режиме реального времени.

Миф 3: электронные деньги легко украсть

Электронные счета защищены так же надежно, как и банковские — по тем же технологиям и требованиям регулятора. Платежные сервисы проходят ту же сертификацию, что и банки, а для подтверждения операций давно уже предлагают не постоянные, а одноразовые смс-пароли и пушки. Сервис Яндекс.Деньги, например, имеет сертификацию PCI DSS, ни разу не был взломан и использует передовую антифрод-систему на базе машинного обучения.

Безопасность онлайн-платежей растет

%



Объем мошенничества относительно всего объема операций по банковским картам измеряется тысячной долей процента (данные ЦБ).

Начиная с 2017 года, объем высокотехнологичных хищений снижается. По данным ФИНЦЕРТ и Group IB, объем несанкционированных операций по банковским картам сократился на 10,6%, хищений с помощью Android-тロjanов — на 77%.

Один из немногих видов высокотехнологичного мошенничества, который процветает, — фишинг, то есть подмена онлайн-ресурса на мошеннический.

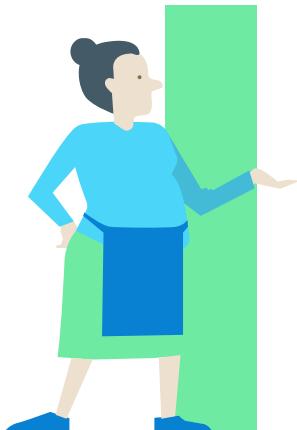
Онлайн-оплата **ничуть не опасней** расчетов в обычной жизни.

Жизненные ситуации, в которых требуется оплата наличными

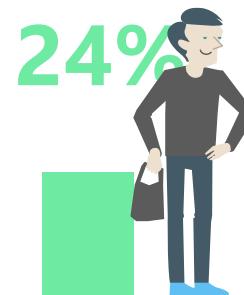
С какими ситуациями, когда приходилось оплачивать товар или услугу наличными деньгами Вы сталкивались?

83%

«Ой, мы карточки не принимаем!»



24%



11%



Почти каждый житель столицы сталкивался с проблемами отсутствия возможности оплатить товары или услуги безналичным способом

9%



8%



7%



4%



3%



Принимаются только наличные

Не работает сервис/сбои в работе

Продавец настойчиво просит оплатить наличными

Возникновение дополнительные комиссии

Долгое ожидание возврата денежных средств

Предоставление скидки

Опасаюсь платить безналичными в новых местах

Покупали в подарок

«А у нас сегодня терминал не работает...»

Комиссия

- Переводы с кредитных карт
- Оплата квитанций



И так, и так

- ЖКУ
- Штрафы ГИБДД
- Денежные переводы
- Снятие наличных с электронных средств платежа



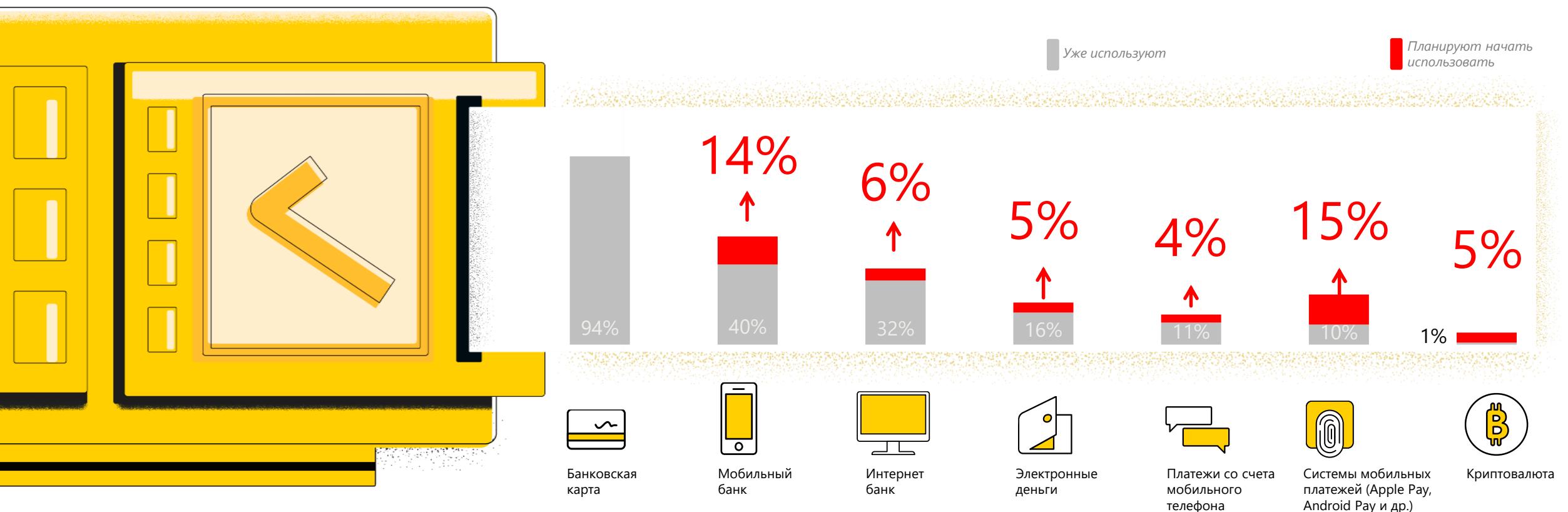
Без комиссии

- Сотовая связь
- Телефония
- Интернет
- Налоги
- Транспортные карты
- Платежи в интернет-магазинах
- Платежи за онлайн-услуги
- Покупки контента и игр
- Оплата с привязанных к сервисам карт



Способы безналичной оплаты товаров и услуг¹

Использование безналичных способов оплаты

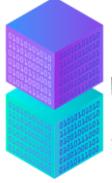


¹ Среди москвичей использующих безналичные способы оплаты



ДЕПАРТАМЕНТ
ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ
ГОРОДА МОСКВЫ

Яндекс Деньги

 **ДИТ**
АНАЛИТИКА
moscowanalytics.ru

 /ditmos

 @ditmos

 mos.ru/dit

Приложение 1.

Угрозы безналичных способов оплаты

Фишинговые сайты

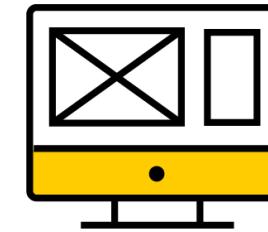
Один из самых популярных способов финансового онлайн-мошенничества и единственный вид кибермошенничества, объем которого в России за последний год вырос (по данным Group IB, на 6%)

Проблема:

Злоумышленники делают сайты, похожие на интернет-магазины, облачные ресурсы, популярные финансовые (чаще всего переводы с карты на карту) или другие онлайн-сервисы, в том числе почтовые, или перехватывают пользователей, которые заходят на настоящие ресурсы, собирая либо данные об их платежных средствах, либо персональные и авторизационные данные, либо перенаправляя платежи в свою пользу.

Выход:

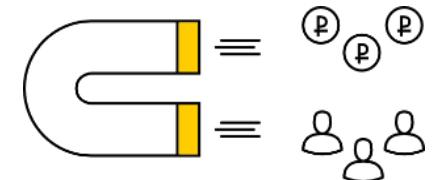
если платите на неизвестном сайте, обращайте внимание на адекватность ресурса (заполненность, наличие контактов, работающие телефоны). Если зашли на знакомый ресурс, перед оплатой убедитесь, что адрес сайта не изменился и вас по дороге не перехватили злоумышленники.



Социальная инженерия в онлайн-платежах

По данным ЦБ РФ, около 90% всех случаев мошенничества с электронными платежами связаны с двумя причинами: воздействие вредоносного кода (вируса) или злоупотребление доверием.

При злоупотреблении доверием используются не компьютерные, а социальные технологии. Мошенник делает ставку на доверчивость или неопытность жертвы



Мошенник — «сотрудник банка»:

по телефону самозванец пытается выведать персональную информацию якобы для обновления данных в системе.

Мошенник — покупатель:

при размещении объявления о продаже чего-либо пользователи часто озвучивают потенциальному «покупателю» номер карты и даже пароль из смс, если им говорят «назовите код из смс, чтобы деньги вам зачислились».

Мошенник — продавец:

если частное лицо предлагает купить что-то онлайн сильно дешевле, чем в других местах — скорее всего, это мошенничество. Чаще всего таким образом люди оплачивают, но не получают смартфоны, ювелирные изделия, дополнительный сверхход от различных «акций, облигаций, биржевых операций».

Мошенник — «друг»:

если аккаунт вашего друга оказался взломан, от его имени может прийти сообщение в стиле «переведи мне срочно 500 рублей, потом верну».

Выход:

в онлайн-расчетах требуется такая же осмотрительность, как в обычной жизни. Информация о ваших платежных средствах, пинкоды и смс-пароли — секретны. Настоящий сотрудник банка никогда ее не спросит, а получение денег в подтверждении не нуждается. Если собеседник предоставил номер телефона, нeliшним будет проверить в интернете код — часто мошенники используют телефон родного региона, а не того, где они должны находиться исходя из контекста. Осмысливайте всю поступающую к вам информацию — будьте критичны.

Проблема:

Чаще всего устройства заражаются через смс с вредоносной ссылкой, при установке зараженных приложений из неофициальных репозиториев, использование поддельных сервисов переводов с карты на карту. Все данные, которые пользователь вводит в зараженное устройство, могут быть перехвачены.

Выход:

использовать антивирусы не только на компьютере, но и на смартфона\планшете, следить за актуальностью, не устанавливать приложения из неизвестных источников, не открывать ссылки, пришедшие от незнакомого отправителя.



Проблема:

мошенники создают ненастоящие интернет-магазины или онлайн-сервисы, которые выглядят как настоящие. Там можно найти популярные смартфоны по сниженной цене, другую электронику с большой скидкой, брендовые вещи, выгодный курс обмена криптовалют. Такие ресурсы всегда требуют онлайн-предоплаты, но товар, как правило, не привозят, или сделку не проводят.

Выход:

если в процессе оплаты вы видите указание, что совершаете «перевод», а не «платеж», значит продавец принимает деньги на счет физического лица. Тогда как по закону коммерческую деятельность, к которой относится торговля электротоварами, могут вести только юридические лица. К сожалению, если деньги уже уйдут, вернуть их можно будет только через суд, так как для банка такая операция – расчеты между двумя частными лицами, в отношении которых кредитная организация не сможет вмешаться по закону. Та же ситуация с обменниками: деньги, переведенные физлицу, по обращению в банк вернуть не получится – только через правоохранительные органы, которые решат, легитимны ли требования о возврате денег.



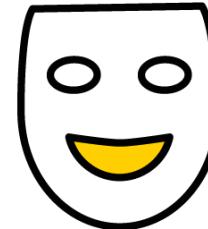
Компрометация счета

Проблема:

В интернете люди часто продают друг другу товары собственного изготовления или бывшие в употреблении, а также договариваются о совместных закупках. Нередко пользователи просят друг друга прислать номер карты или даже фото. Проблема в том, что для платежей во многих интернет-магазинах этой информации достаточно, чтобы деньги списались. Да, владелец карты потом сможет оспорить такую операцию, но время и силы будут потрачены.

Выход:

никогда не называть и не показывать номер карты – и тем более карту целиком. Если незнакомый человек хочет перевести вам деньги, предложите сделать перевод по номеру телефона или виртуальной карты, которую можно тут же выпустить и закрыть после получения денег, или используйте сервис выставления счета. В таком случае вы сможете прислать ему ссылку, по которой будет несколько удобных методов оплаты, а ваши платежные данные будут надежно защищены.



Приложение 2.

Использование безналичных способов для
оплаты товаров и услуг

Банковская карта

Использование банковской карты для оплаты категорий товаров и услуг, % жителей Москвы



Среди всех жителей Москвы

Платят безналичным способом оплаты

Платят банковской картой

Интернет-банк

Использование интернет-банка для оплаты категорий товаров и услуг, % жителей Москвы



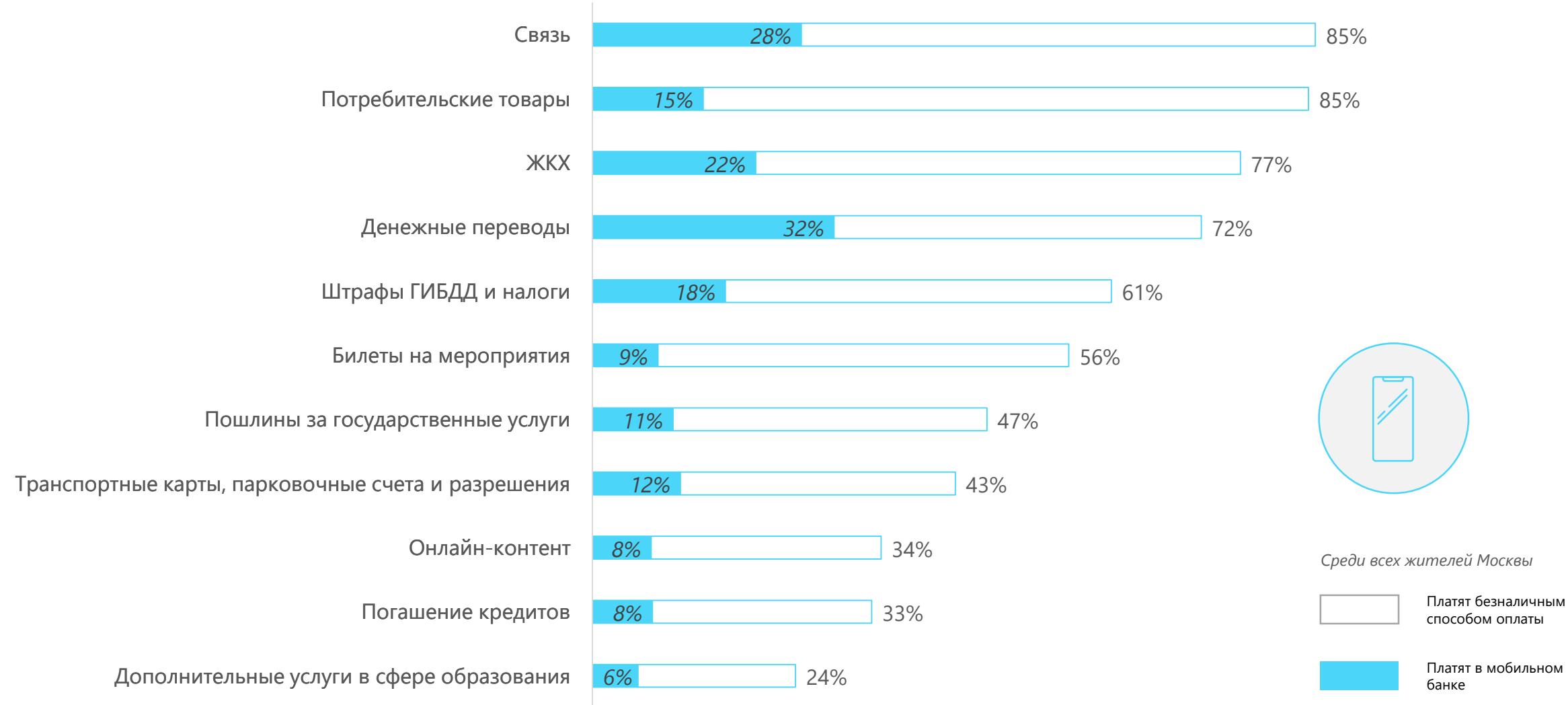
Среди всех жителей Москвы

Платят безналичным способом оплаты

Платят в интернет банке

Мобильный банк

Использование мобильного банка для оплаты категорий товаров и услуг, % жителей Москвы



Платежи со счета мобильного телефона

Использование счета мобильного телефона для оплаты категорий товаров и услуг, % жителей Москвы

