KASPERSKY lab

Безопасность в условиях разнообразия устройств: что думают российские пользователи

Август 2013 г.

Введение

Мир персональных цифровых устройств постоянно меняется. Появляются новые модели гаджетов, онлайн-сервисы, приложения. Все больше люди полагаются на свои компьютеры, смартфоны и планшеты: доверяют им хранение ценной информации, выполняют с их помощью важные задачи. Электронные устройства изменили жизнь людей. Эти же изменения влияют и на то, каким образом должна осуществляться защита пользователей от множества существующих киберугроз.

«Лаборатория Касперского» постоянно работает над улучшением качества защиты в своих продуктах. Для того чтобы решения компании максимально точно соответствовали потребностям людей и умели дать адекватный ответ тем угрозам, с которыми им приходится сталкиваться, «Лаборатория Касперского» ежегодно совместно с международными аналитическими агентствами проводит опросы пользователей по всему миру. Из этих опросов мы узнаем, что люди думают об информационной безопасности, с какими угрозами им приходилось встречаться и что они предпринимали для своей защиты.

Летом 2013 года совместно с международным аналитическим агентством B2B International «Лаборатория Касперского» провела новый опрос, в котором приняли участие 8605 человек из 19 стран Северной и Южной Америки, Европы, Ближнего Востока и Азиатско-Тихоокеанского региона. Все участники опроса старше 16 лет, более трети из них являлись родителями как минимум одного ребенка, абсолютное большинство является пользователями Интернета и различных мобильных устройств. В России было опрошено 1006 человек.

Основные выводы

Согласно результатам опроса, основная тенденция, характерная для сферы потребительской электроники за последние 12 месяцев, заключается во все большем распространении разнообразных устройств: как классических стационарных ПК, так и новейших смартфонов и планшетов.

Подобная «мудьтигаджетность» формирует новую модель использования электронных устройств, в рамках которой люди применяют мобильные устройства наряду с обычными компьютерами. Смартфоны и планшеты – легкие и мощные – позволили людям удобно общаться и делиться друг с другом информацией, загружать мультимедийный контент, пользоваться интернет-сервисами.

По данным опроса, в среднем в России на одно домохозяйство приходится сегодня около 3,7 различных устройств, которые находят самые разные применения. Чаще всего это работа с финансами:

- в среднем 81% россиян использует то или иное устройство для проведения финансовых операций;
- 54% респондентов регулярно пользуются электронными кошельками и платежными системами.
- 57% и 56% владельцев электронных устройств в России используют их для онлайн-шопинга и интернет-банкинга, соответственно.

Использование онлайн-сервисов, работающих с личными финансами людей, сопровождается риском атак со стороны финансовых злоумышленников. И в целом пользователи понимают опасность подобных и других киберугроз, о чем свидетельствуют результаты опроса. Например:

- 75% респондентов сообщили, что создают разные пароли для финансовых сервисов в Интернете и своих учетных записей в электронной почте или социальных сетях;
- в среднем более 68% россиян считают, что их электронное устройство (на любой платформе за исключением ОС от Apple) требует дополнительной защиты. Для пользователей устройств Apple, как мобильных, так и стационарных, этот показатель превышает 44%.

Одновременно велика доля и тех пользователей, кто уделяет недостаточно внимания безопасности своих устройств, либо излишне уверен в безопасности третьих сторон:

- 36% респондентов в России не предпринимают никаких мер безопасности при использовании публичных сетей Wi-Fi;
- 34% уверены, что сайты, которыми они пользуются, достаточно хорошо защищают личные пароли пользователей;

- 47% россиян уверены, что бесплатные защитные средства, которые предлагает банк, обеспечат безопасность любых их операций онлайн.

При этом, несмотря на сравнительно ответственный подход пользователей к информационной безопасности, число людей, подвергшихся вредоносным атакам значительно, а их последствия выливаются в реальные финансовые потери:

- 45% российских пользователей сталкивались с вредоносными атаками;
- Каждая пятая из таких атак приводила к утечкам персональных данных;
- 74% россиян сталкивались хотя бы с одним инцидентом, связанным с попыткой похищения финансовой информации;
- Средний убыток от одной атаки составил 76 долларов США на человека.
- 72% жертв финансовых атак в России не смогли получить полное возмещение похищенных средств.

В ходе опроса российские респонденты отвечали и на другие вопросы, связанные с Интернетом, мобильными устройствами и компьютерами. В частности, они делились своим мнением о киберугрозах, о том, как чаще всего хранят пароли и защищают персональную информацию, а также о проблемах безопасности детей в Интернете. Более подробно об этом – в совместном исследовании B2B International и «Лаборатории Касперского».

Активности в Сети: от шопинга до передачи информации

Социальные сети и сервисы для общения пользуются наибольшей популярностью у россиян

	Любое устройство	Настольный ПК / Ноутбук	Планшет	Смартфон	Любое моб. устройство
Социальные сети	85%	80%	14%	23%	31%
Сервисы обмена мгновенными сообщениями	77%	72%	10%	14%	21%
Скачивание музыки, фильмов, видео и т.д.	76%	74%	7%	9%	14%
Скачивание бесплатного ПО / приложений	71%	66%	10%	17%	23%
Онлайн-игры	60%	56%	7%	7%	12%
Онлайн-шопинг	57%	54%	5%	4%	8%
Онлайн-банкинг	56%	52%	4%	8%	12%
Платежные системы / электронные кошельки	54%	51%	4%	6%	9%
Передача контента / данных	47%	44%	7%	11%	15%
Хранение данных онлайн	33%	29%	5%	7%	10%
Сайты для взрослых	29%	27%	2%	4%	6%
Азартные игры	23%	21%	3%	3%	6%
Любая финансовая активность	**81%**	**79%**	**9%**	**14%**	**20%**
Любая активность	**99%**	**97%**	**17%**	**31%**	**40%**

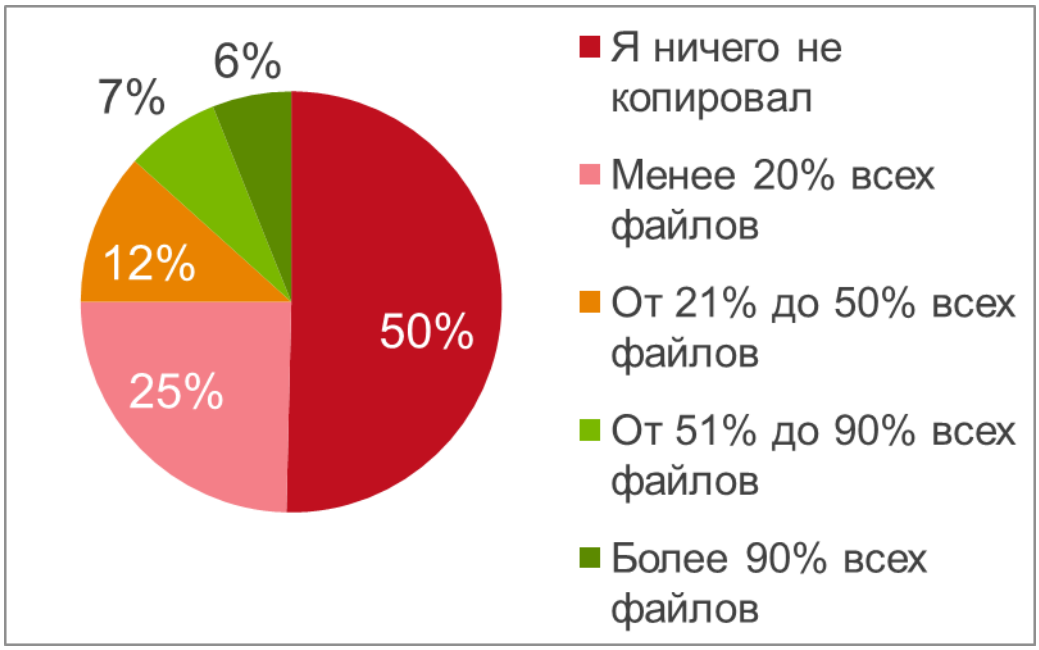
В среднем 81% респондентов регулярно пользуется различными онлайн-сервисами, связанными с финансами. Компьютер или ноутбук остается основным инструментом для доступа к подобным сервисам – 54% респондентов в России сообщили, что покупают товары в интернет-магазинах с помощью ПК; 52% - пользуются системами онлайн-банкинга. В то же время количество мобильных пользователей подобных сервисов в России пока незначительно. Так, например, всего 8% респондентов используют смартфоны для взаимодействия с банком, и еще меньше – 5% – используют планшеты для доступа к интернет-магазинам. Однако становясь более удобными, финансовые сервисы распространяются с настольных компьютеров на мобильные платформы. В таких условиях

едва ли будет трудно переоценить важность использования защитных продуктов на устройствах, с которых осуществляется взаимодействие с финансовыми сервисами.

Впрочем, финансовая активность в Интернете – это не только магазины, банки и платежные сервисы. Контент – музыка, фильмы, игры и др. – популярные товары, на которые пользователи регулярно тратят деньги.

Люди ценят контент на своих устройствах, но не заботятся о его защите

% медиа-файлов, к которым применялось резервное копирование

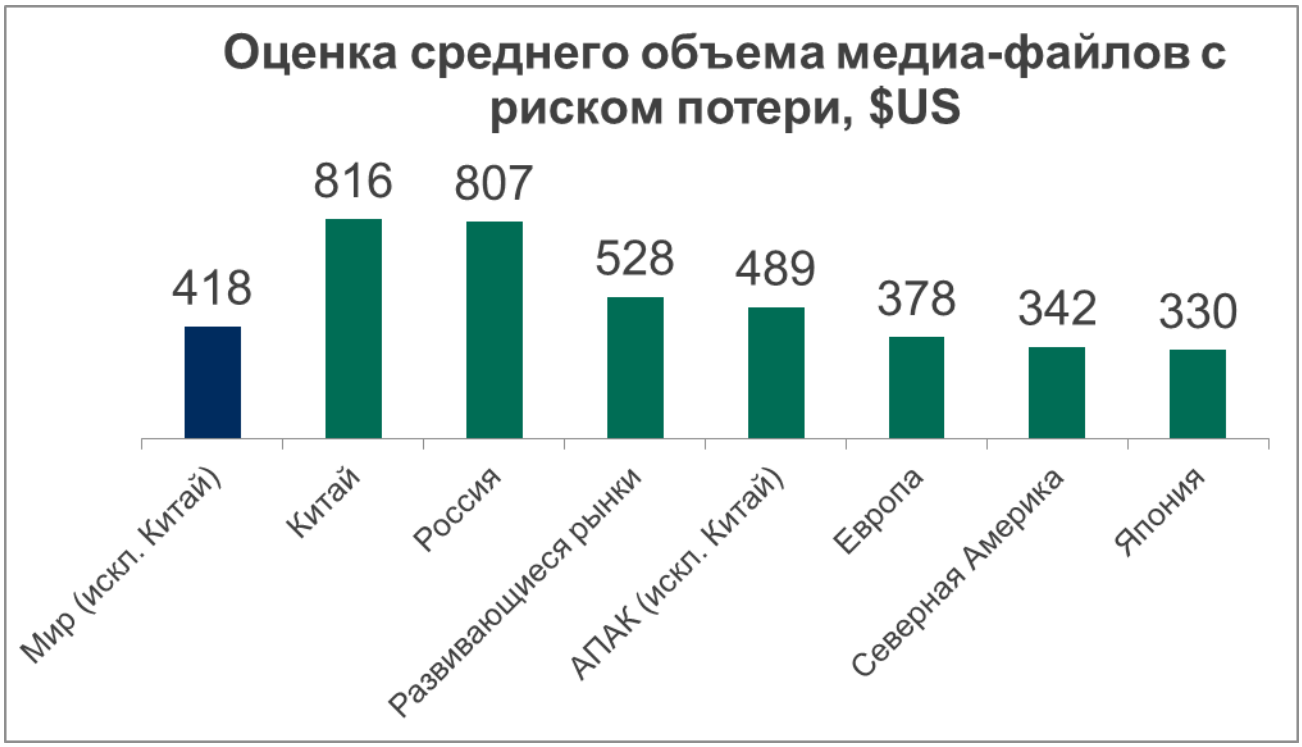


48% россиян считают, что информация, хранимая на устройствах, в частности мультимедийный контент, обладают гораздо большей ценностью, чем устройство само по себе. В среднем, на устройстве российского пользователя хранится 691 музыкальный файл, 36 фильмов или ТВ-шоу и 6 игр.

Одновременно российские пользователи не слишком заботятся о сохранности купленного контента – половина опрошенных (50%) сообщили, что не создают резервных копий медиа-контента, и еще четверть (18%) сообщили, что создают бэкап для менее чем 20% своей медиа-коллекции. Лишь 6% респондентов в России сообщили, что делают резервные копии более чем 90% музыки, фильмов, игр и других мультимедийных файлов. Столь беспечный подход к сохранению данных приводит к серьезным последствиям.

Помимо того, что в результате поломки устройства или вредоносной атаки пользователь может лишиться всей своей коллекции музыки, фильмов, фотографий, документов, подобные инциденты могут привести и к прямым финансовым потерям.

Потеря медиа-контента неизбежно ведет к финансовым убыткам



Легкомысленное отношение к резервному копированию файлов может вылиться в реальные финансовые убытки. При этом пользователи в России в наибольшей степени подвержены риску потерять особенно много – средняя потеря медиа-коллекции в результате вредоносной атаки или поломки устройства обойдется пользователю в **807** долларов США. Эта цифра сложилась из примерной стоимости контента, которым владеют пользователи, с учетом доли файлов, для которых не были сделаны резервные копии.

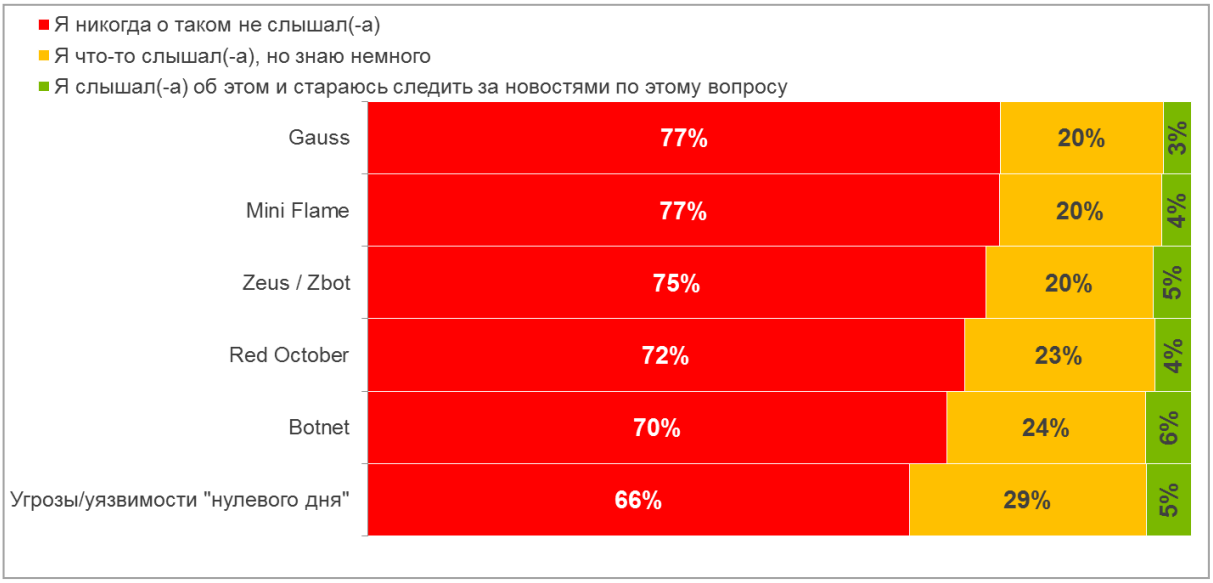
Отношение к кибербезопасности: пользователей больше беспокоит конфиденциальность информации, нежели последствия кибервойны

% согласных с каждым утверждением (Полностью согласен и Согласен

Безопасность личных данных вызывает у российских пользователей наибольшее беспокойство. Чаще всего респонденты сообщали, что их волнует, насколько хорошо компания, которой они доверяют свою конфиденциальную информацию, в том числе финансовую, может обеспечить ее защиту – об этом думает 61% респондентов. Кроме того, 55% опрошенных опасаются вероятности похищения их данных. Наконец, 48% испытывают сходное беспокойство, но уже в отношении представителей государства – далеко не все уверены, что государственные информационные сервисы способны надежно хранить персональные данные своих пользователей. Обеспокоенность растет вместе с повсеместным распространением различных сервисов, позволяющих, в том числе, получать государственные услуги в онлайн-режиме.

Еще одно серьезное опасение участников опроса – перспективы и возможные последствия кибервойн.

Кибероружие и спонсируемые государством атаки? Большинство не знает об этом

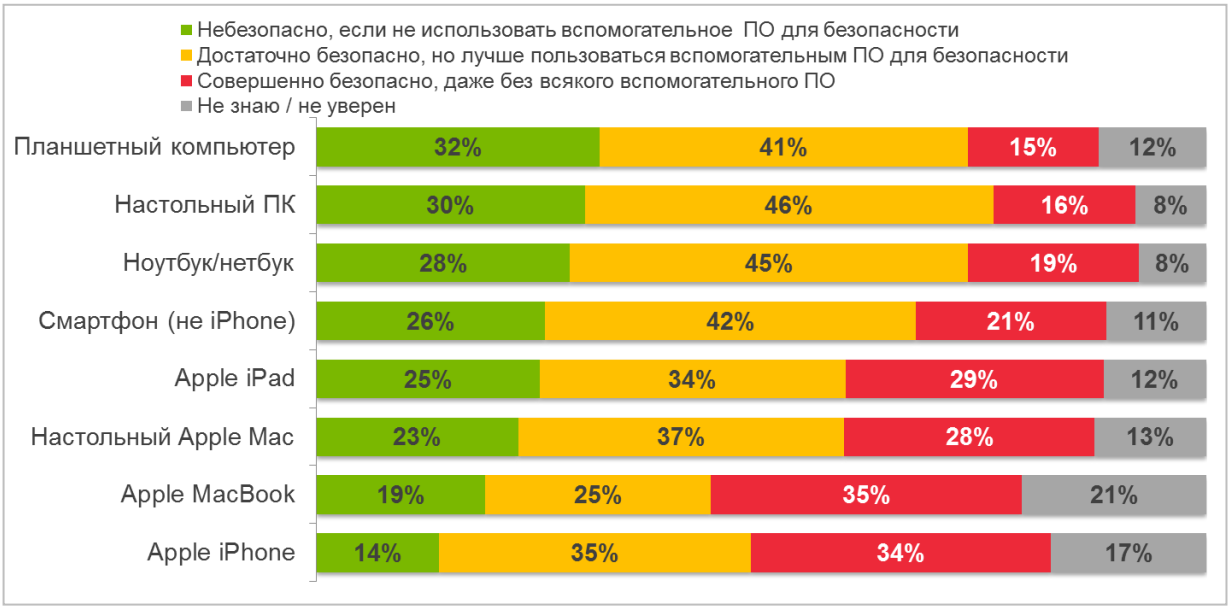


Хотя около 33% респондентов признались, что опасаются кибервойн и того, какой ущерб они могут причинить миру, уровень осведомленности об инструментах подобных войн довольно низкая. Люди в большинстве своем ничего не знают об обнаруженных в последние годы вредоносных программах Mini Flame, Gauss, шпионских кампаниях типа «Красный октябрь» и других явлениях, связанных с кибероружием, несмотря на то, что огромное количество информации о них есть в открытом доступе.

Не слишком беспокоят россиян и такие явления, как «хактивизм», обнаружение фактов, косвенно подтверждающих, что некоторые известные кибератаки были проспонсированы государственными органами разных стран, а также кибератаки на известные софтверные, игровые и медиакомпании, такие, как Adobe, Microsoft, Oracle, Sony, New York Times и др. В среднем лишь около трети опрошенных сообщили, что подобные инциденты стали для них поводом для беспокойства.

Меж тем, достаточно высокий уровень осведомленности о возможных вариантах кибератак и их последствиях – это сама по себе хорошая мера обеспечения безопасности цифровой жизни. Чем больше пользователь будет знать об угрозах, тем труднее злоумышленникам будет вовлечь его в какую-либо мошенническую схему.

Безопасность разных типов устройств: Windows требует дополнительной защиты, но не стоит забывать и про Mac



Самым опасным с точки зрения вероятности вредоносных атак традиционно остается настольный ПК – как правило, под управлением Windows. 76% опрошенных россиян считают, что подобные устройства не следует использовать без дополнительного защитного ПО. Также традиционно велико количество пользователей, убежденных, что компьютеры на системе OS X – Mac и MacBook – неуязвимы для киберугроз – такого мнения придерживаются 35% и 28% опрошенных соответственно. Однако пользователей, считающих, что OS X недостаточно безопасна, чтобы использовать ее без защитного ПО, все же больше. Если конкретнее, то порядка 60% респондентов согласились с необходимостью защищать компьютеры Apple с помощью подобных программ.

Также 68% владельцев смартфонов и 73% пользователей планшетов считают, что лучше защищать подобные устройства с помощью специализированного ПО.

Еще одной важной темой для пользователей является безопасность финансовых онлайн-сервисов.

Финансовая безопасность: некоторые слишком уверены в «третьей стороне»

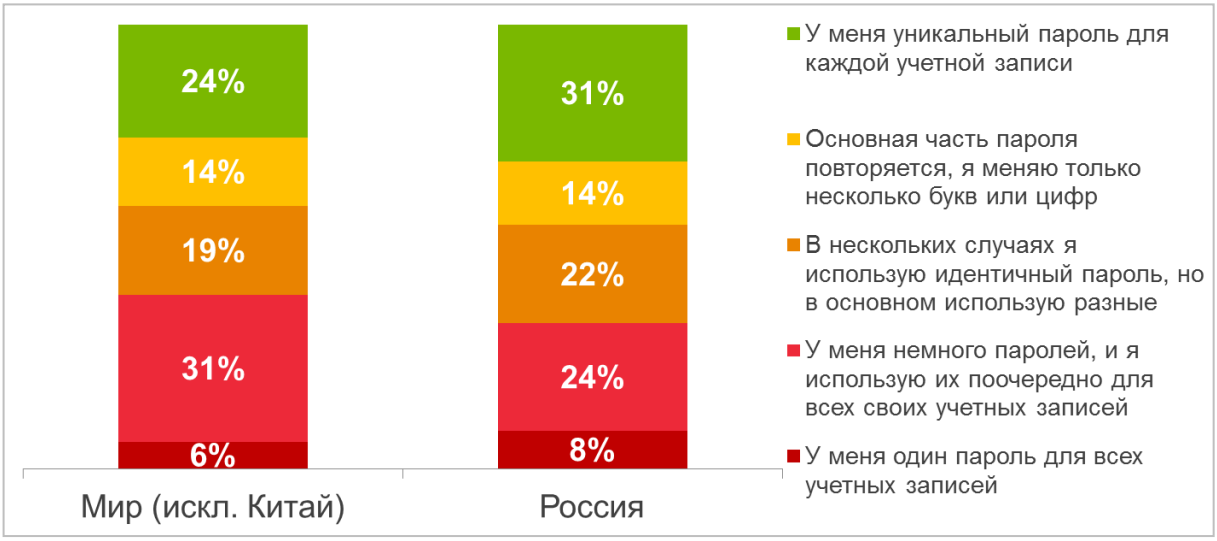
	Весь мир (искл. Китай)	Россия
Меня **беспокоят финансовые мошенничества в Сети**	59%	**63%**
Я **уверен**, что **банк** предпринял **необходимые меры** для **защиты** от финансового мошенничества	57%	**52%**
Я **не чувствую себя в полной безопасности**, осуществляя финансовые транзакции/совершая покупки онлайн	47%	**43%**
В случае кражи денег онлайн я рассчитываю, что **банк вернет мне всю сумму** без проблем	45%	**25%**
Бесплатное защитное ПО, предлагаемое банками, **должно обеспечить достаточную защиту** всех операций онлайн	42%	**47%**
Я **не изучаю методы обеспечения защиты** на тех сайтах, на которых я оставляю свою личную/финансовую информацию	28%	**25%**
С трудом верю, что преступники **будут перехватывать мобильные или Wi-Fi сигналы** для того, чтобы заполучить мои личные/финансовые данные	18%	**28%**
Мой банк не приходит на помощь, когда требуется обеспечить защиту онлайн	18%	**17%**
Киберпреступления, связанные с кражей денег – **редкое явление**, и **вряд ли это случится со мной**	14%	**18%**

Результаты опроса показывают, что россияне довольно хорошо осведомлены о распространенности финансовых мошенничеств в Сети и последствиях, которые несут за собой подобные преступления. Так 63% респондентов выразили беспокойство по поводу такого типа инцидентов. Еще 43% признались, что не чувствуют себя полностью в безопасности, когда осуществляют в Сети финансовые транзакции.

При этом изрядная часть респондентов считает, что ответственность за обеспечение безопасности транзакций должны нести банки. Например, 52% россиян уверены, что банки уже предприняли все необходимые меры для защиты их финансовых операций онлайн. Еще 47% участников опроса выразили мнение, что банк должен бесплатно предоставлять своим клиентам программное обеспечение для защиты онлайн-платежей. В реальности эти убеждения не всегда находят подтверждение. Далеко не всегда банки обеспечивают безопасность онлайн-транзакций со своей стороны, и еще реже – снабжают своих клиентов дополнительным защитным программным обеспечением.

Тем не менее, данные пользователя, связанные с его финансами, очевидно, требуют защиты. Как минимум, качественной защиты требуют пароли. Однако даже с этой базовой задачей справляются далеко не все и не всегда.

Защита данных: лишь немногие используют специальное ПО для создания и хранения паролей



32% опрошенных россиян сообщили, что имеют всего один или несколько паролей для всех своих аккаунтов. 22% пользователей используют пароли с минимальными отличиями друг от друга от аккаунта к аккаунту. И только около трети (31%) пользователей сообщили, что придумывают для каждого аккаунта уникальный пароль. Практика использования небольшого количества паролей для большого числа аккаунтов неудивительна, учитывая, что абсолютное большинство опрошенных (64%), стремясь сохранить пароли, полагаются исключительно на свою память – далеко не каждому удается запомнить множество разных паролей.

Лишь 6% людей используют специальное программное обеспечение для создания и надежного хранения паролей. Остальная часть опрошенных (из тех, кто не старается запомнить все пароли) используют менее безопасные методы хранения: в записной книжке (31%), на листе бумаге, который обычно лежит возле компьютера (12%), в электронном документе на компьютере (10%).

При этом нельзя сказать, что пользователи совсем уж легкомысленно относятся к своим паролям. Например, по результатам опроса, 75% российских респондентов следят за тем, чтобы их пароли для доступа к финансовыми сервисам и, например, социальным сетям отличались друг от друга. Однако, возможно, часть пользователей излишне наивна в оценке надежности третьих сторон, участвующих в хранении паролей. 34% респондентов

предполагают, что сайты и сервисы, которые они используют, надежно хранят и защищают пароли от злоумышленников, что далеко не всегда верно. Многие сайты хранят пароли своих пользователей в открытом виде, либо зашифрованными настолько плохо, что даже не самый подготовленный злоумышленник, взломавший сайт, сможет расшифровать пароли без особого труда, пользуясь общедоступными программами для расшифровки.

Мобильные устройства: широко используются, но плохо защищены

Устройство	iPad	Другой планшет	Другой телефон	Смартфон	iPhone
База	**64**	**120**	**188**	**293**	**45**
Фото / видео / музыка, созданные вами	89%	84%	82%	87%	85%
Личные электронные письма	62%	51%	27%	43%	44%
SMS или MMS	39%	23%	84%	83%	87%
Пароли к персональным аккаунтам, в том числе к почте	33%	16%	14%	18%	27%
Рабочие электронные письма	45%	36%	20%	30%	29%
Рабочие файлы	45%	42%	18%	27%	31%
Личные файлы	65%	59%	34%	48%	56%
Адреса/контакты	43%	28%	89%	86%	82%
PIN коды / банковские пароли и т.д.	11%	7%	15%	13%	20%
Другая банковская информация	11%	9%	9%	10%	9%
Пароли от корпоративных/рабочих аккаунтов	9%	6%	10%	8%	7%
Учебные материалы	2%	2%	1%	3%	4%
Любое из вышеперечисленного	**97%**	**92%**	**99%**	**97%**	**96%**

Персональные мобильные устройства активно используются для хранения действительно очень важной персональной информации. Например, 33% владельцев iPad в России (без учета владельцев других планшетов) хранят на своем устройстве данные для доступа к персональному ящику электронной почты, и 45% - сообщения из рабочей электронной почты. Владельцы iPhone (без учета владельцев других смартфонов) не отстают: 31% хранят на таких устройствах рабочие файлы; 29% - сообщения из рабочей электронной почты; 27% - данные для доступа к личному ящику.

При этом на смартфонах и планшетах также хранятся личные фотографии, видео и аудиозаписи пользователей – в среднем более 82% опрошенных сообщили, что используют свои устройства в таких целях.

Вместе с тем шифруют данные на мобильных устройствах сравнительно немного пользователей. Чаще всего этот способ защиты информации выбирают российские владельцы iPad – 33% из них применяют технологии шифрования данных. Для владельцев iPhone этот показатель составляет 24%. На всех же остальных мобильных устройствах информацию шифрует лишь 23% пользователей.

Хранение важных данных – распространенный сценарий использования мобильных устройств. Наряду с ним, люди применяют смартфоны и планшеты для доступа к всевозможным онлайн-сервисам, что несет в себе серьезную угрозу безопасности. Особенно, когда соединение с Сетью осуществляется через Wi-Fi.

Немногие думают о безопасности, подключаясь к Интернету через Wi-Fi

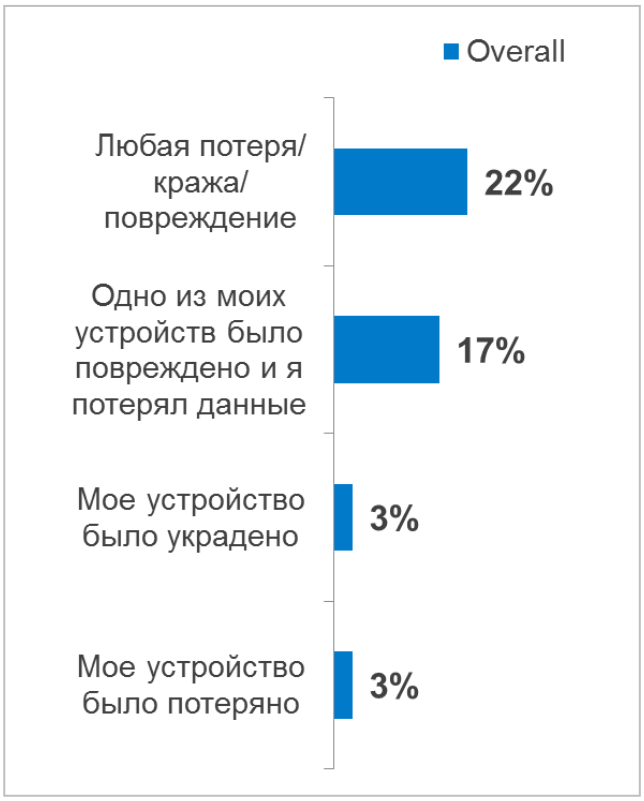
	Домашняя сеть Wi-Fi	Бесплатная общественная сеть Wi-Fi	Платная общественная сеть Wi-Fi	Любая общественная сеть Wi-Fi
Ноутбук	66%	46%	5%	47%
MacBook	72%	64%	18%	73%
Ноутбук/MacBook	**66%**	**46%**	**5%**	**47%**
iPad	89%	86%	3%	86%
Другой планшет	77%	66%	5%	67%
Любой планшет	**80%**	**74%**	**4%**	**74%**
Смартфон	68%	74%	5%	75%
iPhone	87%	84%	9%	87%
Смартфон/iPhone	**70%**	**76%**	**6%**	77%
Любое мобильное устройство	**72%**	**75%**	**6%**	**76%**

В среднем 76% российских респондентов, сообщивших, что у них есть мобильное устройство с возможностью выхода в Интернет, пользуются Wi-Fi. При этом 75% используют бесплатные публичные точки доступа.

При работе с такими хот-спотами важно использовать дополнительные меры защиты, поскольку интернет-трафик может быть перехвачен злоумышленниками. Однако далеко не все пользователи осознают это. Так, 36% респондентов сообщили, что не принимают никаких дополнительных мер безопасности, подключаясь к публичным хот-спотам. Еще 8% заявили, что не опасаются использовать открытые точки доступа для работы с сервисами, обрабатывающими личные финансовые данные людей – интернет-магазины, сервисы онлайн-банкинга, платежные системы. Лишь 10% российских пользователей сказали, что

прежде чем воспользоваться хот-спотом, они выясняют, какие стандарты шифрования используются для соединения точки доступа с персональным устройством.

Потеря или кража: почти четверть россиян потеряли свое мобильное устройство, а вместе с ним и данные



22% опрошенных россиян сообщили, что за последние 12 месяцев одно из их электронных устройств было потеряно, украдено или сломано. Наиболее часто устройства все же повреждаются – об этом сообщили 17% участников опроса. Кражи и потери случаются реже – по 3% респондентов столкнулись с такими ситуациями. При этом похищения или утери мобильных устройств происходят чаще, чем инциденты, связанные с потерей или хищением других ценных вещей. Так, с цифровыми устройствами по причине утери или кражи расставались 6% россиян, с платежными картами – 5%, с ключами от дома – 4%, с бумажниками – 3%, с часами и паспортами – по 2%.

Сразу после утери или хищения россияне чаще всего блокируют SIM-карту, о чем сообщили 43% респондентов. Чуть меньше – 33% участников опроса – сообщили, что меняют пароли к своим онлайн-аккаунтам. Столько же людей (33%) используют средства, позволяющие

удаленно заблокировать доступ к потерянному или украденному устройству. Значительно меньшее количество пользователей прибегают к специализированным механизмам, позволяющим удаленно стереть с устройства всю важную информацию (13%) или сфотографировать лицо незаконного владельца устройства (10%), чтобы потом передать фотографию в полицию.

Почти треть пользователей ошибочно полагает, что их устройства изначально защищены

	Весь мир (искл. Китай)	Россия
Мне было бы некомфортно использовать мобильный телефон в качестве прямого средства оплаты, например, в магазинах в будущем	38%	**37%**
Я бы никогда использовать смартфон / планшет для совершения платежных операций (например, в онлайн-магазине)	33%	**37%**
Я предполагаю, что мой телефон/планшет имеет изначальную защиту с того момента, как я приобрел его	30%	**29%**
Я бы никогда не сталь пользоваться онлайн-банкингом на смартфоне/планшете	28%	**25%**
Я откладываю покупку смартфона/планшета на базе Android, потому что эта платформа потенциально уязвима	13%	**11%**
Я использую iPhone / iPad, который не подвержен киберугрозам	11%	**4%**

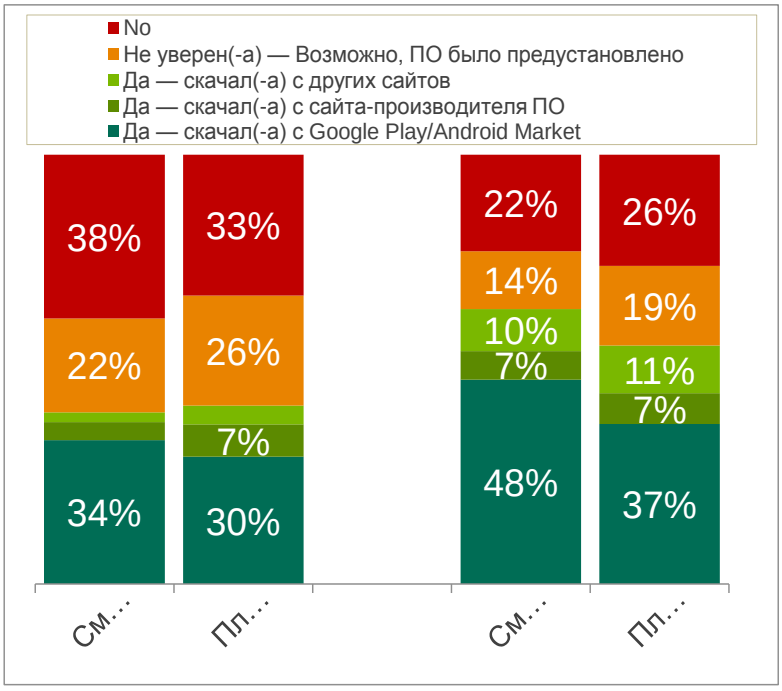
В целом большое число российских пользователей с недоверием относятся к уровню защищенности мобильных устройств от киберугроз. Например, 37% заявили, что никогда не выбрали бы смартфон или планшет для совершения финансовых операций. Столько же людей (37%) не чувствовали бы себя в безопасности, если бы пришлось пользоваться финансовыми онлайн-сервисами со смартфонов и планшетов. Также 11% опрошенных сообщили, что отказались от покупки мобильного устройства на самой популярной в мире операционной системе Android из соображений безопасности – постоянные случаи появления информации о новых вредоносных программах под эту систему и уязвимостях в ней серьезно подрывают доверие пользователей к Android.

Одновременно, значительная часть пользователей, отвечая на вопросы о безопасности своих мобильных устройств, придерживается мнений, которые во многих случаях являются заблуждениями. Например, 29% респондентов сообщили, что, по их предположениям, смартфон или планшет, который они купили, уже «из коробки» был защищен от кибератак. Это не всегда так – далеко не все производители смартфонов предварительно устанавливают на свои устройства защитные решения, а если и устанавливают, то очень часто это максимально простые программы с сильно ограниченным функционалом.

Любопытно, что 4% российских пользователей устройств от Apple – iPhone и iPad – говорит, что используют именно эти устройства, в том числе потому что они неуязвимы для хакерских атак. Действительно, данные устройства по сравнению с устройствами на Android гораздо реже становятся объектами атак злоумышленников. Однако их безопасность, как и безопасность любых других устройств, содержит бреши, информация о которых регулярно появляется в открытом доступе.

Впрочем, Android, все же остается главной темой, когда речь заходит о безопасности мобильных устройств.

Безопасность платформы Android – по-прежнему животрепещущий вопрос



Высокий уровень опасений в отношении защищенности мобильных устройств от киберугроз, в том числе работающих под управлением Android, привел к тому, что российские пользователи стали самыми ответственными и в большинстве своем установили специализированное защитное ПО на эти устройства. Сделали это 64% владельцев смартфонов и 56% владельцев планшетов на базе Android в России. Это значительно больше, чем в целом по миру (40% и 42% соответственно).

Однако значительный процент пользователей Android все так же остается без защиты. Особенно тревожно это выглядит на фоне того ландшафта киберугроз, с которыми приходилось сталкиваться российским владельцам электронных устройств.

Киберугрозы: почти половина пользователей в России стали жертвами киберпреступников

Почти 20% всех вредоносных атак привели к потере важных данных

	Весь мир (искл. Китай)	Россия
Заражение вредоносным ПО привело к тому, что мой компьютер стал плохо работать/перестал работать вообще	15%	20%
Компьютер был заражен в результате открытия вложения в электронном письме	9%	9%
Компьютер был заражен в результате использования USB-флешки или другого внешнего носителя	8%	19%
Из-за вредоносной атаки я потерял личные файлы, хранившиеся в моем компьютере	5%	12%
Сталкивались с вредоносными атаками	**27%**	**45%**

В совокупности за последние 12 месяцев почти половина россиян – 45% – столкнулись хотя бы с одной атакой, в ходе которой устройство было заражено вредоносной программой. Чаще всего (20% случаев) заражение вредоносным ПО провоцировало нестабильную работу компьютера или вовсе его выход из строя. В 12% случаев заражение приводило к потерям сохраненных на компьютере данных.

19% всех вредоносных атак выливались в утечку важных данных пользователя. В 65% случаев восстановить их полностью не удалось. Вредоносные атаки также приводили и к финансовым потерям.

Одна вредоносная атака ведет к финансовым убыткам в размере до 750 долларов США

Вы понесли какие-либо финансовые потери в связи с заражением вирусом/вредоносным ПО?

Направления затраты средств

В 39% случаев российские пользователи терпели финансовые убытки в результате вредоносных атак. Чаще всего – 17% ответов – им приходилось тратиться на услуги по лечению устройства от заражения; 15% пользователей платили за услуги по восстановлению данных.

В среднем одна успешная вредоносная атака на устройство вынуждает пользователя расстаться с 76 долларами США. Однако в отдельных случаях траты были выше. Например, за услуги по восстановлению работоспособности устройства и данных на нем, пострадавшим приходилось платить до 120 долларов, а когда в результате атаки пользовательское устройство выходило из строя, расходы могли возрасти до цены нового устройства – от 225 долларов за планшет на базе Android до 750 долларов за MacBook.

74% россиян хотя бы раз сталкивались с финансовой киберугрозой

	Весь мир (искл. Китай)	Россия
Анонимные/незапрошенные сообщения в электронной почте или социальных сетях с подозрительными вложениями/ссылками	40%	39%
Подозрительное сообщение в электронной почте якобы от банка, запрашивающего мой пароль или другую персональную информацию	30%	10%
Подозрительное сообщение в электронной почте якобы от социальной сети / интернет-магазина / другого сайта	22%	17%
Всплывающее окно в браузере с уведомлением о том, что мой компьютер заражен и мне необходимо купить антивирус	21%	56%
Перенаправление на подозрительную веб-страницу, запрашивающую данные моей банковской карты (например, в процессе онлайн-шопинга)	10%	11%
Ввод персональной/финансовой информации на веб-сайте, в легитимности которого я не уверен	6%	9%
Стал жертвой онлайн-мошенничества, в результате которого потерял деньги	4%	8%
Столкнулись с любой из финансовых угроз	62%	74%

74% российских пользователей Интернета, участвовавших в опросе, сообщили, что хотя бы раз подвергались атакам, целью которых являлось похищение персональной информации, связанной с финансами. Например, 10% респондентов сообщили, что получали подозрительное письмо, в котором говорилось, что оно от банка, но которое таковым – как выяснялось впоследствии – не являлось. Около 56% подверглись атакам злоумышленников, промышляющих распространением фальшивых антивирусов. Почти каждый десятый пользователь (11%) хотя бы раз перенаправлялся на подозрительную страницу, где ему предлагалось ввести данные о своей платежной карте. Около 8% опрошенных сообщили, что стали жертвами финансовых мошенников. При этом абсолютное большинство россиян – 72% – не смогли полностью вернуть похищенные деньги.

Впрочем, вредоносные атаки не всегда выливались в финансовые потери. Были и другие неприятные последствия. Например, взлом аккаунтов.

Неавторизованные посты и удаление персональных данных – рядовые последствия взлома онлайн-аккаунтов

	Весь мир (искл. Китай)	Россия
Кто-то получил доступ к аккаунту моей электронной почты/изменил мой пароль без моего ведома	7%	7%
Кто-то получил доступ к моему аккаунту в соцсетях/изменил мой пароль без моего ведома	6%	23%
Кто-то получил доступ к моему аккаунту на другом сайте/изменил мой пароль без моего ведома	4%	7%
Любое из вышеперечисленного	**14%**	**31%**

В совокупности 31% опрошенных россиян столкнулись хотя бы с одним инцидентом, в рамках которого один из их аккаунтов был взломан злоумышленниками. Более половины (56% респондентов) сообщили, что им вовремя удалось сбросить пароль и вернуть доступ к аккаунту, однако остальные жертвы взломщиков сталкивались с разнообразными негативными последствиями таких инцидентов. В частности 44% респондентов сообщили, что от их имени совершались публикации, 14% признались, что кто-то из их онлайн-друзей переходил по вредоносной ссылке, разосланной из взломанного аккаунта. В 14% случаев взломщики удаляли персональные данные своих жертв.

Для множества пользователей любая кибератака – это посягательство на их личное виртуальное пространство, которое можно пресечь, в случае если человек ответственно подходит к защите своих данных. Все гораздо сложнее, когда речь заходит о пользователях, у которых есть несовершеннолетние дети.

Дети в Интернете – каждый третий ребенок подвергается риску

Угрозы для детей в Сети варьируются от нежелательного контента до опасных коммуникаций с незнакомцами

	Весь мир (искл. Китай)	Россия
Я регулярно разрешаю детям пользоваться моим смартфоном / планшетом без моего присмотра за этим процессом	13%	18%
Мои дети видели нежелательный контент в Сети	11%	20%
Мои дети случайно удалили информацию / данные из моего компьютера	10%	14%
Мои дети общались с незнакомцами / подозрительными людьми в Сети	7%	5%
Мои дети неожиданно потратили мои деньги в магазине приложений / в социальных сетях	5%	2%
Мои дети случайно выложили в открытый доступ информацию / данные, хранящиеся на моем компьютере	5%	3%
Мои дети использовали мои платежные карты/аккаунты без моего разрешения	4%	1%
Мои дети стали жертвами агрессии в Интернете	3%	2%
Любой риск	**27%**	**36%**
Любые потерянные деньги/данные	**18%**	**17%**

36% российских родителей признались, что их дети подвергались риску во время своих интернет-сессий. В частности, 20% детей сталкивались с нежелательным для них контентом, 5% - вступали в переписку с незнакомцами. Кроме того, 17% родителей понесли финансовые убытки, либо потеряли важные данные из-за действий детей. В основном, отпрыски случайно удаляли важные сведения и без спроса пользовались платежными средствами родителей.

В целом 79% родителей выразили согласие с тем, что эффективные средства для защиты детей в Сети были бы очень полезны и востребованы ими.

Что же делали родители, чтобы защитить своих детей?

Каждый пятый родитель в России не предпринимает никаких действий для того, чтобы обезопасить своих детей в Сети

	Весь мир (искл. Китай)	Россия
Я стараюсь следить за детьми, когда они в Сети	**40%**	39%
Я ограничиваю время, которое дети могут проводить в Сети	**38%**	39%
Я регулярно проверяю историю посещений сайтов в интернет-браузере	**31%**	30%
Я использую функции родительского контроля	**25%**	26%
Я добавил своих детей в друзья в социальных сетях	**19%**	16%
Я попросил своего интернет-провайдера заблокировать доступ к нежелательным сайтам	**12%**	9%
Другое	**4%**	4%
Ничего из вышеперечисленного	**22%**	**22%**

Хотя большинство респондентов считают, что детей нужно защищать в онлайне, методы, которые они избирают для достижения этой цели, серьезно разнятся. Например, 39% заявили, что пытаются контролировать деятельность детей в Интернете. Так же 39% родителей ограничивают время, которое дети проводят в Интернете, а 30% регулярно проверяют историю браузера, которым пользуется ребенок.

В то же время 22% родителей никак не ограничивают деятельность детей в Сети, тем самым подвергая их серьезному риску столкнуться с контентом или пользователями, которые могут нанести им вред.

При этом лишь 26% родителей используют защитное ПО с функциями родительского контроля, которое обычно позволяет очень гибко настраивать то, как часто и как долго ребенок может пользоваться интернетом и какие сайты он может посещать.

Заключение: разнообразие устройств требует специальных мер для обеспечения киберзащиты

Из результатов опроса видно, что распространение практики использования одним человеком множества устройств не только сделало его онлайн-жизнь увлекательной и комфортной, но и пополнило список актуальных киберугроз.

Функционал современных мобильных устройств позволяет использовать смартфоны и планшеты в качестве замены видео- и фотокамерам, что и делают люди. Более того, эти устройства достаточно функциональны, чтобы решать не только личные, но и рабочие задачи, что – опять-таки – регулярно делают пользователи. Однако эти же тенденции повышают риск того, что в результате вредоносной атаки, кражи или потери устройства, пользователь расстанется с крайне важными персональными данными: личными фотографиями, видео- и аудиозаписями, рабочими документами, что в итоге нанесет серьезный финансовый и моральный ущерб. Следует также отметить, что многие пользователи довольно ответственно подходят к обеспечению безопасности своего цифрового мира, но вместе с тем, велика доля и тех людей, кто относится к важным вопросам безопасности с, возможно, излишней доверчивостью и иногда беспечностью.

Чтобы свести к минимуму вероятность возникновения инцидента, связанного с сохранностью цифровых ценностей, владельцам различных устройств нужно соблюдать несколько простых правил информационной безопасности:

- использовать надежное защитное решение для всех устройств пользователя и его близких;
- ответственно подходить к созданию паролей для онлайн-сервисов, особенно тех, что связаны с проведением финансовых транзакций;
- пользуясь финансовыми сервисами, обеспечивать дополнительную защиту транзакций с помощью специализированной защитной технологии, например такой, как «Безопасные платежи», входящей в состав защитного решения Kaspersky Internet Security;
- регулярно делать резервные копии ценной информации, хранящейся не только на ПК, но и на мобильных устройствах;
- не забывать о том, что Интернет не делает различий в возрасте пользователей, и по умолчанию дети имеют свободный доступ ко всему контенту, который есть в Сети. Для их безопасности родители должны использовать защитное решение с функционалом родительского контроля;
- использовать только защищенные соединения с Wi-Fi хот-спотами.

Для владельцев одновременно нескольких устройств «Лаборатория Касперского» предлагает Kaspersky Internet Security для всех устройств – мощное защитное решение, включающее в себя отдельные продукты для обеспечения безопасности личной информации людей, владеющих устройствами на разных операционных системах: Windows, OS X и Android. Каждый продукт, входящий в состав этого решения, содержит передовые технологии противодействия всем видам кибератак, а кроме того – оптимизирован под конкретную платформу таким образом, чтобы оказывать минимальное воздействие на вычислительные ресурсы компьютера, смартфона или планшета пользователя и быть максимально удобным в использовании.