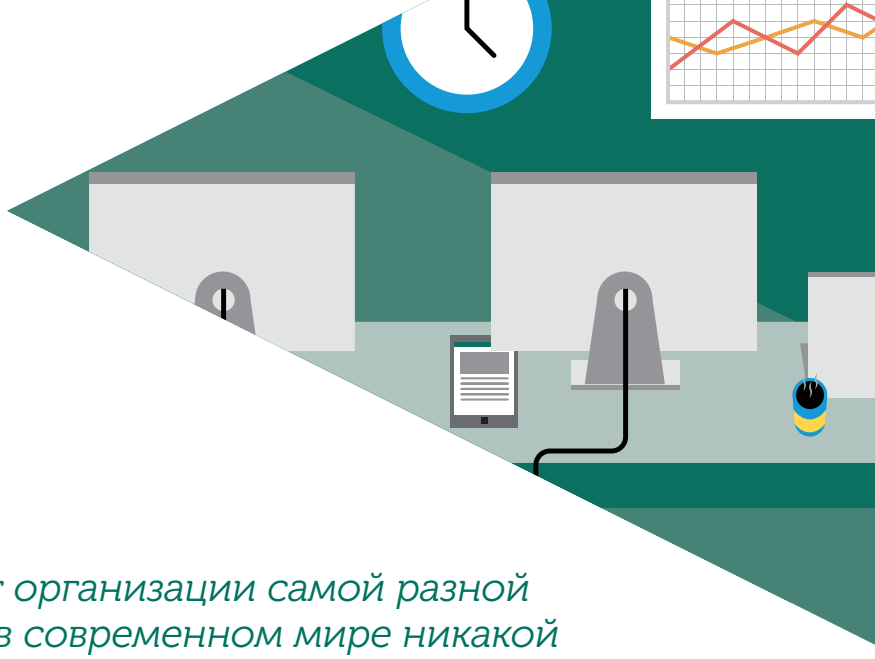
KASPERSKY lab

# IT-БЕЗОПАСНОСТЬ МАЛОГО БИЗНЕСА: ПРАКТИЧЕСКОЕ РУКОВОДСТВО

*Как обеспечить комплексную защиту вашего бизнеса от информационных угроз*

kasperskysmb.ru



*К малому бизнесу причисляют организации самой разной структуры и размера. Однако в современном мире никакой бизнес – ни офисные команды, ни частные предприниматели, работающие на дому, – не может себе позволить игнорировать проблему интернет-безопасности.*

О киберпреступлениях часто пишут на первых полосах газет, но обычно это происходит, когда жертвой становится крупная международная или правительственная организация. Но куда чаще удар принимают на себя небольшие компании.

Только за 2014 год было обнаружено 143 млн новых вредоносных объектов[1]. Большинство их было нацелено на простых пользователей и на организации, которые вряд ли считали, что представляют интерес для злоумышленников.

Реальность такова, что сегодня мы все – под прицелом. Но не стоит отчаиваться: быть целью еще не значит стать жертвой.

Исход противоборства зависит главным образом от того, кто окажется более подготовленным. Поэтому мы и составили данное руководство - чтобы рассказать, как обеспечить безопасность бизнеса.

## ? ЗНАЕТЕ ЛИ ВЫ...ЧТО ТАКОЕ ВРЕДОНОСНОЕ ПО?

Термином «вредоносное ПО» обозначаются компьютерные программы, созданные в преступных целях. Как правило, они проникают на устройства без ведома пользователей. «Лаборатория Касперского» – мировой лидер и эксперт в обнаружении вредоносных программ, что регулярно подтверждается независимыми тестами.[2]

## ? ЗАЧЕМ НУЖНА ЗАЩИТА?

Киберпреступники могут нанести серьезный ущерб вашему бизнесу, даже если не станут покушаться на ваш банковский счет. Вредоносное ПО может нарушить рабочий процесс, стать причиной перебоев в работе, что повлечет за собой цепочку негативных последствий, в числе которых отсрочка поступления денежных средств, потеря клиентов и пр.
Защитить компанию от подобных происшествий относительно просто. Спокойствие обойдется вам не слишком дорого.

[1] AV Tests
[2] Результаты ТОП-3 независимых тестов

# ФОРМУЛА IT-БЕЗОПАСНОСТИ

**ПЕРВЫМ ШАГОМ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ БИЗНЕСА ДОЛЖЕН СТАТЬ АНАЛИЗ РАБОЧИХ ПРОЦЕССОВ И ОПРЕДЕЛЕНИЕ УЯЗВИМЫХ МЕСТ, ГДЕ НУЖНО СНИЗИТЬ РИСКИ. ОЦЕНИТЕ СОСТОЯНИЕ IT-БЕЗОПАСНОСТИ ВАШЕЙ КОМПАНИИ.**

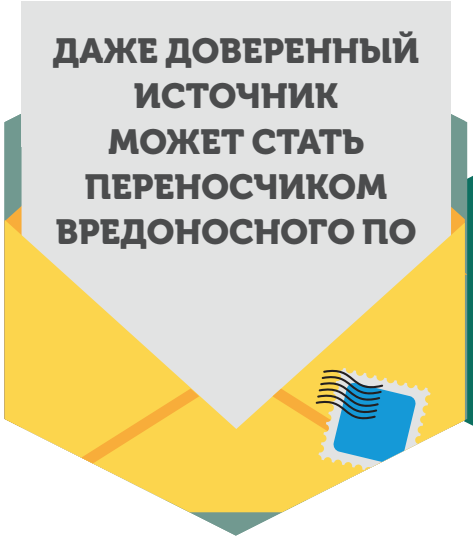
## ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО ✔

Средства для защиты от вредоносного ПО, как программа медицинского страхования, должны быть не просто хорошими, а лучшими из возможных. Если у вас еще нет эффективных программ для защиты устройств от заражения, их приобретение должно стать приоритетной задачей.

Простой осторожности при использовании интернета уже недостаточно. Все мы знаем, что нельзя открывать вложения в письмах, полученных от неизвестных отправителей, и загружать файлы с подозрительных сайтов. К сожалению, это не дает полной гарантии от заражения, поскольку множество вредоносных программ присылается из доверенных источников, которые оказались заражены.

## ПОВЕДЕНИЕ В ИНТЕРНЕТЕ ✔

Обучение сотрудников основам безопасности в интернете может сэкономить массу времени и нервов. Ваши сотрудники должны понимать, что на работе не стоит посещать сторонние сайты, которые могут быть небезопасными. Рекомендуем использовать инструменты блокирования нежелательных веб-ресурсов, чтобы они были недоступны с рабочих компьютеров. Также, практически все работники теперь имеют мобильные устройства (как минимум смартфон или планшет), которыми пользуются не только в личных, но и в рабочих целях, и покинув офис, уже не думают о безопасности данных. Повышение осведомленности ваших сотрудников об угрозах IT-безопасности поможет им соблюдать правила безопасности вне офиса при пользовании личными устройствами в рабочих целях.




## ? ПОЧЕМУ ЭТО ВАЖНО ДЛЯ МЕНЯ?

Приходилось ли вам получать от коллеги, друга или родственника письмо с интересной ссылкой, которая потом вела на подозрительный сайт? Если вредоносное ПО проникло на компьютер, то дальше оно может действовать без ведома пользователей, например рассылать почтовые сообщения. Поэтому даже так называемым доверенным источникам не всегда можно доверять.

## ПАРОЛИ ✔

У сотрудников обязательно должны быть надежные уникальные пароли, в которых присутствуют цифры, буквы обоих регистров и специальные символы. Пароль, представляющий собой обычное слово из повседневного словаря, легко взламывается программами, в которых используется метод простого перебора слов. Но даже надежный пароль может стать причиной серьезных проблем, если он используется в нескольких местах.

## ОБНОВЛЕНИЯ ПРОГРАММ ✔

Ежедневно специалисты «Лаборатории Касперского» фиксируют 325 тысяч новых угроз. То есть каждую секунду появляется четыре новых вредоносных объекта[3]. Как справиться с таким потоком? Защитные программы необходимо дополнять инструментами, которые будут отслеживать наличие уязвимостей и отсутствие обновлений в программах и операционных системах, поскольку киберпреступники нередко используют уязвимости, чтобы проникнуть в корпоративную сеть.

## А ВЫ ИСПОЛЬЗУЕТЕ НАДЕЖНЫЕ ПАРОЛИ?

1. У вас простой пароль, который легко запомнить, например, «пароль» или «123456». Но такой пароль так же легко подобрать и взломать.
2. В качестве пароля вы используете своей адрес электронной почты или другую легко доступную информацию.
3. Вы выбрали легкий вопрос для восстановления пароля, например, «Девичья фамилия матери». Злоумышленники могут легко найти ответы на такой вопрос и установить собственный пароль.
4. Ваш пароль представляет собой распространенное слово, которое вы дополнили одной-двумя цифрами в конце или начале.
5. Вы используете распространенные фразы и словосочетания в качестве паролей. Даже небольшие предложения (например, «этомояжизнь») легко подбираются и взламываются.

Если хотя бы один из перечисленных пунктов - про вас, то ответ на этот вопрос, к сожалению, «нет».

*О том, как создавать надежные пароли, читайте в нашем блоге business.kaspersky.ru*


[3] AV Tests

**В 2014 ГОДУ ПОЯВИЛОСЬ**

**295 500**

**НОВЫХ УГРОЗ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ[4]**

## БАНКОВСКИЕ ОПЕРАЦИИ ✔

Киберпреступники используют самые разные методы, чтобы получить доступ к вашей финансовой информации: от заманивания на поддельные версии доверенных сайтов до установки шпионских программ, следящих за вашими действиями. Чтобы им противодействовать, нужно активно принимать меры.

Помните о так называемых фишинговых атаках, когда мошенники отправляют сообщения от имени банка. Всегда пользуйтесь безопасным браузером и внимательно проверяйте URL-адрес, перед тем как вводить свои данные на любом сайте. Кроме того, лучше не включать финансовые и другие конфиденциальные данные в сообщения электронной почты, которые могут прочитать злоумышленники (или просто случайные люди).

## МОБИЛЬНЫЕ УСТРОЙСТВА ✔

Киберпреступники знают, что теперь многие сотрудники компаний работают вне офиса, и все чаще их внимание привлекают мобильные устройства. За 2014 год было обнаружено 295 500 новых вредоносных программ, созданных специально для мобильных устройств (смартфонов и планшетов)[5]. Месячное число атак с использованием мобильного вредоносного ПО выросло на порядок – с 69 000 атак в августе 2013 года до 644 000 в марте 2014 года[6].

## ШИФРОВАНИЕ ✔

Если на ваших устройствах хранятся конфиденциальные данные, их следует шифровать, чтобы никто не смог ими воспользоваться в случае потери или кражи устройства. Важно понимать, что информация представляет для бизнеса ценный ресурс, который нуждается в защите.

## ? ЧТО ТАКОЕ ФИШИНГ?

Фишингом называется попытка киберпреступников разузнать важную информацию (пароли, данные кредитных карт и т. п.), представляясь сотрудником доверенного учреждения, а затем присвоить деньги, воспользовавшись добытой информацией.

[4] и [5] По данным «Лаборатории Касперского»
[6] Информационная безопасность бизнеса, 2014 г.

# ПОНИМАНИЕ РИСКОВ

**О КИБЕРБЕЗОПАСНОСТИ ГОВОРИТСЯ МНОГО ХОРОШИХ И ПРАВИЛЬНЫХ СЛОВ, И МАЛО КОМУ ЗАХОЧЕТСЯ НА СЕБЕ ИСПЫТАТЬ ПОСЛЕДСТВИЯ ДЕЙСТВИЯ КИБЕРУГРОЗ. МЕЖДУ ТЕМ ДЛЯ БОЛЬШИНСТВА ЛЮДЕЙ КИБЕРБЕЗОПАСНОСТЬ ОСТАЕТСЯ ЧЕМ-ТО НЕПОНЯТНЫМ. ПОЭТОМУ НИЖЕ МЫ ПРИВОДИМ ПАРУ НАГЛЯДНЫХ СЦЕНАРИЕВ.**

## *Слишком дорогой кофе*

Проводив последнего за день клиента, Иван вышел с работы, поручив партнеру запереть двери. Иван должен был встретиться с другом в кафе рядом с офисом. Вспомнив, что завтра подходит срок платежа одному из поставщиков, он решил немедленно, пока не забыл, заняться этим делом.

Иван подключил свой ноутбук к сети Wi-Fi в кафе, зашел на веб-сайт банка и провел платеж. Затем он позволил себе насладиться вечерним кофе, радуясь, что вовремя вспомнил о важном деле.

Проверяя свой счет в следующий раз, Иван обнаружил, что тот пуст.

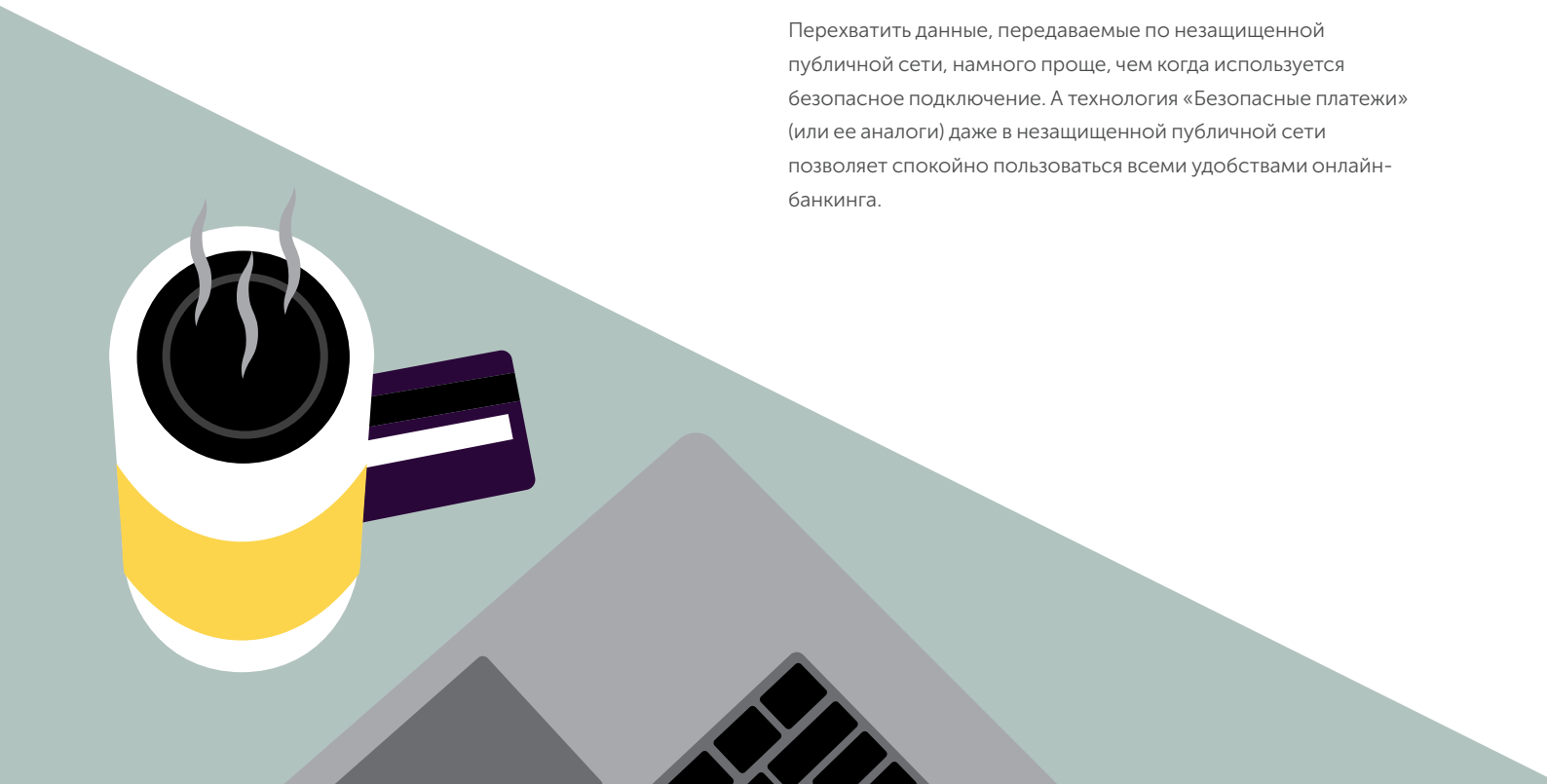
### КАК ТАКОЕ ПРОИЗОШЛО?

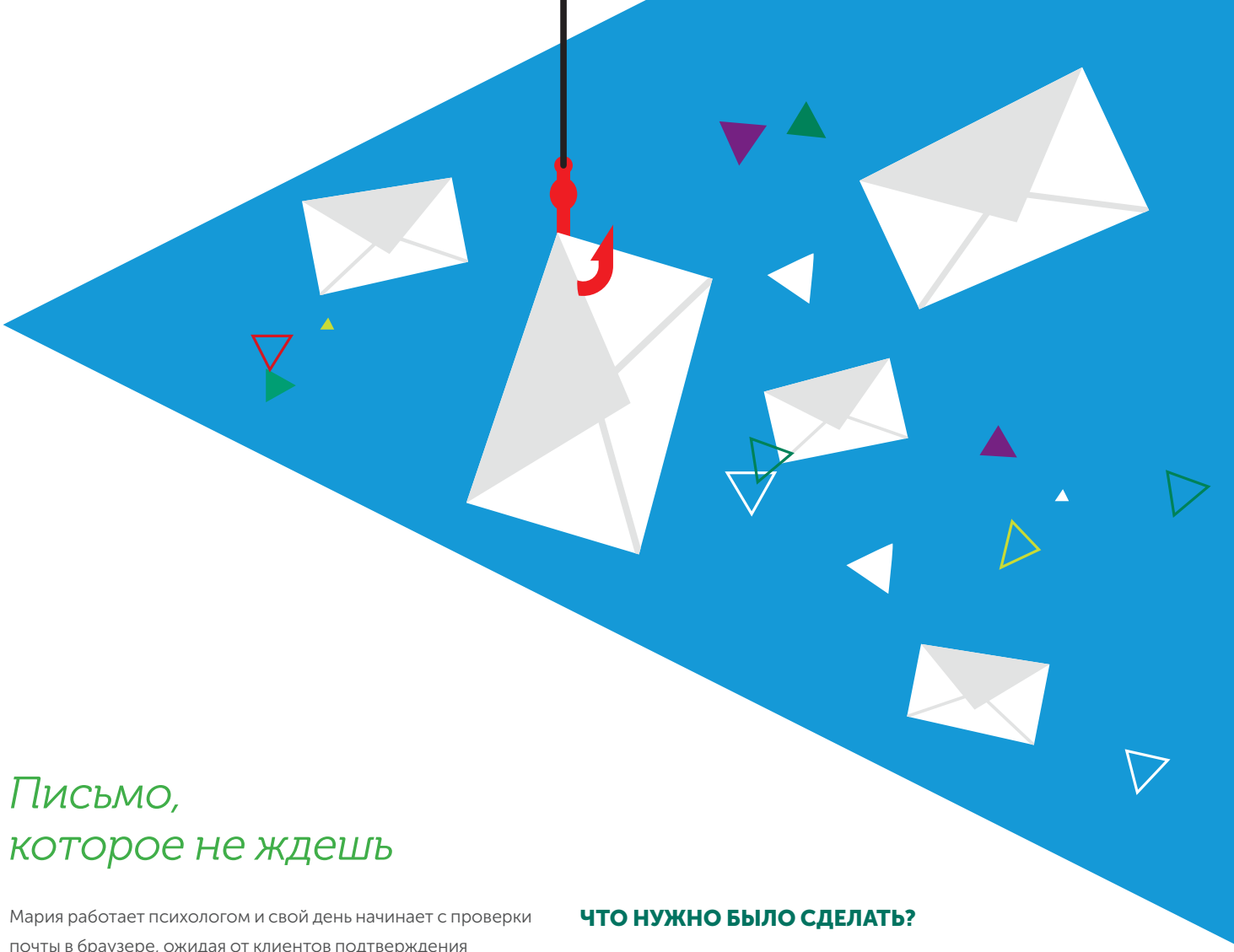
К сожалению, на ноутбуке Ивана не было установлено никакой защиты от вредоносного ПО, и туда загрузился клавиатурный шпион. А поскольку Иван пользовался публичной сетью Wi-Fi, он подвергался риску перехвата информации, которую вводил на сайтах. Именно таким образом злоумышленники и получили все данные Ивана о банковской транзакции.

### ЧТО НУЖНО БЫЛО СДЕЛАТЬ?

Банковские операции следует проводить только на устройствах, где установлена защита от вредоносного ПО, и всегда через безопасный браузер. Например, с технологией «Лаборатории Касперского» «Безопасные платежи» Иван совершил бы транзакцию без таких неприятных последствий.

Перехватить данные, передаваемые по незащищенной публичной сети, намного проще, чем когда используется безопасное подключение. А технология «Безопасные платежи» (или ее аналоги) даже в незащищенной публичной сети позволяет спокойно пользоваться всеми удобствами онлайн-банкинга.





# *Письмо, которое не ждешь*

Мария работает психологом и свой день начинает с проверки почты в браузере, ожидая от клиентов подтверждения назначенных встреч. Она замечает новое сообщение от своей социальной сети, в котором ей предлагают сменить пароль на более надежный. Мария переходит по ссылке в письме, подтверждает существующий пароль (который у нее совпадает с паролем от почты), а затем пишет новый пароль, заменив одну букву на знак вопроса.

Она возвращается к разбору входящих писем, довольная, что теперь ее учетная запись лучше защищена от взлома, а вскоре вовсе забывает об этом письме...

...Пока не приходит письмо от злоумышленников, которые угрожают опубликовать данные обо всех клиентах, приходивших к Марии на терапию.

## КАК ТАКОЕ ПРОИЗОШЛО?

Мария стала жертвой фишинга. Сайт социальной сети выглядел так же, как тот, на который она заходила тысячи раз, и тем не менее он был поддельным. Получив доступ к профилю Марии в социальной сети, злоумышленники узнали о ее психологической практике. Затем они попытались взломать ее рабочую почту, воспользовавшись паролем к аккаунту в социальной сети, который был получен с помощью фишинга. Пароль подошел, и злоумышленники получили доступ ко всем письмам Марии со всеми вложенными файлами, в одном из которых был полный список клиентов с контактными данными.

## ЧТО НУЖНО БЫЛО СДЕЛАТЬ?

Во-первых, Мария должна была знать, что никакие (кроме мошеннических) организации и сайты никогда не запрашивают контактные данные пользователей по электронной почте. Но даже когда она открыла ссылку, качественное защитное ПО предупредило бы ее о том, что сайт поддельный.

Во-вторых, ни в коем случае нельзя было пользоваться одним паролем и для рабочей почты, и для личной страницы в социальной сети.

# IT-БЕЗОПАСНОСТЬ МАЛОГО БИЗНЕСА: ПРОСТО И ЭФФЕКТИВНО

Предприятия малого и среднего бизнеса ежедневно сталкиваются почти с таким же количеством угроз, что и крупные компании. В связи с этим небольшим предприятиям необходимо решение, использующее максимально эффективные механизмы для обеспечения защиты от всех актуальных угроз. При этом такое решение должно быть понятным, простым и удобным в использовании, ведь в большинстве подобных организаций нет штатного IT-специалиста.

«Лаборатория Касперского» учла все эти требования при создании защитных решений для малого и среднего бизнеса. Так, Kaspersky Small Office Security рассчитан не на IT-администраторов, а на рядовых пользователей. В этом продукте реализованы передовые механизмы защиты, при этом его легко установить и настроить. Такое решение позволяет управлять IT-безопасностью небольшой компании без специальной подготовки. А организациям с более сложной IT-инфраструктурой подойдет комплексное решение Kaspersky Endpoint Security для бизнеса, которое обеспечит надежную защиту компании и в дальнейшем будет расти вместе с ней.

Ознакомиться с продуктами «Лаборатории Касперского» и выбрать защиту для своего бизнеса вы можете на сайте kasperskysmb.ru.

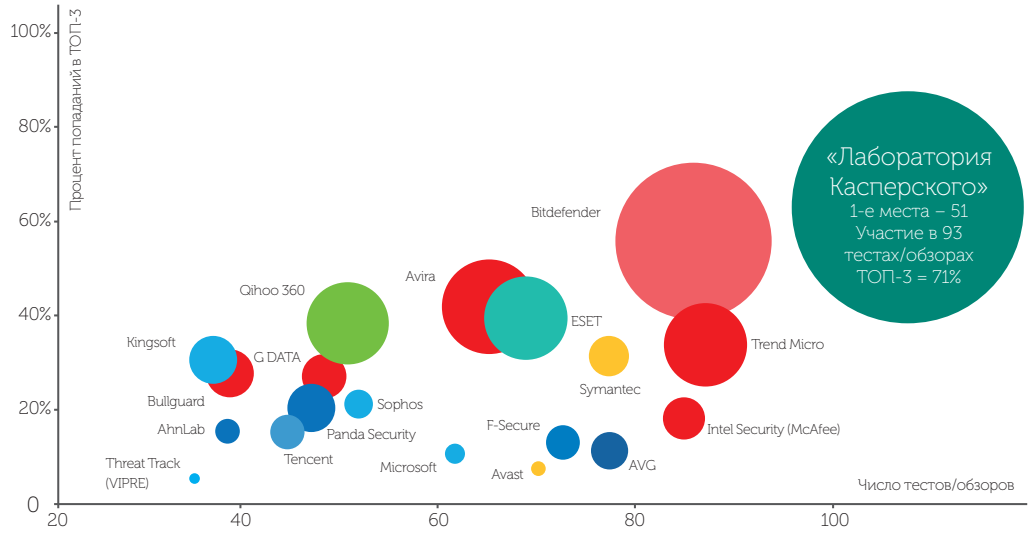
## РАЗВЕ БЕСПЛАТНОЙ ЗАЩИТЫ НЕДОСТАТОЧНО?

Конечно, существуют и бесплатные защитные решения. Однако они не обеспечивают всестороннюю комплексную защиту. Более того, именно версии с ограниченными возможностями распространяются производителями в качестве бесплатных – чтобы стимулировать пользователей перейти на платную версию. Когда речь идет о безопасности вашего бизнеса, нужно всегда пользоваться самой лучшей защитой.

# ПОЧЕМУ «ЛАБОРАТОРИЯ КАСПЕРСКОГО»?

## *Потому что «Лаборатория Касперского» обеспечивает лучшую защиту**

Эффективность продуктов «Лаборатории Касперского» регулярно подтверждается результатами независимых тестов. В 2014 году компания заняла первое место среди производителей защитных решений по показателю TOP-3. По итогам 93 различных испытаний, проведенных авторитетными тестовыми организациями разных стран, решения «Лаборатории Касперского» вошли в тройку лидеров в 71% случаев и 51 раз занимали первое место. Это неоспоримое доказательство того, что «Лаборатория Каперского» предоставляет лучшую в отрасли защиту.




** Примечание*

- *Включает тесты продуктов для бизнеса, домашних пользователей и мобильных приложений за 2014 год*
- *В обзор включены тесты, проведенные следующими независимыми организациями и изданиями: тестовые лаборатории AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs; Virus Bulletin*
- *Диаметр круга соответствует числу занятых первых мест*

Подробнее: kaspersky.ru/top3

# О «ЛАБОРАТОРИИ КАСПЕРСКОГО»

«Лаборатория Касперского» – крупнейшая в мире частная компания, работающая в сфере информационной безопасности, и один из наиболее быстро развивающихся вендоров защитных решений. Компания входит в четверку ведущих мировых производителей решений для обеспечения IT-безопасности пользователей конечных устройств (IDC, 2014).
С 1997 года «Лаборатория Касперского» создает инновационные и эффективные защитные решения и сервисы для крупных корпораций, предприятий среднего и малого бизнеса и домашних пользователей.
«Лаборатория Касперского» – международная компания, работающая почти в 200 странах и территориях мира; ее технологии защищают более 400 миллионов пользователей по всему миру. Более подробная информация доступна на сайте www.kaspersky.ru.

+7 (495) 737-34-12
sales@kaspersky.com
www.kasperskysmb.ru