Киберугрозы и информационная безопасность в корпоративном секторе: тенденции в мире и в России

Для выявления основных проблем и тенденций в области IT-безопасности в корпоративном секторе «Лаборатория Касперского» провела глобальное исследование, в рамках которого были опрошены специалисты, отвечающие за информационную безопасность в компаниях разного масштаба. Исследование проводилось совместно с агентством B2B International в 14 странах мира, включая Россию.

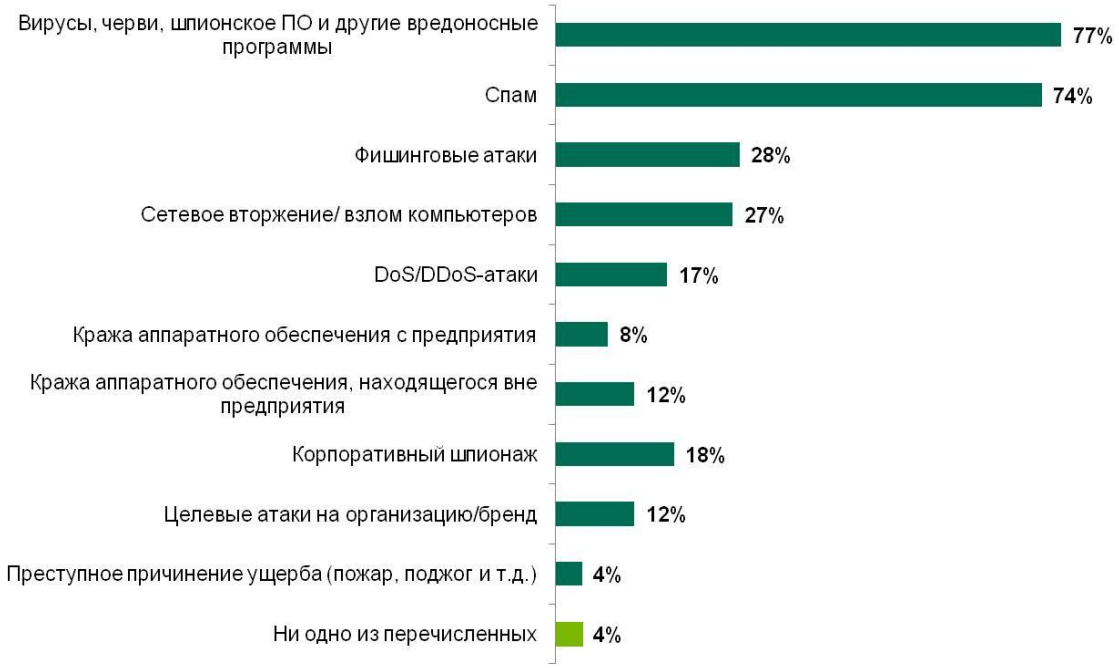
9 из 10 компаний сталкиваются с внешними киберугрозами

Результаты исследования показали, что уровень опасности в сфере информационных технологий чрезвычайно высок. За последний год 91% компаний, представители которых приняли участие в опросе, сталкивались с угрозами информационной безопасности. В России этот показатель еще выше – 96%. Более того, ситуация становится только хуже: почти половина участников исследования утверждает, что количество кибератак за этот период увеличилось, и лишь 8% говорят о незначительном снижении их числа.

Многие организации пострадали от киберпреступников: например, треть вирусных атак (а в российских компаниях – почти половина) закончилась потерей данных, при этом для 10% фирм это была важная для бизнеса информация.

Перечисляя киберугрозы, которые представляются им самыми значительными, большинство участников исследования во всем мире ставят на первое место вирусы, шпионское ПО и другие вредоносные программы (61%). Спам назвали источником угрозы 56% респондентов. Третье место (36%) заняли фишинговые атаки, за ними идут сбои, вызванные проникновением в корпоративную сеть (24%), и DDoS-атаки (19%).

Типы внешних угроз, с которыми сталкивались российские компании



Вредоносное ПО – самая частая причина проблем с безопасностью, опережающая в рейтинге спам и фишинговые атаки. Примечательно, что первые пять мест в рейтинге занимают внешние угрозы

Опрос российских IT-специалистов показал, что чаще всего сбои в системе безопасности приводят к потере данных о платежах (13%), интеллектуальной собственности (13%), клиентских баз (12%) и информации о сотрудниках (12%).

84% российских компаний не считают себя объектом кибератак

В условиях роста количества киберугроз вызывает интерес и то, как оценивают защищенность компаний в IT-сфере представители этих организаций. 60% опрошенных в России (в мире – 59%) уверены в том, что их корпоративные сети хорошо защищены. Любопытно, что треть участников исследования являются фаталистами, полагая, что сбои в работе системы защиты трудно предсказать и почти невозможно предотвратить. В России таких компаний меньше – 23%.

Только 16% респондентов в России считают свою организацию объектом целевых кибератак – приблизительно вдвое меньше, чем в целом по миру (30%).

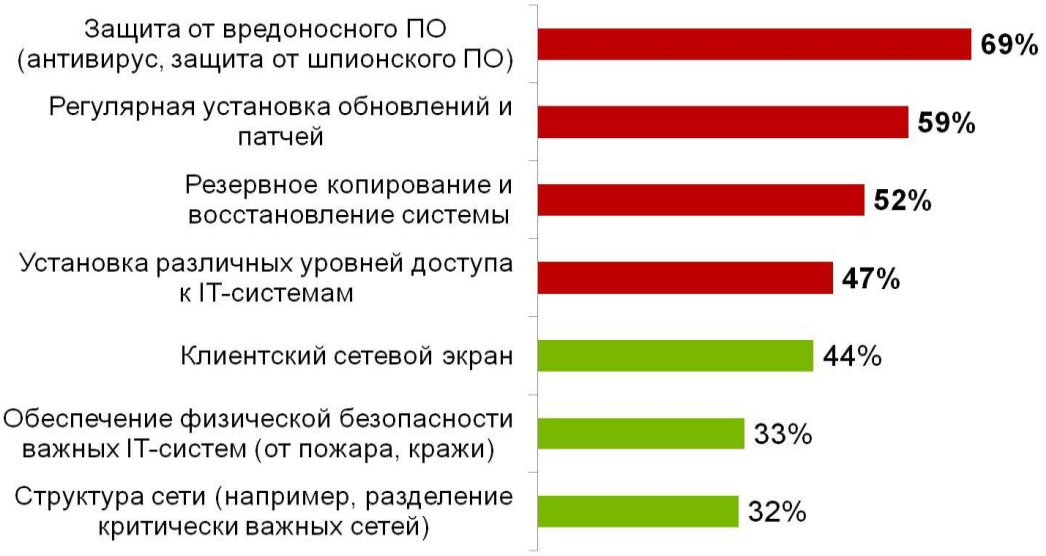
31% российских организаций не используют антивирусную защиту в полной мере

Результаты исследования показывают, что представители компаний хорошо осведомлены об уровне опасности, однако степень защищенности бизнеса от киберугроз оставляет желать лучшего: некоторые компании плохо защищены, в ряде организаций выбранные меры защиты не соответствуют характеру опасности и серьезности возможных последствий для бизнеса.

Согласно мнению специалистов, принимавших участие в опросе, главной задачей IT-персонала является обеспечение бесперебойной и четкой работы системы информационной безопасности. Все участники исследования назвали информационную стратегию компании одной из важнейших в бизнесе, причем в России по значимости она даже выше, чем финансовая, маркетинговая и кадровая стратегии.

Самые популярные меры, применяемые для защиты от киберугроз в компаниях в мире и в России, – антивирусная защита, клиентские межсетевые экраны, установка обновлений (в том числе и устраняющих уязвимости в программном обеспечении) и резервное копирование данных. Тем не менее, 31% компаний в России не полностью внедрили антивирусную защиту (для сравнения – в Великобритании и США антивирусная защита внедрена в 92% и 82% компаний соответственно). Одна российская компания из ста не имеет вообще никакой защиты (а в мире – 3% организаций).

Наиболее широко применяемые в России меры по обеспечению информационной безопасности



Защита от вредоносного ПО – мера безопасности, наиболее широко применяемая в России. И все же 31% компаний по-прежнему не используютя ее в полном объеме

В 84% российских компаний ограничен доступ к социальным сетям

IT-персонал как во всем мире, так и в России считает, что общение в социальных сетях и совместный доступ к файлам являются наиболее опасными видами онлайн-активности конечных пользователей с точки зрения информационной безопасности. В России этой проблемой озабочены больше, чем в других странах: опасность в социальных сетях видят 52% опрошенных, в то время как в среднем по миру они вызывают беспокойство у 35% IT-специалистов.

Наиболее опасные виды онлайн-активности сотрудников с точки зрения IT-безопасности

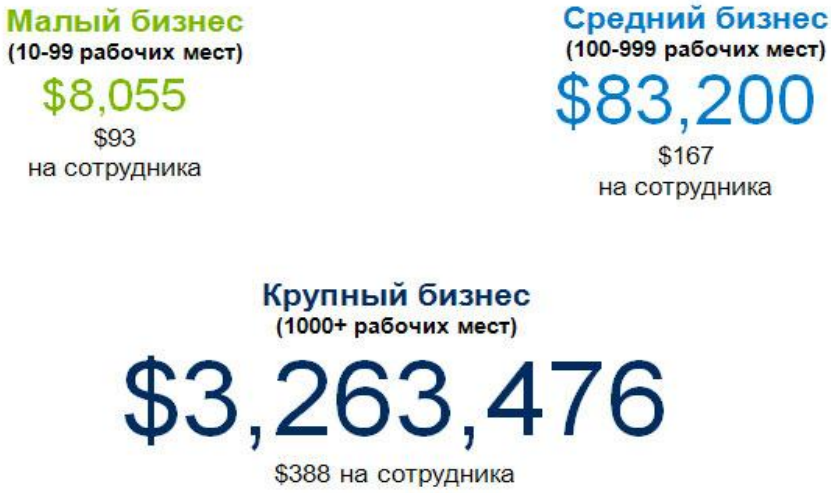
Вид активности/ Приложение	В целом	США	Россия	Китай
Общий доступ к файлам/ P2P	**55%**	62%	50%	44%
Социальные сети	**35%**	44%	52%	26%
Загрузка файлов, передача файлов, FTP-сервисы	**34%**	33%	44%	28%
Доступ к веб-сайтам	**32%**	35%	42%	29%
Личная электронная почта/ веб-почта	**31%**	36%	22%	28%
Службы мгновенного обмена сообщениями	**23%**	20%	19%	36%
Онлайн-игры	**21%**	19%	16%	21%
Потоковое видео/ Интернет-ТВ	**13%**	8%	12%	21%
Сетевой подход в маркетинге	**11%**	5%	4%	24%
Голосовая связь по IP-протоколу (VoIP)	**10%**	5%	9%	17%

Во всех странах социальные сети рассматриваются как одна из важнейших угроз, но в России их опасаются больше всего

Поскольку сотрудники недостаточно информированы об угрозах IT-безопасности, компании предпочитают ограничивать их общение в соцсетях. В 84% компаний в России сотрудники не имеют доступа к сайтам и приложениям социальных сетей, или доступ к подобным ресурсам ограничен. В мире этот показатель несколько ниже – 72%.

При проведении исследования много внимания было уделено анализу ресурсов, которыми располагают компании для борьбы с угрозами. В настоящее время затраты на обеспечение безопасности корпоративной сети в год составляют в среднем $8000 для малого бизнеса, $80 000 для среднего бизнеса и $3,2 миллиона для крупных корпораций. Важно отметить, что большинство участников исследования считают бюджет, выделяемый в их организациях на информационную безопасность, недостаточным и требующим увеличения.

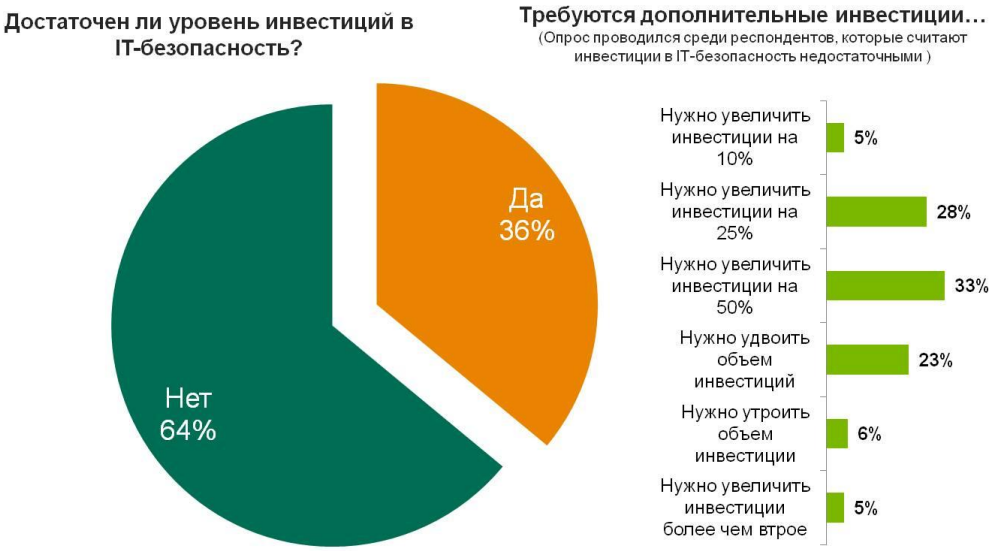
Инвестиции в IT-безопасность (в среднем в год)



В крупных компаниях на одного сотрудника приходится больше средств, вкладываемых в IT-безопасность

Достаточным уровень инвестиций в IT-безопасность называют 55% опрошенных. В России ситуация отличается в худшую сторону – объем вкладываемых средств удовлетворительным признали лишь 36% участников исследования. При этом, по мнению IT-специалистов, не хватает не только финансирования: 70% респондентов ссылаются на нехватку персонала, знаний или недостаточность системных ресурсов.

Большинство российских IT-специалистов считает уровень инвестиций в информационную безопасность недостаточным



95% опрошенных в России считают, что инвестиции нужно увеличить на 25% и более

В большинстве компаний более популярен реактивный подход к IT-безопасности. Это в полной мере относится и к инвестициям: компании начинают вкладывать деньги в систему защиты после того, как инцидент уже произошел.

Однако зачастую распределение финансов в компаниях осуществляется без учета важности вопросов информационной безопасности. 63% представителей компаний считают, что их руководство придает проблеме защиты корпоративных сетей недостаточное значение. В России эта проблема стоит более остро – 73% принявших участие в опросе думают, что их руководители должны проявлять больший интерес к вопросам IT-безопасности.

44% российских компаний считают киберугрозы одним из главных бизнес-рисков в будущем

Проводя исследование, «Лаборатория Касперского» стремилась не только узнать, как IT-специалисты оценивают сложившуюся ситуацию в области информационной безопасности, но и определить, как изменятся киберугрозы в ближайшие несколько лет.

Рост числа сотрудников, работающих дистанционно, ставит перед IT-специалистами российских компаний новую задачу – обеспечить безопасность мобильных устройств. 49% респондентов утверждают, что их компании сейчас гораздо сильнее озабочены этим вопросом, чем год назад. Эти цифры соответствуют общемировой тенденции – всего в мире подобную озабоченность выражают 55% опрошенных.

Постоянно растет и количество личных устройств, которые сотрудники используют в рабочих целях: сегодня практически всем компаниям, в особенности крупным, приходится иметь дело с большим числом пользовательских устройств, подключенных к сети. Три четверти компаний ожидают, что через год таких устройств станет еще больше. Поскольку ни у кого нет сомнения в том, что число сотрудников, работающих удаленно, продолжит увеличиваться, мобильные устройства должны быть защищены специальными политиками безопасности и антивирусными решениями, как и обычные персональные компьютеры. Однако в настоящий момент специальная политика безопасности для мобильных устройств действует лишь в 24% российских организаций, еще меньше компаний требуют шифрования данных, передаваемых этими устройствами. При этом компании, в которых такие меры были приняты, оценивают их как малоэффективные. Неудивительно, что треть всех организаций как в России, так и в мире считает использование мобильных устройств слишком рискованным для бизнеса.

Инновации в бизнесе не ограничиваются новыми устройствами. Новые технологии тоже расцениваются многими организациями как возможные источники рисков информационной

безопасности. Так, например, 23% респондентов рассматривают облачные технологии как угрозу. В России таких компаний больше – 29%.

Подобный взгляд на облачные технологии не способствует их внедрению. Более 40% компаний как в России, так и в мире неохотно используют инновации из-за потенциальных рисков.

В каждой четвертой компании в мире наиболее значимой внешней киберугрозой в будущем называют сетевые вторжения или хакерские атаки. В России процент опасающихся этих угроз, больше – 34% опрошенных. Еще четверть участников опроса как во всем мире, так и в России главной информационной угрозой в течение следующих нескольких лет считает вирусы, черви и другие вредоносные программы.

Необходимо отметить, что IT-специалисты прогнозируют дальнейшее развитие и увеличение количества информационных угроз. В настоящее время лишь около 15% респондентов в России и в мире считают киберугрозы одним из трех наиболее критичных для своей организации бизнес-рисков, однако почти половина опрошенных (44%) видит их одной из главных угроз для компаний через 2 года.

70% российских компаний считают, что у них недостаточно ресурсов для борьбы с киберугрозами

Исследование показало, что IT-специалисты как в мире, так и в России достаточно хорошо информированы об угрозах информационной безопасности. Почти у половины респондентов ситуация вызывает растущее беспокойство. За последний год практически во всех компаниях были инциденты, связанные с киберугрозами, а почти треть организаций столкнулась с проблемой потери конфиденциальной информации.

В то же время в большинстве компаний считают, что средств, выделяемых из бюджета предприятия на обеспечение информационной безопасности, недостаточно, и что финансирование необходимо увеличить. Кроме того, нередко не используются даже существующие решения – несмотря на то, что защита от вредоносных программ является неотъемлемой частью общей системы безопасности, внедрена она только в 69% организаций.

Очевидно, что отношение к информационной защите бизнеса должно измениться. В 70% российских компаний считают, что для надежной защиты от киберугроз им предстоит еще многое сделать. Речь идет об увеличении числа специалистов службы IT-безопасности, большем объеме инвестиций и внедрении новейших решений и технологий.

Результаты проведенного исследования помогли экспертам «Лаборатории Касперского» определить актуальные проблемы информационной безопасности в корпоративном секторе. Полученные данные используются при разработке новых решений для защиты предприятий, а также в работе с партнерами и заказчиками.

* Изучалась ситуация в организациях разного масштаба – небольших (с количеством сотрудников 10-99 человек), средних (от 100 до 999 сотрудников) и крупных (со штатом более 1000 человек). В опросе, который проводился во втором и третьем квартале 2011 года, приняли участие более 1700 IT-специалистов из 14 стран мира. Важно отметить, что все респонденты участвуют в оценке угроз информационной безопасности и оказывают влияние на формирование IT-политики в своих компаниях.