2013

Информационная безопасность бизнеса

Исследование текущих тенденций в области информационной безопасности бизнеса

www.kaspersky.ru/business

KASPERSKY lab

ВВЕДЕНИЕ

«Лаборатория Касперского» является крупнейшей в мире частной компанией, занимающейся разработкой защитных решений для домашних пользователей и корпоративных IT-инфраструктур. Чтобы всегда предоставлять своим клиентам надежную и отвечающую их потребностям защиту, компания регулярно проводит специализированные исследования, позволяющие выявить главные риски и угрозы, которые беспокоят представителей бизнеса.

С 2011 года «Лаборатория Касперского» совместно с международной аналитической компанией B2B International проводит ежегодный глобальный опрос IT-специалистов малых, средних и крупных компаний по всему миру. Исследование позволяет узнать мнение этих профессионалов относительно самых важных вопросов безопасности корпоративной IT-инфраструктуры: о корпоративном защитном программном обеспечении, об уровне осведомленности о киберугрозах, а также о том, с какими проблемами в области кибербезопасности чаще всего приходится сталкиваться компаниям, как они эти проблемы решают и чего ожидают в этой сфере в будущем.

Сравнение новых данных с теми, что были получены в предыдущие годы, позволяет выявить тенденции, характерные для исследуемой области, и проанализировать их, что в конечном итоге дает максимально полную и, по нашему мнению, объективную картину ландшафта угроз, проблем и перспектив в сфере информационной безопасности бизнеса.

ТЕРРИТОРИАЛЬНЫЙ ОХВАТ И РЕСПОНДЕНТЫ ОПРОСА

Отчет B2B International подготовлен по итогам интервью 2895 IT-специалистов, работающих в компаниях из 24 стран мира, включая Россию (Центральный, Южный, Северо-Западный, Дальневосточный, Северо-Кавказский, Сибирский, Уральский и Приволжский федеральные округа). Все участники опроса имеют влияние на формирование политики своих компаний в области IT и обладают хорошими знаниями в отношении как рисков информационной безопасности, так и функционирования других бизнес-подразделений компании. В опросе представлено мнение сотрудников компаний малого и среднего бизнеса, а также крупных корпораций.

ОСНОВНЫЕ ТЕНДЕНЦИИ

Согласно результатам глобального опроса, приоритетом №1 для большинства компаний является разработка четкой стратегии развития IT-инфраструктуры. В России значимость этого вопроса существенно ниже, что не может не влиять на принятие решений в области информационной безопасности. Участившиеся инциденты IT-безопасности и связанные с ними крупные финансовые потери послужили основными причинами повышенного внимания компаний к обеспечению безопасности своей IT-инфраструктуры.

Основные результаты опроса:

- Только треть российских компаний (34%) уделяет достаточно времени и средств на разработку и внедрение политик информационной безопасности.

- Практически все IT-специалисты российских компаний (95%) недооценивают скорость появления новых угроз.

- Главной угрозой IT-безопасности в России остаются вирусы и другое вредоносное ПО. Основные изменения по сравнению с предыдущими исследованиями – уменьшение количества хакерских атак и сетевых вторжений и участившаяся утрата ценных корпоративных данных в результате утери и кражи мобильных устройств.

- 95% респондентов сообщили о том, что в их компаниях был зарегистрирован как минимум один инцидент информационной безопасности, связанный с использованием мобильных устройств (смартфонов и планшетов). Интересно, что беспокойство в компаниях вызывают не возможные атаки на устройства, а тот факт, что их использование повышает риск утечки важных корпоративных данных.

- Атаки с использованием вредоносного ПО лидируют среди всех угроз для российских компаний.

- В 65% инцидентов утечка данных привела к нарушениям функционирования компании, а в 55% случаев серьезно пострадала ее репутация.

- Успешные атаки с использованием известных брешей в системе информационной безопасности привели к потере в среднем около $14 тыс. для СМБ-компаний и около $791 тыс. для крупных компаний (за один инцидент).

- 62% компаний вкладывают средства в дополнительную программно-аппаратную защиту своей IT-инфраструктуры.

- 77% компаний после успешной атаки предпринимают меры для предотвращения подобных инцидентов в будущем, что приводит к дополнительным расходам.

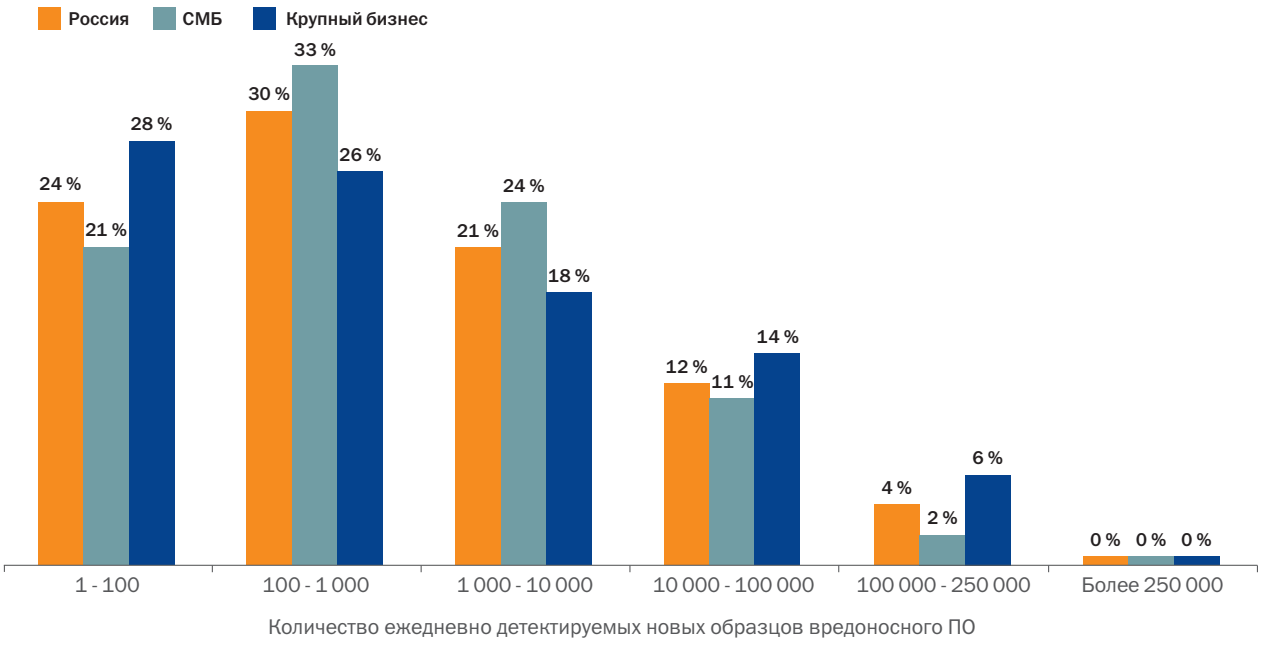
- 68% компаний после инцидента вынуждены раскрывать информацию о нем по требованию третьей стороны. Крупным предприятиям чаще приходится передавать информацию регуляторам и прессе. Вынужденное раскрытие информации такого рода наносит дополнительный ущерб репутации компаний.

РАССТАНОВКА ПРИОРИТЕТОВ

Наиболее приоритетные задачи и проблемы, которые стоят перед IT-отделами

Защита данных остается приоритетом №1 для российских IT-специалистов в 2013 году – этим вопросом обеспокоены более 40% компаний. Следующим пунктом идут политики восстановления IT-систем после сбоев, важность которых признали почти 30% опрошенных (в прошлом году показатель был на 4% ниже). Наиболее значительно снизился интерес к таким мерам, как инвестиции в IT и обучение пользователей работе с IT-системами. Вопрос контроля использования мобильных устройств, который ранее не выделялся в отдельный блок в подобных исследованиях, теперь имеет довольно высокий приоритет и составляет 22%.

КАК КОМПАНИИ ОЦЕНИВАЮТ КИБЕРУГРОЗЫ?



Количество ежедневно детектируемых новых образцов вредоносного ПО

Как выяснилось в ходе опроса, абсолютное большинство компаний недооценивают масштабы современных киберугроз. По данным «Лаборатории Касперского», ежедневно появляется около 200 тыс. новых образцов вредоносного ПО. Близкую оценку дали лишь 4% опрошенных, в то время как около 95% занизили цифру. В этом отношении сотрудники российских компаний повторяют ошибку своих зарубежных коллег: лишь 6% участников глобального опроса назвали цифру, близкую к среднестатистической. Любопытно, что среди российских IT-специалистов никто не переоценил угрозу, в то время как в других странах 4% опрошенных существенно завысили показатель.

СМБ-компании оценивают масштаб киберугроз более легкомысленно, чем крупный бизнес: в 33% небольших предприятий ошибочно полагают, что ежедневно появляется менее 1 000 образцов уникального вредоносного кода, и лишь 2% назвали правильный диапазон – от 100 000 до 250 000.

Руководствуясь только этими данными, сложно дать объективную оценку готовности компаний к защите от инцидентов информационной безопасности. Тем не менее, адекватная оценка уровня угроз может оказать серьезное влияние на решения, которые компания принимает при подборе средств для защиты своей IT-инфраструктуры.

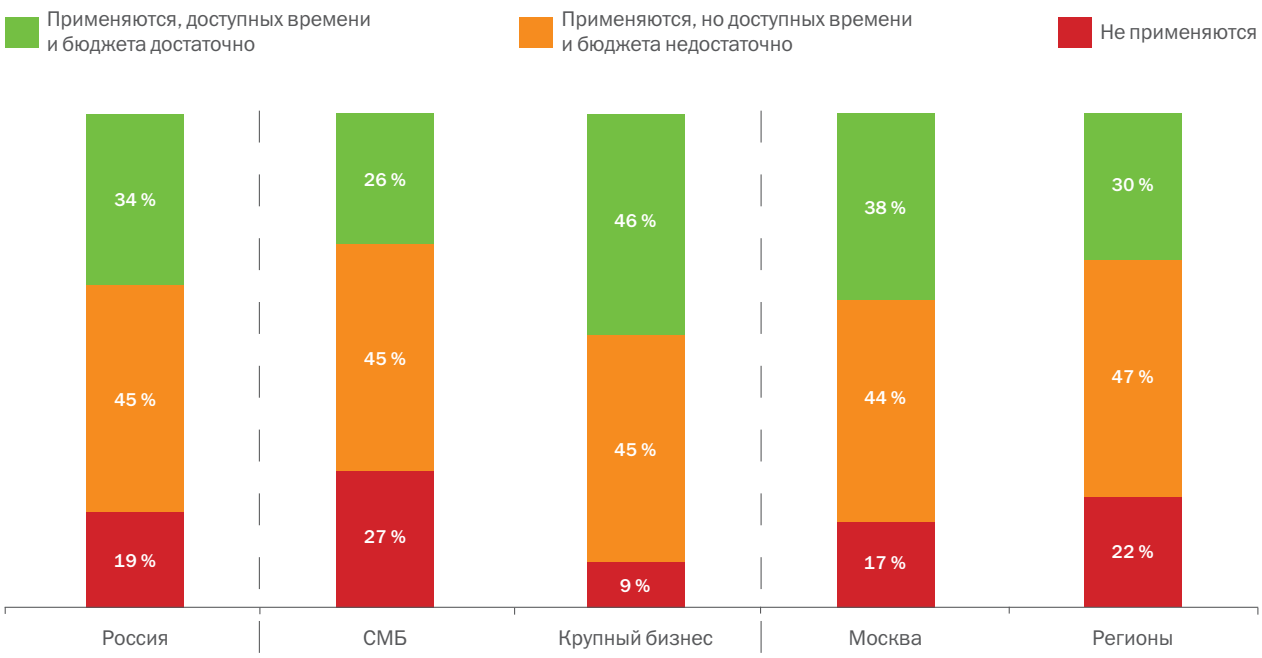
ПРИМЕНЯЕМЫЕ МЕТОДЫ ЗАЩИТЫ

Антивирусная защита – наиболее распространенная мера для обеспечения информационной безопасности IT-инфраструктуры в компаниях любых размеров по всему миру. Около 74% респондентов сообщили о том, что в их организациях развернуты полнофункциональные решения для защиты от вредоносного ПО. Регулярное обновление ПО и установка исправлений (патчей) – по-прежнему на втором месте (59%), но по сравнению с прошлым годом популярность этой меры для всех компаний стала ниже. Наибольший рост (+7%) показали такие методы, как разграничение уровня доступа к различным участкам IT-инфраструктуры (49%) и шифрование данных на съемных носителях (24%). Кроме того, несколько более популярным (+5%) стал метод разграничения политик безопасности для съемных устройств.

Примечательно, что помимо трех основных методов защиты, компании малого и среднего бизнеса уделяют значительное внимание контролю съемных устройств (35%) и контролю приложений (31%).

Также в ходе опроса выяснилось, что компании принимают дополнительные меры безопасности, которые в прошлом году либо применялись нечасто, либо вовсе не использовались. К таким мерам относятся: контроль съемных устройств, контроль приложений, шифрование файлов и папок, а также внедрение антивирусных решений для мобильных устройств.

ПОЛИТИКИ IT-БЕЗОПАСНОСТИ



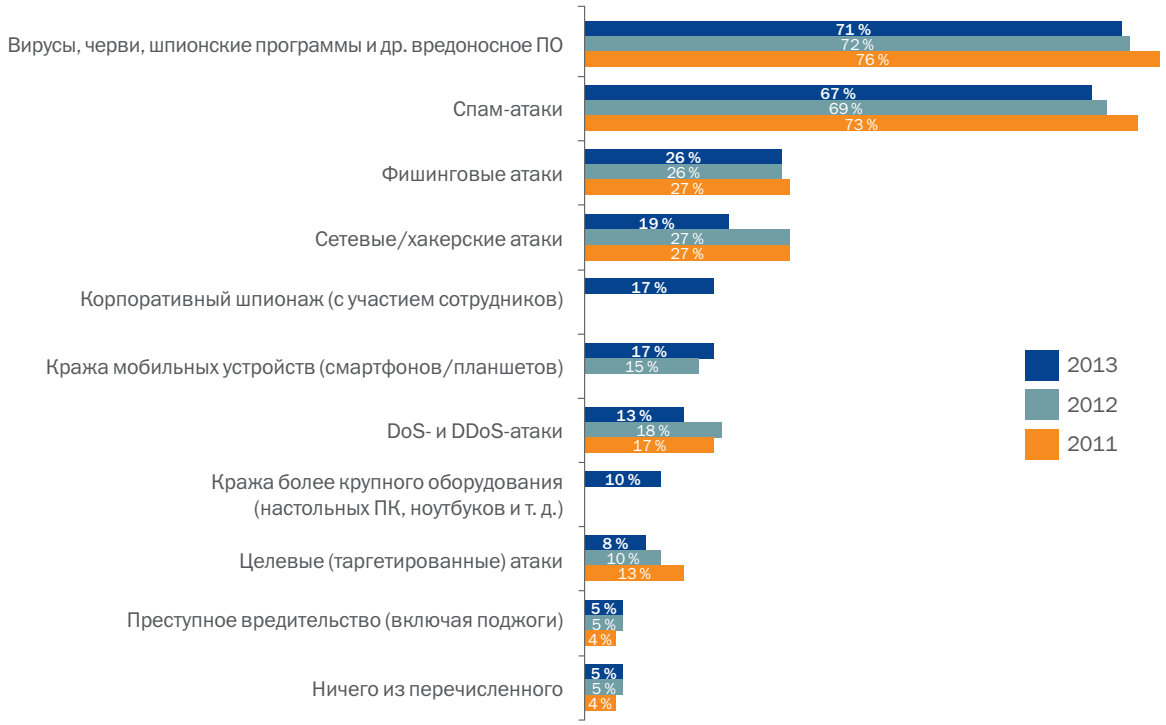
Выделен ли в вашей компании бюджет и время специально для разработки общих политик IT-безопасности?

Разработка и внедрение политик IT-безопасности – это еще одно средство обеспечения дополнительной защиты компании. Всего подобные политики существуют в 79% российских компаний (интересно, что во всем мире этот показатель составляет порядка 86%). Но лишь 34% российских респондентов отметили, что в их компаниях на разработку и внедрение политик выделяется достаточно времени и бюджетных средств, в то время как в 19% компаний этот вопрос даже не рассматривается. Доля компаний, где время и средства выделяются, но недостаточно, составляет 45% – в среднем такая оценка характерна для всех российских компаний, вне зависимости от их размера и территориального положения.

Лучше всего с разработкой и внедрением политик IT-безопасности дело обстоит в крупных компаниях – почти половина (46%) респондентов из таких компаний удовлетворены объемом времени и ресурсов, выделяемых на решение этой задачи, и лишь 9% признались, что в их компаниях отсутствует соответствующая отдельная статья расходов. В сегменте СМБ только 27% компаний специально выделяют средства на внедрение политик IT-безопасности и только 26% опрошенных удовлетворены объемом этих средств.

Если же обратиться к региональному делению, то в Москве ситуация немного отличается в лучшую сторону по сравнению с другими регионами России, что можно объяснить размещением штаб-квартир многих крупных предприятий в столице.

ИНЦИДЕНТЫ IT-БЕЗОПАСНОСТИ: ВНЕШНИЕ УГРОЗЫ



В течение года IT-инфраструктура 95% российских организаций как минимум один раз подверглась внешней атаке. Вредоносное ПО по-прежнему является самой серьезной среди внешних угроз – ее назвали 71% представителей всех компаний. Спам-атаки продолжают удерживать второе место (в них видят угрозу 67% компаний), хотя их популярность за последние три года стабильно снижается (73% в 2011 году, 69% годом позже). Намечается смещение значимости угроз с сетевых вторжений, частота которых снизилась с 27% до 19%, в сторону фишинговых атак, которые вышли на третье место с показателем 26%. Кроме того, выросла (с 15 до 17%) доля новых угроз, таких как утрата данных в результате утери или кражи мобильных устройств. В этом году респондентам было впервые предложено оценить такие угрозы, как корпоративный шпионаж (с участием сотрудников компании) и кража более крупного оборудования (настольных ПК и ноутбуков), которые сразу получили 17% и 10% соответственно.

Любопытно, что в регионах атаки с использованием вредоносного ПО отмечаются чаще: данную угрозу указали 74% респондентов, в то время как в Москве этот показатель самый низкий – 69%. Также региональные компании чаще беспокоят фишинговые атаки (28%) и кража более крупного оборудования (12%).

ОЦЕНКА ПОТЕРЬ ОТ ВНЕШНИХ УГРОЗ

Один из ключевых параметров, позволяющих определить, насколько серьезный ущерб причинила та или иная атака, – это наличие или отсутствие в атакованной компании утечки данных. В ходе опроса выяснилось, что для 40% компаний (что на 5% больше среднемирового показателя) самыми разрушительными были атаки с использованием вредоносного ПО. Эти атаки в 9% случаев привели к утечке ценных конфиденциальных данных, разглашение которых причинило ущерб бизнесу предприятия.

Следом на одном уровне в 13% находятся корпоративный шпионаж, хакерские и фишинговые атаки. Любопытно, что хакерские атаки потеряли 5% по сравнению с прошлым годом, а фишинговые атаки, хотя и встречались достаточно часто, привели к ощутимым потерям для бизнеса всего в 3% случаев.

ИНЦИДЕНТЫ IT-БЕЗОПАСНОСТИ: ВНУТРЕННИЕ УГРОЗЫ

С внутренними инцидентами информационной безопасности в течение года сталкивались 87% организаций. Внутренней угрозой номер один являются уязвимости в программном обеспечении, используемом в организации. По сравнению с результатами прошлогоднего опроса доля подобных инцидентов выросла с 48% до 51%. На втором месте с показателем в 27% – случайные утечки данных, спровоцированные сотрудниками компании.

Третье место (21%) поделили между собой преднамеренная утечка/распространение данных персоналом и инциденты, связанные с утерей или кражей мобильных устройств сотрудников. Еще одной важной угрозой (17%) стала утечка данных/незащищенный обмен корпоративной информацией через мобильные устройства (по электронной почте, через SMS и т. д.).

Региональные компании сильнее страдают от мошенничества сотрудников, не связанного с использованием информационных технологий (19%). В Москве с подобными угрозами сталкивается 12% компаний, а всего по России их выделили 15% респондентов.

В России из пяти основных угроз лишь две связаны с использованием смартфонов и планшетов, в то время, как по данным глобального исследования, четыре из пяти наиболее значимых типов внутренних инцидентов безопасности связаны с мобильными устройствами. Это свидетельствует о более медленном развитии тренда BYOD в нашей стране, однако позволяет прогнозировать направление развития внутренних угроз в будущем.

ОЦЕНКА ПОТЕРЬ ОТ ВНУТРЕННИХ УГРОЗ

Внутренние угрозы приводят к потере данных не реже, чем внешние: 39% респондентов отметили, что их компании пострадали от утечки данных в результате незакрытых уязвимостей в программном обеспечении и при этом 13% из них потеряли важную для бизнеса информацию. На втором месте по размеру ущерба находятся случайные утечки данных, спровоцированные сотрудниками (24%), при этом в 6% случаев была утрачена информация, не подлежащая разглашению.

Третье место с небольшим отставанием занимают инциденты, связанные с умышленным разглашением корпоративной информации (18%); они привели к потере критически важных для бизнеса данных в 9% случаев. На том же уровне (18%) находится утечка информации в результате утери/кражи мобильных устройств сотрудников, а потеря ценных данных при этом произошла в 8% случаев.

Хотя уязвимости в ПО являются основной угрозой, другие внутренние инциденты, связанные с действиями персонала и использованием мобильных устройств, также представляют значительный риск с точки зрения утраты важных для бизнеса конфиденциальных данных.

ОБЩИЙ РЕЙТИНГ УГРОЗ, ПРИВОДЯЩИХ К УТЕЧКЕ ДАННЫХ

В общем рейтинге угроз, послуживших причиной утечки ценных данных в российских компаниях, лидируют атаки с использованием вредоносного ПО (24%). На втором месте – незакрытые уязвимости (14%), а на третьем – случайная утечка данных, спровоцированная сотрудниками (8%).

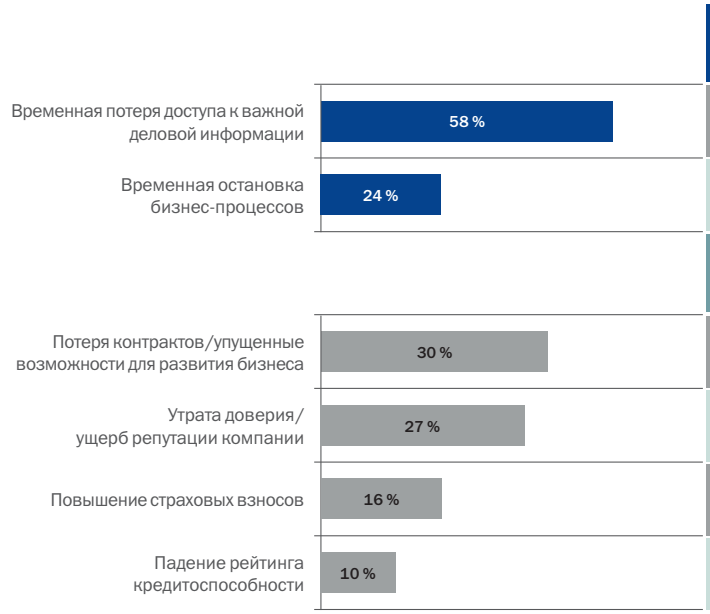
При этом для среднего и малого бизнеса перечисленные выше основные угрозы представляют бóльшую опасность – в результате подобных атак СМБ-компании теряют данные чаще, чем крупные организации (в среднем показатель выше на 5%). Однако когда речь заходит об утечке/незащищенном обмене информацией через мобильные устройства, ситуация меняется: здесь крупные предприятия теряют данные ровно в два раза чаще СМБ-компаний: 10% против 5%. В целом же российские компании теряют данные по этой причине в 7% случаев.

ОЦЕНКА ПОСЛЕДСТВИЙ: ОТ $50 ТЫС. ДО $649 ТЫС. ЗА ОДИН ИНЦИДЕНТ

В 2013 году в рамках глобального опроса Global Corporate IT Security Risks компании B2B International и «Лаборатория Касперского» впервые предложили респондентам дать оценку финансового ущерба, который причиняют компаниям инциденты информационной безопасности. По самым скромным оценкам, ущерб от одного серьезного инцидента для крупных компаний по всему миру составил в среднем $649 тыс. Для предприятий малого и среднего бизнеса ущерб составил в среднем $50 тыс. В некоторых случаях для небольших компаний финансовый ущерб от инцидента сопровождался еще и потерей примерно 5% ежегодной выручки, а иногда и полным прекращением работы компании в одном из регионов.

Примечательно и то, что в зависимости от типа атаки объем финансового ущерба значительно меняется. Например, для крупной компании успешная DDoS-атака может привести к убыткам в размере $527 тыс., а успешная целевая атака – к потере $2,4 млн.

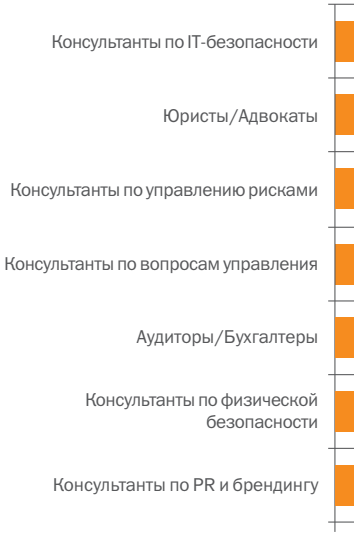
ПОСЛЕДСТВИЯ КИБЕРАТАК В РОССИИ: НАРУШЕНИЕ БИЗНЕС-ПРОЦЕССОВ/УЩЕРБ РЕПУТАЦИИ



	Кратко-временно	Недолго	Довольно долго	Продолжи-тельно
Временная потеря доступа к важной деловой информации	22 %	41 %	27 %	9 %
Временная остановка бизнес-процессов	14 %	51 %	29 %	6 %
	Незначительно, кратковременно	Незначительно, продолжительно	Значительно, кратковременно	Значительно, продолжительно
Потеря контрактов/упущенные возможности для развития бизнеса	26 %	26 %	35 %	14 %
Утрата доверия/ ущерб репутации компании	35 %	32 %	26 %	5 %
Повышение страховых взносов	14 %	50 %	32 %	2 %
Падение рейтинга кредитоспособности	18 %	39 %	36 %	7 %

В 65% случаев утечка данных привела к серьезным нарушениям бизнес-процессов предприятия, а 55% инцидентов причинили значительный ущерб репутации компании. 58% респондентов отметили, что утечка данных вызвала временную утрату доступа к важной деловой информации, и почти в четверти случаев (24%) инцидент привел к потере важных деловых контрактов и упущенным возможностям для развития бизнеса.

ПОСЛЕДСТВИЯ КИБЕРАТАК В РОССИИ: ЗАТРАТЫ НА УСЛУГИ ВНЕШНИХ СПЕЦИАЛИСТОВ



	Никаких доп. расходов	Небольшие доп. расходы	Большие, но краткосрочные доп. расходы	Долгосрочные/ постоянные доп. расходы
Консультанты по IT-безопасности	23 %	49 %	22 %	6 %
Юристы/Адвокаты	23 %	35 %	36 %	5 %
Консультанты по управлению рисками	11 %	53 %	28 %	9 %
Консультанты по вопросам управления	22 %	49 %	20 %	7 %
Аудиторы/Бухгалтеры	26 %	53 %	12 %	7 %
Консультанты по физической безопасности	27 %	42 %	25 %	6 %
Консультанты по PR и брендингу	14 %	46 %	31 %	6 %

88% инцидентов, связанных с утечкой ценных корпоративных данных, потребовали получения пострадавшей компанией дополнительных профессиональных услуг, таких как консультации IT-специалистов, специалистов по управлению рисками, юристов, консультантов по физической безопасности и специалистов в области связей с общественностью. В 38% случаев дополнительные траты на услуги узких специалистов были определены компаниями как значительные.

Две трети случаев (66%) потребовали привлечения консультантов по информационной безопасности. В 36% случаев использовались услуги юристов, которые многими респондентами были оценены как самые дорогостоящие. На третьем месте по востребованности находятся консультации специалистов по управлению рисками – их привлекали в 30% случаев.

ПОСЛЕДСТВИЯ КИБЕРАТАК В РОССИИ: ОЦЕНКА ПОТЕНЦИАЛЬНЫХ ФИНАНСОВЫХ ПОТЕРЬ

Средний ущерб
для СМБ-компаний
от серьезного инцидента

Средний ущерб
для крупных предприятий
от серьезного инцидента

Для расчета среднего ущерба оценивались следующие параметры: затраты на услуги внешних специалистов, упущенные для бизнеса возможности, остановка бизнес-процессов (простой)

В России средний размер ущерба в результате серьезного инцидента кибербезопасности можно оценить в $14 тыс. для малых и средних компаний и $695 тыс. для крупных организаций.

СМБ-компаниям вынужденный простой может обойтись в среднем в $13 тыс., а крупным организациям – в $791 тыс. Упущенные возможности выразились в финансовых потерях, средний размер которых для малых и средних компаний составил $16 тыс., а максимально возможный ущерб, по оценкам опрошенных, мог достигать $375 тыс.

В среднем общие расходы на дополнительные услуги различных специалистов для компаний из сегмента среднего и малого бизнеса составили $6,6 тыс., а для крупных корпораций – $26 тыс. Эти цифры сильно отличаются от данных глобального исследования: во всем мире дополнительные расходы СМБ-компаний составили в среднем $13 тыс., а крупных предприятий – $109 тыс.

В то же время максимальные дополнительные затраты для небольших российских компаний находятся в диапазоне от $150 тыс. до $375 тыс. (в 4% случаев). Для крупных организаций максимальные затраты (в 5% случаев) составили свыше $7,5 млн.

Но и это еще не все. Помимо финансовых убытков, вызванных самим инцидентом, компании расходуют средства на ряд дополнительных защитных мер, призванных, в том числе, снизить вероятность возникновения подобных инцидентов в будущем.

МЕРЫ ПО ПРЕДОТВРАЩЕНИЮ ИНЦИДЕНТОВ В БУДУЩЕМ

Наиболее популярной мерой по предотвращению инцидентов кибербезопасности в будущем является развертывание дополнительных программных и аппаратных решений для защиты IT-инфраструктуры – в целом 62% российских компаний поступают именно так. В 42% случаев они проводят обучение сотрудников безопасной работе с IT-системами, а 29% набирают новый персонал, в обязанности которого входит предотвращение утечки данных.

Крупные корпорации инвестируют в инфраструктуру в 74% случаев, уделяют значительное внимание обучению сотрудников (55%) и подбору дополнительного персонала (42%). Распределение расходов небольших компаний на эти меры сохраняет примерно те же пропорции: в 60% случаев средства вкладываются в инфраструктуру, в 40% – в обучение и в 28% – в новый персонал.

В среднем подбор дополнительного персонала для обеспечения информационной безопасности обходится малым и средним компаниям в $5 тыс., а крупным корпорациям – в $75 тыс. На обучение сотрудников первые тратят около $4,5 тыс., вторые – около $34 тыс. На усовершенствование аппаратно-программных средств защиты своей IT-инфраструктуры СМБ-предприятия в среднем расходуют около $6 тыс., а крупные компании – около $13 тыс.

ПРЕДОТВРАЩЕНИЕ ИНЦИДЕНТОВ: ОЦЕНКА ВОЗМОЖНЫХ ЗАТРАТ

Средние расходы
для СМБ-компаний

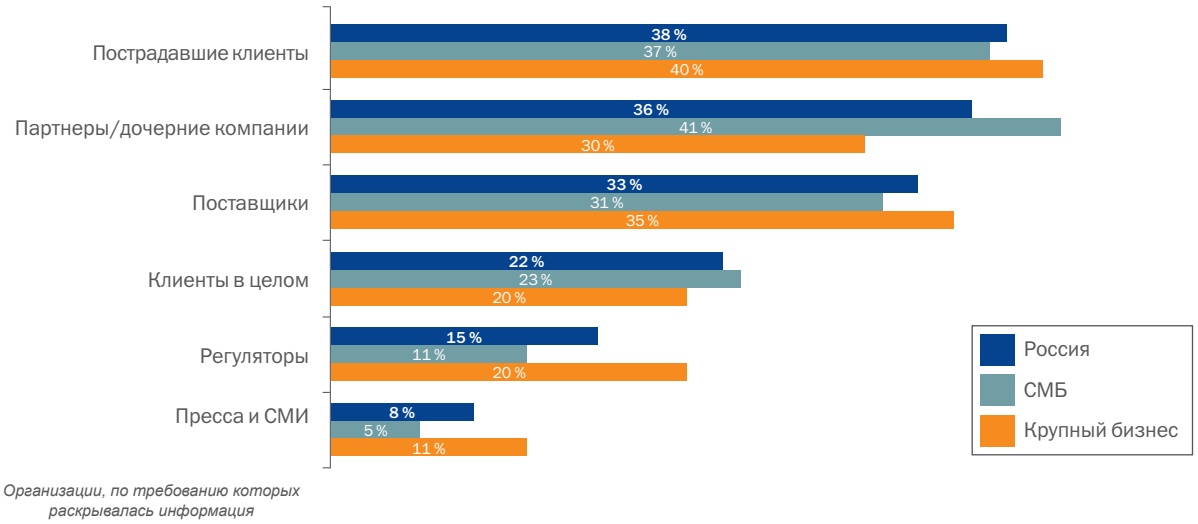
Средние расходы
для крупных предприятий

Для расчета объема дополнительных затрат оценивались следующие параметры: затраты на рекрутинг, на обучение и дополнительные вложения в IT-инфраструктуру

Как и в случае с оценкой прямого ущерба от инцидента, общая оценка дополнительных затрат включает в себя только расходы, характерные для большинства компаний. Например, если причиной инцидента стала халатность сотрудника, вполне может быть, что для устранения его последствий усовершенствование аппаратного и программного обеспечения может не потребоваться. Однако поскольку большинство успешных атак являются следствием недосмотра ответственных сотрудников или отсутствия у них необходимых знаний, 77% компаний приходится нести дополнительные расходы – например, связанные с подбором и обучением персонала. Из этих трат и складывается средняя оценка дополнительных расходов, направленных на предотвращение инцидентов в будущем. Для малых и средних компаний эта цифра составляет $7 тыс., для крупных – $57 тыс.

Кроме того, инциденты кибербезопасности могут не только вызвать финансовые потери, но и нанести серьезный ущерб репутации компании.

ВЫНУЖДЕННОЕ РАСКРЫТИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ



Организации, по требованию которых раскрывалась информация

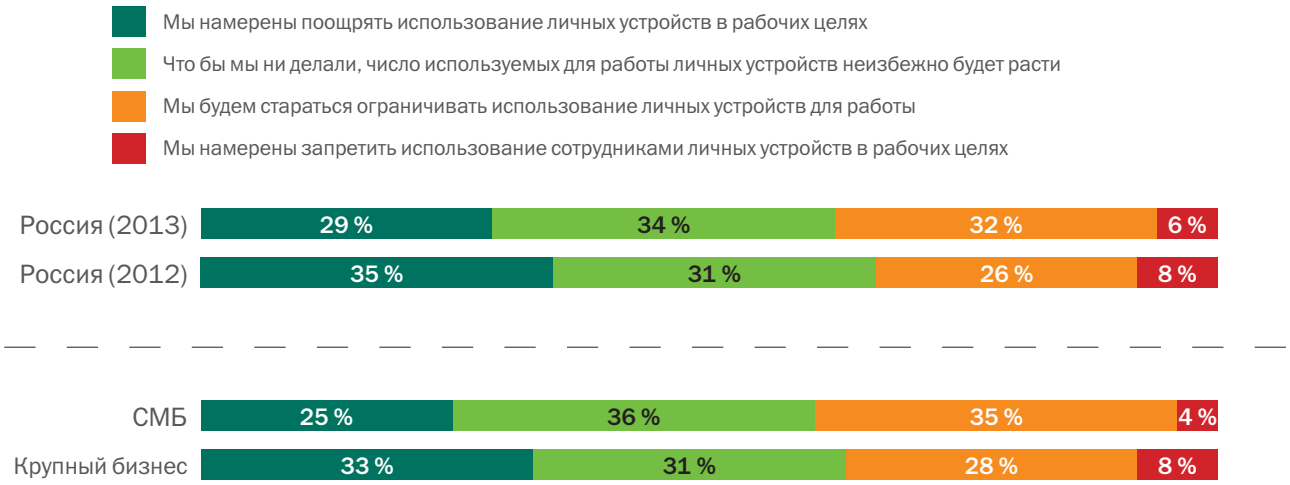
Часто утечка конфиденциальных данных приводит к необходимости информирования об этом инциденте широкой общественности. 68% опрошенных заявили, что после инцидента им пришлось распространить информацию о нем по требованию третьей стороны. Чаще всего (в 38% случаев) такого разглашения требовали клиенты, на которых могла повлиять утечка. Крупные корпорации в большинстве случаев обязаны сообщить об инциденте регулятору, клиентам и прессе, что наносит серьезный удар по деловой репутации таких компаний.

МОБИЛЬНЫЕ УСТРОЙСТВА

Инциденты, связанные с использованием мобильных устройств – в частности, смартфонов – присутствуют в списках как внешних, так и внутренних опасных угроз. Тенденция использования личных смартфонов и планшетов сотрудников для работы (BYOD, Bring Your Own Device) в настоящее время очень актуальна. Быстрый рост числа этих устройств не может не сказываться на безопасности корпоративной сети. По данным опроса, в 95% российских компаний был зарегистрирован как минимум один инцидент информационной безопасности, связанный с мобильными устройствами. При этом в качестве главной угрозы (42%) респонденты назвали утечку важных корпоративных данных. В 33% случаев опасение вызывает возможное заражение мобильных устройств вирусами/несанкционированный доступ к другим устройствам. Эта угроза намного больше беспокоит компании в регионах, особенно небольшие (до 40%). Немного реже (в 31% случаев) респонденты называли проблему кражи устройств.

Для защиты от мобильных угроз компаниям необходимо применять дополнительные политики безопасности, однако пока российский бизнес уделяет этому вопросу мало внимания.

ПОЛИТИКИ В ОТНОШЕНИИ ИСПОЛЬЗОВАНИЯ ЛИЧНЫХ УСТРОЙСТВ СОТРУДНИКОВ ДЛЯ РАБОТЫ



Представители российских компаний реже своих зарубежных коллег видят угрозу для бизнеса в использовании личных устройств сотрудников в рамках корпоративной инфраструктуры. Лишь немногим больше половины респондентов (57%) признали тренд BYOD угрожающим, в то время как во всем мире этот показатель составил 65%. Однако по сравнению с прошлым годом число компаний, которые активно приветствуют использование личных устройств, сократилось с 35% до 29%. При этом число компаний, где планируется регулировать количество и тип устройств, используемых сотрудниками, возросло с 26% до 32%. Несмотря на не слишком высокую оценку угрозы в целом, эти тенденции подтверждают общее настороженное отношение российских компаний к политике BYOD. Хотя стоит отметить, что количество респондентов, принимающих эту тенденцию как неизбежную, увеличилось с 31% до 34%. Такие IT-специалисты отмечают, что, по их мнению, ни одна из запретительных мер уже не способна сколь-либо значительно повлиять на количество личных устройств сотрудников, используемых в рабочих целях.

Среди крупных компаний одна треть приветствует использование сотрудниками своих смартфонов и планшетов для работы, а в 8% это строго запрещено. Среди средних и малых компаний пока только четверть поддерживает BYOD, а запрещают использование личных смартфонов лишь 4%.

ЗАКЛЮЧЕНИЕ И РЕКОМЕНДАЦИИ

Хотя большинство компаний пока не в состоянии оценить реальные масштабы современных киберугроз, в целом бизнес осознает необходимость эффективной защиты от них. Разработка и применение политик информационной безопасности и средств защиты в российских компаниях носит скорее реактивный, чем проактивный характер (особенно в секторе малого и среднего бизнеса).

Вредоносное ПО, а также разнообразные атаки, в которых задействованы сотрудники корпораций и их личные мобильные устройства, стали главными причинами инцидентов, в результате которых компании теряли ценную бизнес-информацию.

Утрата конфиденциальных данных приводит к ощутимым финансовым потерям, которые могут исчисляться миллионами долларов за один инцидент, и это не считая ущерба для репутации компании и возможных последствий вынужденного раскрытия конфиденциальной информации по требованию третьей стороны. Политика Bring Your Own Device – одна из актуальных тенденций, которая уже получила широкое развитие во всем мире. Ее влияние на IT-безопасность бизнеса отмечают и представители российских компаний, однако в меньшей степени, чем их зарубежные коллеги.

Основываясь на результатах исследования, «Лаборатория Касперского» рекомендует компаниям следующие меры, направленные на повышение уровня информационной безопасности.

Инвестиции в безопасность

Инциденты IT-безопасности способны причинить компании значительный финансовый и репутационный ущерб. Его масштабы могут существенно увеличить расходы компании на средства обеспечения информационной безопасности, помогающие избежать утечки важных данных и остановки бизнес-процессов в результате успешной атаки в будущем. В связи с этим важно инвестировать в безопасность IT-инфраструктуры компании заблаговременно.

Профессиональная защита и управление

Количество, разнообразие и сложность вредоносного ПО неуклонно растут. В создание и распространение вирусов, троянских и шпионских программ вовлечены целые преступные группы, которые щедро финансируются. Злоумышленники все чаще используют уязвимости в популярных приложениях, чтобы заразить корпоративные компьютеры. В этих условиях угрозам уже невозможно противостоять без специальных защитных средств. Для обеспечения безопасности необходимы качественное антивирусное решение, эффективная система обновления ПО и удобные средства управления защитой узлов корпоративной сети.

Контроль мобильных устройств

Для многих компаний использование сотрудниками личных мобильных устройств для работы стало повседневной реальностью. Однако широкое распространение этой тенденции не делает менее опасными связанные с ней угрозы. Поэтому если в компании не возбраняется использование личных устройств в рабочих целях, необходимо также внедрение полнофункциональных решений для управления мобильными устройствами и их защиты.

ЗАКЛЮЧЕНИЕ И РЕКОМЕНДАЦИИ

Политики и обучение сотрудников

Разработка, внедрение и тщательный контроль применения политик IT-безопасности позволяет значительно повысить уровень защищенности IT-инфраструктуры компании. Следует также помнить, что прямыми или косвенными виновниками утечки ценных корпоративных данных часто становятся сотрудники организаций, причем в большинстве случаев это происходит непредумышленно. Поэтому крайне важно уделять внимание информированию персонала о современных киберугрозах и способах противодействия им.

Комплексный подход

В связи с огромным разнообразием киберугроз практически невозможно найти единственное решение, которое бы раз и навсегда избавило компании от всех проблем, связанных с информационной безопасностью. Внедрение современного эффективного решения для защиты корпоративной IT-инфраструктуры и управления ею позволяет радикально повысить уровень безопасности компании. Однако чтобы оградить компанию от всех IT-угроз, в том числе новейших, необходимо также следить за актуальными тенденциями развития киберугроз и средств защиты от них, грамотно выбирать и внедрять необходимое аппаратное и программное обеспечение, поддерживать высокий уровень осведомленности сотрудников, включая тех, чья деятельность напрямую не связана с IT. Только комплексное применение этих мер позволяет обеспечить по-настоящему надежную защиту компании.

www.kaspersky.ru/business

KASPERSKY lab