Создано при поддержке «Лаборатории Касперского»

IT-безопасность

для "чайников"™

Подготовлено

KASPERSKY lab

Джорджина Гилмор
Питер Бирдмор

О «Лаборатории Касперского»

«Лаборатория Касперского» — одна из наиболее динамично развивающихся компаний в сфере информационной безопасности. Компания входит в четверку ведущих производителей решений для защиты конечных устройств*. «Лаборатория Касперского» существует более 15 лет и все это время остается инноватором в отрасли IT-безопасности, разрабатывая эффективные защитные решения для крупных, малых и средних компаний, а также домашних пользователей. Сейчас «Лаборатория Касперского» осуществляет свою деятельность более чем в 200 странах, защищая свыше 300 миллионов пользователей по всему миру.

Подробнее см. на www.kaspersky.ru/business

* Компания заняла четвертое место в рейтинге аналитического агентства IDC «Выручка вендоров от продажи решений класса Endpoint Security» (Worldwide Endpoint Security Revenue by Vendor) за 2011 г. Рейтинг был включен в отчет IDC «Прогноз развития мирового рынка решений класса Endpoint Security на 2012-2016 гг. и доли вендоров в 2011 г.» (Worldwide Endpoint Security 2012-2016 Forecast and 2011 Vendor Shares), опубликованный в июле 2012 года (IDC #235930). В основу рейтинга легли данные о выручке от продажи решений класса Endpoint Security в 2011 г.

IT-безопасность

для

"Чайников"™

Издано «Лабораторией Касперского», ограниченный тираж

IT-безопасность

для

"Чайников"™

Издано «Лабораторией Касперского», ограниченный тираж

Джорджина Гилмор

и Питер Бирдмор

WILEY

IT-безопасность для «ЧАЙНИКОВ»®– издание, выпущенное компанией «Лаборатория Касперского» ограниченным тиражом

Опубликовано издательством:
John Wiley & Sons, Ltd
The Atrium, Southern Gate, Chichester,
West Sussex, PO19 8SQ, England (Англия)

Чтобы узнать, как создать собственную книгу категории *для «ЧАЙНИКОВ»* для своей компании или организации, свяжитесь с компанией Wiley по электронной почте: `CorporateDevelopment@wiley.com`. Чтобы узнать о лицензии на использование торговой марки *для «ЧАЙНИКОВ»*, обращайтесь по адресу: `BrandedRights&Licenses@Wiley.com`.

Посетите нашу домашнюю страницу: `www.customdummies.com`

Издательство Wiley также публикует свои книги в различных электронных форматах. Отдельные фрагменты данной печатной версии могут отсутствовать в электронных версиях.

ISBN 978-1-118-84041-2 (печатная версия); ISBN 978-1-118-84822-7 (электронная книга)

Напечатано и переплетено печатным домом Page Bros в г. Норидж, Великобритания

Введение

Вас приветствует книга *IT-безопасность для «ЧАЙНИКОВ»*. В ней рассказывается о некоторых проблемах информационной безопасности, с которыми сталкиваются компании любого масштаба в нашем объединенном Интернетом мире. Советы и рекомендации, которые вы найдете в этой книге, помогут вашей компании защитить конфиденциальную информацию и таким образом избежать нормативных и правовых санкций или ущерба вашей деловой репутации.

В последнее десятилетие колоссальный скачок в развитии компьютерных технологий помог компаниям сократить расходы, повысить эффективность и качество обслуживания клиентов. Однако эти же технологии открыли хакерам новые пути для атак. Сейчас как никогда раньше всем компаниям (даже считающим, что они не владеют конфиденциальной информацией, которую нужно защищать) важно знать об угрозах IT-безопасности и способах защиты от них. С этой целью и написана данная книга.

Об этой книге

Несмотря на маленький размер, книга содержит массу полезных сведений, которые помогут развивающимся компаниям выбрать оптимальные пути защиты конфиденциальной информации, в том числе данных клиентов, а также уберечь свои компьютеры и мобильные устройства от вирусов, вредоносных атак и других угроз.

От небольших предприятий до крупных корпораций — все без исключения организации могут стать мишенью хакеров, которые владеют изощренными методами получения доступа к конфиденциальной информации и кражи денег с банковских счетов. В этой ситуации крупные международные компании могут позволить себе нанять команду экспертов по информационной безопасности, в то время как в штате небольших фирм таких специалистов обычно нет. Книга *IT-безопасность для «ЧАЙНИКОВ»* предназначена помочь компаниям, уделив внимание следующим вопросам:

- почему практически все компании владеют персональными данными, которые необходимо защищать;
- спектр и характер актуальных рисков информационной безопасности;
- простые способы защитить конфиденциальную информацию без лишних затрат;
- удобные в использовании продукты, способные существенно повысить информационную безопасность компании.

Смелые предположения

Мы надеемся, что в этой книге вы найдете ценную для себя информацию, поэтому сделали несколько предположений:

- компания, которой вы владеете, руководите или в которой работаете, использует ноутбуки, настольные компьютеры или мобильные устройства;
- вы хотите быть уверены в том, что компания соблюдает законы об информационной безопасности;
- вам важно обеспечить конфиденциальность бизнес-данных;

- вас интересует, как избежать хакерских атак, способных нарушить нормальную работу компании;
- вы рассматриваете возможность хранения определенных бизнес-данных в «облаке»;
- вы не против получить несколько советов по выбору программного обеспечения для защиты информационных систем компании.

Как организована эта книга

Книга *IT-безопасность для «ЧАЙНИКОВ»* разделена на шесть небольших, но при этом информационно насыщенных глав.

- **Глава 1. Почему любой компании необходимо защищать конфиденциальную информацию.** Мы объясняем, чем опасно ложное чувство безопасности.
- **Глава 2. Что нужно именно вашей компании?** Безопасность необходима всем компаниям, но требования к ней бывают разными.
- **Глава 3. Вся правда об угрозах безопасности.** Узнайте, почему современные IT-системы стали сложнее, а угрозы для бизнеса — опаснее.
- **Глава 4. Планирование повышения уровня информационной безопасности.** Оцените имеющиеся риски, а затем разработайте стратегию защиты от них. Мы также расскажем, на что следует обратить внимание при хранении информации в «облаке».
- **Глава 5. Выбор подходящего защитного решения.** Мы поговорим о факторах, которые помогут выбрать правильный продукт среди множества представленных на современном рынке.
- **Глава 6. Десять вопросов, которые вам помогут.** Используйте эти вопросы в качестве шпаргалки.

Используемые обозначения

Чтобы упростить поиск нужной информации, рядом с важными сведениями используются специальные обозначения.

Знак мишени означает, что нужно обратить внимание на важный совет.

Значок с узелком означает, что нужно запомнить важную информацию.

Обратите внимание на потенциальные трудности!

Какую главу читать дальше

Эта книга читается быстро и легко. Вы можете изучить главы в произвольном порядке или методично прочитать весь текст от начала до конца. Какой бы способ вы ни выбрали, мы уверены, что вы найдете здесь много ценных советов по защите информации своих клиентов и других важных данных, которые хранит и обрабатывает ваша компания.

Глава 1

Почему любой компании необходимо защищать конфиденциальную информацию

В этой главе

- Оценка дополнительных рисков для небольших компаний
- Защита ценной бизнес-информации
- Как избежать угроз, вызванных ложным чувством безопасности
- Почему компания любого размера может стать жертвой киберпреступников

В первой главе мы рассмотрим несколько рисков информационной безопасности для компаний и объясним, почему неразумно отодвигать вопросы защиты на второй план.

Компании — в опасности

В нашу информационную эпоху знание — уже не просто сила; это большая сила. Успех вашей компании во многом зависит от информации, которую она хранит, будь то данные о ноу-хау, продуктах или клиентах. Утрата доступа к каким-либо из этих ценных данных может нарушить налаженную работу компании.

Но это еще не самое страшное. Представьте себе последствия в том случае, если эта информация попадет в руки злоумышленников! А что будет, если преступник получит доступ к компьютерам компании и украдет данные, позволяющие управлять ее счетами через Интернет? Катастрофа!

К сожалению, компания любого размера может стать мишенью киберпреступников, которые используют широкий арсенал методов для нарушения бизнес-процессов предприятий, получения доступа к конфиденциальной информации и кражи денег с корпоративных счетов. К сожалению, очень часто жертвы подобных атак узнают о проблеме, когда уже слишком поздно.

Киберпреступления и киберпреступники

Преступникам всегда удается находить бреши в защите, позволяющие нажиться за чужой счет. Ненадежная защелка на окне офиса или сигнализация, которую легко отключить, — злоумышленники не упустят шанс воспользоваться любым недочетом. В век повсеместного использования Интернета нам угрожает новая категория злоумышленников — киберпреступники.

Киберпреступлениями называется широкий спектр противозаконных действий, выполняемых через информационные системы и Интернет. Многие компании легко забывают об угрозах такого рода, а злоумышленникам это только на руку.

Киберпреступники работают очень целеустремленно и обладают высокой квалификацией в области разработки сложных методов атак на компьютеры, получения доступа к конфиденциальной информации и кражи денег. Финансовый ущерб от этих действий может быть огромным, а стоимость реализации атаки — очень низкой. Это обеспечивает такую окупаемость, о которой другие преступники могут только мечтать! Поэтому количество киберпреступлений продолжает расти.

Меньше компания — больше риски

В своей повседневной работе маленькие предприятия сталкиваются с теми же рисками, что и крупные компании, а также с целым рядом других проблем. Все компании вынуждены непрерывно приспосабливаться к постоянно меняющимся условиям рынка, реагировать на действия конкурентов и на шаг опережать требования и предпочтения клиентов. Но помимо всех этих факторов, малому бизнесу приходится решать дополнительные задачи, возникающие по мере развития и роста компаний, например:

- регулярно нанимать и обучать новых сотрудников для удовлетворения растущего спроса;
- искать помещения большей площади и организовывать переезд без прерывания ежедневной работы компании;
- привлекать дополнительное финансирование для развития бизнеса;
- открывать новые офисы;
- находить время на выстраивание бизнесс-процессов, которые уже налажены в больших компаниях, например защиты информации клиентов.

Все эти шаги необходимы для эффективного управления предприятием и его подготовки к дальнейшему развитию.

Это не моя забота!

Учредителям и сотрудникам развивающихся компаний приходится решать множество самых разных задач. На маленьком предприятии одному сотруднику или нескольким исполненным энтузиазма единомышленникам приходится быть мастерами на все руки, зачастую выполняя

намного более широкий круг обязанностей, чем на предыдущих местах работы. В таких компаниях обычно нет отдела кадров и специального юридического или IT-персонала, на квалификацию которого можно положиться.

Если вы хотите, чтобы бизнес преуспевал, нельзя распылять свое внимание на решение множества различных вопросов. Вам и вашим коллегам необходимо сконцентрироваться на ведении бизнеса и овладеть всеми тонкостями этого процесса.

Да, можно нанимать квалифицированных специалистов на почасовой основе, однако это дорогое удовольствие. Каждый рубль, доллар, евро или фунт, потраченный не на целевую деятельность организации, сокращает инвестиции в другие важные области и может даже замедлить развитие бизнеса.

Что такого особенного в IT?

Большинство компаний просто не могут функционировать без использования хотя бы базовых элементов IT, например ноутбуков. Даже если IT — всего лишь средство для достижения поставленной цели, это ключевое звено, позволяющее существенно повысить эффективность бизнеса и улучшить взаимодействие с клиентами, сотрудниками и поставщиками. Однако IT-системы должны служить бизнесу, а значит, быть простыми в настройке и управлении. Аналогично, программное обеспечение, защищающее компьютеры и конфиденциальную информацию компании, должно быть простым и удобным в использовании.

Действуют законы джунглей... позаботьтесь о защите!

Компании, считающие компьютеры неизбежным злом, обычно таким же образом относятся к защите информации,

которая на них хранится. Подобный подход вполне понятен, если IT — не ваша сильная сторона.

Однако факты говорят о том, что безопасность деловой информации сейчас важна, как никогда раньше. Причем это касается компаний любого размера. Принимая во внимание, насколько высок сейчас уровень угроз и как часто злоумышленники используют Интернет для взлома корпоративных компьютеров, ни одна компания просто не может себе позволить игнорировать вопросы безопасности. Иногда всего нескольких простых защитных мер достаточно, чтобы сохранить вам нервы и немалую сумму денег.

Вы можете считать необходимость обеспечить безопасность IT-систем и данных неизбежным злом... Но только помните, что ключевое слово здесь — «неизбежное»! А «зло» — лишь напоминание о киберпреступниках, организующих атаки на ни в чем не повинные компании.

Ни один владелец супермаркета не оставит кассу открытой настежь, чтобы любой негодяй мог ее опустошить. Точно так же каждая компания, использующая компьютеры, мобильные устройства или Интернет, должна позаботиться о том, чтобы ее IT-система не была уязвимой для атак. В наше время стать жертвой киберпреступников, использующих скрытые бреши в системе безопасности компьютеров, планшетов и смартфонов, очень легко. Поэтому вам следует принять все возможные меры, чтобы предотвратить кражу своих конфиденциальных данных или денег с банковских счетов.

Большая польза от маленькой защиты

Между полным отсутствием защиты и несколькими простыми мерами безопасности — огромная разница. Иногда достаточно пары базовых защитных мер, чтобы среднестатистический киберпреступник передумал атаковать вашу компанию и выбрал другую мишень.

На графике видно, как самое скромное вложение средств в безопасность может радикально снизить вероятность успешной вредоносной атаки.

Безопасность не должна тормозить бизнес

Время — деньги! И этим все сказано. Конечно, это избитая фраза, но ведь это правда. Лишние заботы, которые отвлекают вас от дел, приносящих доход, отбирают у вас время, возможности и деньги. Быстрая реакция и полная концентрация на решении актуальных бизнес-задач — это главные качества, благодаря которым вы основали компанию. Поэтому, несмотря на всю важность IT-безопасности, нельзя позволить ей мешать достижению поставленных вами бизнес-целей.

Все, что отнимает ваше время, вынуждает вас меньше заниматься ключевой деятельностью, тем самым препятствуя наращиванию конкурентных преимуществ и развитию бизнеса. Неправильно выбранный подход к информационной безопасности и неподходящие технологии защиты могут мешать развитию вашей компании, хотя изначально они предназначались для ее защиты.

Легкая добыча для киберпреступников

Учитывая опасения относительно сложности и снижения производительности, неудивительно, что многие небольшие компании предпочитают закрывать глаза на IT-безопасность. Однако если еще несколько лет назад для стартапов и маленьких предприятий такой подход был приемлем, то при нынешнем уровне киберпреступлений это весьма сомнительная стратегия. А если при этом учесть, что небольшая компания — более легкая жертва по сравнению с крупной организацией, становится очевидно: IT-безопасность вашего бизнеса больше нельзя пускать на самотек.

Но есть и хорошие новости: существует много простых средств, способных помочь вашей компании защитить конфиденциальную информацию. Более того, на современном рынке есть несколько программных продуктов, специально разработанных для защиты систем и данных небольших компаний, ограниченных во времени и средствах. Эти решения позволяют обеспечить IT-безопасность бизнеса, не тратя много времени на установку и освоение сложного программного обеспечения, которым к тому же трудно управлять.

Даже крупные организации могут не обладать достаточными ресурсами для полного восстановления после атаки с использованием губительных брешей в системе защиты. А маленьким компаниям может и вовсе не хватить сил, чтобы продолжить свою деятельность после подобного инцидента.

Ложное чувство безопасности?

Некоторые компании теряют бдительность, ошибочно полагая, что киберпреступники охотятся только за крупной добычей. «Нам не о чем беспокоиться, — уверен владелец предприятия. — Кому нужно атаковать нашу маленькую компанию, когда есть цели покрупнее и побогаче? На радарах киберпреступников нас попросту нет».

Ну, радарами киберпреступники не пользуются. Зато они пользуются всевозможными сканирующими средствами другого рода: «интеллектуальные» инструменты, которые работают через Интернет, позволяют им находить компании, компьютеры которых не защищены должным образом.

Сканеры практически мгновенно находят следующую жертву и определяют ее уязвимые места.

Похоже на сюжет фантастического фильма, однако это правда. Каждый день этот и другие сложные методы используются для атак на мелкие компании. За один день «Лаборатория Касперского» в среднем идентифицирует около 12 000 атак с использованием вредоносных программ. И это число продолжает расти.

Мелкие компании — более легкая добыча для преступников

Обычно киберпреступники стремятся получить максимальный доход от своих незаконных действий, вложив минимум времени и усилий. Хотя взлом системы безопасности международной корпорации может принести огромную прибыль, проникнуть через сложные защитные барьеры, которыми обычно оснащены такие организации, очень и очень непросто.

Поэтому зачастую злоумышленники предпочитают организовать нападение на множество небольших компаний. Конечно, выручка от каждой отдельной атаки будет значительно меньше, но если такие компании недостаточно или вовсе не защищены, эти деньги могут достаться киберпреступникам почти без усилий. Атаки на десять-двадцать мелких предприятий могут в сумме принести такой же доход, как одно нападение на крупную компанию, и потребовать гораздо меньших затрат.

Поскольку многие мелкие компании не могут выделить время на внедрение системы защиты, некоторые киберпреступники целенаправленно выбирают для атак небольшие предприятия в надежде на легкую добычу. Не допустите, чтобы в их числе оказалась ваша компания.

Киберпреступники используют мелкие компании как трамплин

Киберпреступники знают, что небольшие предприятия часто являются поставщиками для крупных компаний. Это еще одна причина их атаковать. В результате нападения на такое предприятие киберпреступник может завладеть информацией, которая может помочь ему организовать следующую атаку – уже на крупную корпорацию.

Злоумышленники могут преднамеренно выбирать компании из-за их связи с более крупными корпорациями. С другой стороны, киберпреступник может просто воспользоваться подвернувшимся шансом украсть у небольшой компании информацию о ее клиентах.

Разумеется, если впоследствии будет совершена атака на крупную организацию, и станет известно, какую роль сыграла в ней небольшая компания, последнюю ожидают большие неприятности.

Даже если маленькая компания не сделала ничего противозаконного, отсутствие надлежащих защитных мер привело к взлому ее систем и помогло организовать атаку на ее крупного клиента. Если о роли маленькой компании в этом преступлении станет известно, ее могут ожидать такие последствия, как судебный процесс, выплата компенсаций, штрафы, потеря клиентов и деловой репутации.

Двойная неудача

Представим себе небольшое предприятие, которое покупает сырье у крупной корпорации, а затем продает готовые изделия международной компании. В целях повышения эффективности поставщик сырья использует онлайн-системы для обработки заказов и взаимодействия с клиентами, в число которых входит и это небольшое предприятие. Международная компания также требует, чтобы это предприятие отправляло электронные счета непосредственно в ее внутренние бухгалтерские системы.

Это означает, что предприятие напрямую подключается к компьютерным системам корпорации-поставщика и международной компании-клиента.

Если киберпреступник взломает компьютеры этого предприятия, он сможет завладеть информацией, которая позволит атаковать как поставщика, так и его клиента. Даже если эти атаки не будут успешными, нашему небольшому предприятию придется ответить на много неприятных вопросов... Возможно, ему даже будет запрещено пользоваться электронными системами своих поставщиков и клиентов. Это может негативно сказаться на эффективности работы и рентабельности небольшого предприятия, особенно если его конкуренты будут иметь преимущество более тесного взаимодействия с поставщиками и клиентами.

Глава 2

Что нужно именно вашей компании?

В этой главе

- Знание своих правовых и нормативных обязательств
- Оценка ожиданий в своей отрасли
- Почему сейчас угрозы опаснее, чем когда-либо раньше
- Различия в требованиях к безопасности

В этой главе мы рассмотрим, где совпадают и в чем различаются требования к безопасности для различных компаний.

Некоторые требования к безопасности одинаковы для компаний любого размера

Многие компании ошибочно полагают, что не владеют информацией, которая может представлять интерес для киберпреступников. Кроме того, владелец бизнеса может считать, что потеря информации не нанесет его компании значительного урона. К сожалению, зачастую это далеко не

так, причем не важно, о какой компании идет речь – о небольшом предприятии или более крупной организации.

Даже простая база данных с контактной информацией клиентов может представлять ценность — как для киберпреступников, которые могут использовать эти данные для «кражи личности», так и для конкурентов, мечтающих переманить ваших клиентов.

Правовые обязательства по защите информации

Во многих странах в отношении компаний действуют строгие требования к работе с персональными данными. Невыполнение этих требований может наказываться крупными штрафами, в некоторых случаях могут быть предъявлены иски директорам или владельцам компаний, а определенные нарушения могут даже привести к тюремному заключению.

В некоторых странах к крупным организациям применяются более строгие законодательные и нормативные требования относительно обработки и хранения личных данных. Но даже если местные власти требуют от крупных корпораций внедрять более сложные меры безопасности, небольшие компании также обязаны действовать ответственно и осуществлять определенные действия для защиты важной информации.

Компании, которые игнорируют меры безопасности, обязательные для данного типа бизнеса и размера компании, могут навлечь на себя большие неприятности.

Более строгие требования к безопасности

Многие юрисдикции обязывают все компании проявлять большую осторожность при работе с особо

конфиденциальными материалами или другой информацией, утечка которой может причинить третьей стороне существенный вред.

И наконец, для некоторых отраслей и секторов рынка могут действовать еще более строгие требования по защите информации. Например, обычно компании, работающие в юридической и медицинской сферах, обязаны проявлять особую осторожность в отношении информации, которую они используют, хранят и обрабатывают.

Но даже если повышенные требования не касаются вашей компании, утечка конфиденциальной информации может иметь для нее печальные последствия.

Под угрозой даже кошка

Разве существует более далекое от информационных технологий предприятие, чем гостиница для кошек и собак? Нужно ли задумываться об информационной безопасности в таком деле? Конечно! Подумайте о том, сколько адресов и имен клиентов хранится на компьютерах в такой организации, плюс электронное расписание с датами пребывания хвостатых гостей.

А если эта информация попадет в руки злоумышленников? Очевидно, что если Барсика или Рекса оставили в гостинице, значит за питомцем некому присматривать – а для грабителей эти сведения очень полезны. Зная, когда хозяев не будет дома, воры смогут без помех вынести все ценные вещи.

Разные уровни понимания и ресурсов

Несмотря на схожесть некоторых стандартов по защите информации, применимых ко всем компаниям, существуют четкие различия в том, как компании разных размеров должны рассматривать и решать вопросы безопасности.

Настали другие времена

Изощренный и неумолимый характер современных атак на информационные системы означает, что нынешние угрозы стали на несколько порядков опаснее, чем они были еще несколько лет назад. Компании, которые этого не осознают, подвергают себя большому риску.

Чтобы защитить информационные системы, крупные компании могут позволить себе держать в штате специалистов по IT-безопасности. Однако для небольших предприятий это слишком большая роскошь.

Размер имеет значение?

Очевидно, что объем доступных ресурсов — один из факторов, отличающих мелкие предприятия от крупных корпораций. Большие компании могут нанять штатных экспертов, которые будут принимать квалифицированные решения о том, в какие защитные технологии стоит инвестировать деньги. Они также обладают необходимыми финансовыми средствами и ресурсами поддержки, чтобы внедрить выбранное решение. Кроме того, их штатные команды специалистов обладают опытом разработки и постоянного усовершенствования планов и политик безопасности, позволяя компании всегда на шаг опережать киберпреступников и не оставлять брешей в своей системе защиты.

Мелкие компании в этом отношении могут быть полностью безоружны. Кроме того, в растущей компании всегда есть сразу несколько направлений, в развитие которых можно вложить лишние деньги (хотя «лишние деньги» — это явление, с которым мы никогда еще не сталкивались на практике). Поэтому компьютерная безопасность должна занять свое место в очереди и полностью оправдывать каждый потраченный на нее рубль.

Различия требований к безопасности

Имея много общего, требования к информационной защите разных типов компаний часто все же различаются... как могут различаться и точки зрения относительно необходимого уровня безопасности. Кроме того, по мере развития компании ее потребности в области информационной безопасности также могут меняться.

Знакомы ли вам следующие типы компаний и их взгляды на IT-безопасность?

Стартап

В возрасте 36 лет начинающий предприниматель Сергей решает покинуть большую компанию с офисом в центре города и вместе с двумя коллегами-юристами создает новую фирму.

Как используются IT в компании:

- Сергей и его коллеги не могут обойтись без ноутбуков, планшетов и смартфонов, которые позволяют им работать практически где угодно;
- новоиспеченные владельцы компании планируют интенсивно использовать электронную почту для

общения с клиентами и компьютеры — для написания писем, предложений и заметок.

Отношение компании к безопасности:

- компания будет работать с высококонфиденциальной информацией, в том числе финансовой, обеспечить защиту которой чрезвычайно важно;
- любая утечка или потеря информации создаст много проблем и может нанести значительный урон репутации Сергея и его фирмы. На Сергея даже может быть заведено судебное дело;
- информационная защита компании имеет исключительную важность, и Сергей понимает, что стандартного антивирусного программного обеспечения будет недостаточно.

Сергей говорит: «Нам нужно купить, установить и настроить новое антивирусное решение. В то же время нам необходимо как можно быстрее начать получать доход, поэтому выбранное ПО должно не только обеспечивать необходимый уровень защиты, но и быть простым в настройке, управлении и обслуживании. Кроме того, поставщик ПО должен предоставлять поддержку когда и где это будет необходимо, позволив нам сконцентрироваться на обслуживании клиентов. И наконец, защитное решение должно легко адаптироваться к новым требованиям, возникающим по мере развития нашего бизнеса».

Развивающийся бизнес

Амбициозный Руслан многого достиг для своих 48 лет. Он владеет сетью ателье по пошиву мужской одежды, в которой работают восемнадцать человек. И его бизнес продолжает расширяться.

Как используются IT в компании:

- компания открывает новый магазин и параллельно с этим запускает веб-сайт для продажи костюмов через Интернет;
- в связи с расширением компании необходимо приобрести много нового оборудования, в том числе дополнительные кассовые терминалы (PoS), компьютеры, сетевые маршрутизаторы Wi-Fi и новый сервер;
- хотя Руслан не очень много внимания уделяет новинкам в сфере IT, он использует свой новый смартфон для работы с электронной почтой.

Отношение компании к безопасности:

- компания использует антивирусный продукт, который приобрел для Руслана его «разбирающийся в технологиях племянник» в большом компьютерном магазине. Однако Руслан понимает, что этого продукта недостаточно для надежной защиты бизнес-информации, особенно учитывая стремительное расширение деятельности компании. Руслан не может допустить, чтобы его ближайший конкурент завладел списком постоянных клиентов и моделью расчета цен компании;
- Руслан обязан соблюдать стандартные требования к защите данных при работе с платежными картами, в связи с чем ему необходимо установить защитное ПО и поддерживать его базы в актуальном состоянии для обеспечения IT-безопасности.

Он говорит: «Дело моей жизни — пошив одежды, а не информационные технологии. Однако сейчас нужно приобрести более профессиональное решение для обеспечения IT-безопасности, чтобы потом уже со спокойной душой посвятить себя любимому занятию. Нам необходим продукт,

который обеспечит достаточную защиту, но при этом будет простым в установке и управлении. Мне нужно ПО, которое будет делать свое дело, а мне позволит заниматься моим. С тех пор как я взял на себя управление бизнесом моего отца, мы заметно расширились. Сейчас мы открываем пятый магазин и запускаем продажи через вебсайт, поэтому нам нужно защитное решение, которое будет развиваться вместе с нами».

Организация, меняющая подход к безопасности

Раздраженная Элеонора — 40-летний врач, возглавляющая медицинский кабинет, в котором заняты еще два врача, один физиотерапевт и три регистратора/администратора, работающих неполный рабочий день.

Как используются IT в компании:

- у каждого врача есть свой настольный компьютер, и еще один компьютер стоит в комнате физиотерапевта. Еще два компьютера находятся на стойке регистратуры и один — в кабинете администратора.
- Интернет и компьютеры изменили способ работы этой медицинской компании, значительно упростив ведение записей о пациентах, получение сведений о новых препаратах и процедурах и другой информации.

Отношение компании к безопасности:

- учитывая зависимость своей компании от IT и высокую конфиденциальность информации, с которой она имеет дело, Элеонора полностью осознает важность программного обеспечения для защиты IT;
- при этом используемое в настоящее время ПО раздражает всех сотрудников. Компьютеры загружаются невыносимо долго, а когда выполняется проверка на наличие вредоносных программ, и вовсе «виснут».

Элеонора говорит: «Конфиденциальность сведений о пациентах — это самое важное. Поэтому мы никогда не сомневались в необходимости защитного ПО. Однако текущее решение ощутимо ухудшает производительность наших компьютеров.

Теперь, когда лицензия на исходе, самое время перейти на другой защитный продукт, который не будет снижать производительность компьютеров и позволит эффективнее работать с пациентами. Нам просто нужно средство, которое защитит высококонфиденциальную информацию, не мешая максимально качественно обслуживать пациентов».

Компания, которая уже обожглась

Обеспокоенной Светлане 32 года, она владеет успешным маркетинговым агентством, в котором работают 22 человека. Светлане удалось быстро развить бизнес. Благодаря своим способностям в сфере продаж и маркетинга она легко завоевывает новых клиентов.

Как используются IT в компании:

- основной штат работает в офисе, однако многие сотрудники выезжают к клиентам;
- команда дизайнеров использует компьютеры Apple, а остальной персонал — комбинацию настольного компьютера или ноутбука и смартфона;
- многие сотрудники также пользуются планшетами. Так как планшеты принадлежат сотрудникам, они не являются официальными корпоративными устройствами. Светлана очень рада, что персонал использует собственные устройства. Она считает, что благодаря следованию этой модной тенденции ее агентство выглядит очень современно.

Отношение компании к безопасности:

- к сожалению, недавно агентство пережило серьезный инцидент безопасности. После встречи с клиентом один из директоров по работе с клиентами взял свой ноутбук в бар, где устройство было украдено. На ноутбуке хранился ряд высококонфиденциальных файлов, включая планы по запуску новых продуктов, способных обеспечить клиенту существенное преимущество на рынке;
- Светлане пришлось рассказать о случившемся клиенту, которого эта новость привела в ярость. Инцидентом занялся юридический отдел клиента. Сейчас клиент собирается разорвать отношения с агентством, в связи с чем оно потеряет значительную часть своего бизнеса. Кроме того, агентство также может столкнуться с правовыми последствиями.

Светлана говорит: «Цена этой ошибки для нас с каждым днем продолжает расти. Теперь моя главная задача — полностью исключить возможность повторения подобной ситуации. Нам нужно как можно быстрее внедрить комплексное решение для защиты данных. Однако оно также должно быть простым в управлении, чтобы я могла поручить его настройку и обслуживание одному из наших дизайнеров, который прекрасно разбирается в технических вопросах».

Самонадеянная компания

Беспечному Роману 53 года, и он владеет бухгалтерской фирмой, в которой работают пять человек. Это уже сложившаяся компания, которая никогда не принимала угрозы безопасности всерьез. Роман всегда придерживался позиции «со мной не может произойти ничего плохого».

Как используются IT в компании:

- Роман и два других консультанта по бухгалтерским вопросам много времени проводят с клиентами. Благодаря ноутбукам они не привязаны к офису;

- два администратора компании используют настольные компьютеры;
- компания также использует файловый сервер, на котором установлена CRM-система.

Отношение компании к безопасности:

- недавно в одном экономическом журнале Роман прочитал статью о том, что конкурирующая фирма серьезно пострадала из-за бреши в системе информационной безопасности. Администратор загрузил вложенный в электронное письмо файл с вредоносной программой, которая таким образом получила доступ к конфиденциальным файлам клиентов. Взлом был обнаружен только когда один из клиентов узнал, что его конфиденциальные данные продаются в Интернете;
- после прочтения статьи Роман заволновался об IT-безопасности собственной фирмы. Теперь он понимает, что используемое фирмой бесплатное защитное решение, вероятно, не обеспечивает должный уровень безопасности.

Роман говорит: «За последние годы сфера, в которой мы работаем, очень изменилась. Сейчас действует намного больше законодательных требований. Кроме того, характер подстерегающих угроз вынуждает внедрить намного более надежную IT-защиту».

Разные решения для разных нужд

Хотя рассмотренные в этой главе компании работают на разных рынках и по-разному используют IT, всех их объединяет одно — необходимость защитить ценную информацию. Однако в связи с тем, что компании используют различные устройства и обладают разной квалификацией в сфере IT, их потребности в защите также различаются.

Конечно, эти компании — обобщенные примеры того, как разные типы предприятий относятся к защите IT и какие требования к ней они предъявляют. Количество разных бизнес-моделей и размеров компаний практически бесконечно, и настолько же разнятся их требования к IT.

Небольшая компания, состоящая из трех-пяти человек, вполне может управлять крупномасштабными процессами, требующими интенсивного использования компьютеров. Такая компания, скорее всего, будет обладать намного более широкой и разноплановой IT-инфраструктурой, чем другие компании того же размера. Поэтому ей понадобится защитное решение, учитывающее все сложности ее IT-среды, включая наличие в последней интернет-шлюзов, прокси-серверов и виртуальных систем.

Глава 3

Вся правда об угрозах безопасности

В этой главе

- Как сложность IT добавляет новые проблемы
- Почему одной антивирусной защиты уже недостаточно
- Знакомство с интернет-угрозами
- Защита транзакций интернет-банкинга

В этой главе мы рассмотрим, как растущая сложность типичных программных решений для бизнеса и изощренность компьютерных вирусов, вредоносных программ и кибератак усложняют жизнь всем компаниям.

Все стало намного сложнее

Еще несколько лет назад все устройства, которые нуждались в защите, были всегда «в зоне видимости» руководителя компании. Так же просто было нарисовать воображаемое кольцо вокруг компьютерной сети. Раньше можно было просто установить надлежащее программное обеспечение на всех компьютерах — и вот вы в безопасности.

Так было во времена ограниченной мобильности и невозможности доступа к бизнес-информации вне стен офиса. И это было задолго до того, как бизнес стал настолько зависим от IT.

Компании не могут обойтись без IT

Вы готовы попробовать управлять своей компанией без использования бизнес-приложений и вездесущего мобильного доступа к важной бизнес-информации? Конечно же, нет — вы же не хотите, чтобы ваши конкуренты хохотали всю дорогу по пути в банк.

Однако эти технологические достижения влекут за собой определенные последствия. Такая удобная возможность удаленного доступа к корпоративным ресурсам значительно повышает сложность IT. Если вы и ваши сотрудники собираетесь получать доступ к информации с помощью ноутбуков, смартфонов и планшетов, то где будут проходить границы того воображаемого кольца, внутри которого применяются защитные меры?

BYOD добавляет еще один уровень сложности

Все еще больше усложняется при использовании подхода BYOD (Bring Your Own Device — использование собственных устройств сотрудников для работы), когда сотрудникам разрешается получать доступ к информации и системам компании с помощью личных устройств. В таком случае система безопасности должна работать в условиях возможности доступа с любого устройства и из любой точки земного шара.

Компании быстро осознали потенциальные преимущества BYOD с точки зрения экономии средств и повышения производительности. Однако BYOD также означает необходимость обеспечить безопасность широчайшего

спектра мобильных устройств, включая различные модели Android, iPhone, BlackBerry, Symbian, Windows Mobile и Windows Phone, которые могут не принадлежать компании.

К счастью, некоторые поставщики продуктов по обеспечению безопасности быстро поняли, сколько головной боли добавляет повышение сложности IT владельцам небольших предприятий. Поэтому они заботливо создали инновационные решения, которые значительно упрощают защиту различных устройств, включая мобильные, в условиях набирающей популярность концепции BYOD.

Подробнее проблемы мобильной безопасности и доступные решения описаны в книге *Безопасность мобильных устройтств для «ЧАЙНИКОВ»*, которую вы можете найти на странице: `www.kaspersky.ru/business`.

Вирусы или вредоносное ПО?

Некоторые компании ошибочно считают, что вирусы и вредоносное ПО — это одно и то же, поэтому для борьбы с ними подходят одни и те же продукты. Но это не так, и подобная ошибка может дорого стоить.

Большинство людей знакомо с компьютерными вирусами, которые распространяются между компьютерами. Однако понятие «вредоносное ПО» охватывает намного более широкую группу опасных программ. В нее, помимо компьютерных вирусов, входят черви, троянцы, клавиатурные шпионы, шпионское ПО и программы-вымогатели, а также многие другие угрозы.

Поэтому программный продукт для защиты от вредоносного ПО оберегает информацию и компьютеры от широкого диапазона угроз, а не просто от вирусов.

Опасность современных угроз неуклонно растет

Практически все пользователи в той или иной степени знают, что такое компьютерный вирус. Трудно найти человека, который никогда не заражался вирусом (мы имеем в виду компьютеры, ничего личного) или хотя бы не знаком с кем-то, кто сталкивался с такой проблемой. Однако многие из этих страшных историй, которые пересказываются в кругу друзей и семьи, могут относиться к периоду расцвета киберхулиганства, когда вредоносные программы создавались для развлечения. В наши дни цель вредоносного ПО — получение финансовой прибыли.

Время безобидных шуток прошло

Как правило, киберхулиганством раньше занимались студенты и школьники, чтобы похвастаться своими компьютерными и хакерскими способностями. Они создавали и распространяли вирусы, которые так или иначе нарушали работу зараженных компьютеров. Например, вирусы могли удалить несколько файлов или «подвесить» компьютер. Хотя такие программы и могли причинить определенные неудобства, в основном они носили характер безобидной шутки.

Эти вирусы редко создавали серьезные проблемы для компаний и не пытались воровать деньги с банковских счетов людей или организаций. Кроме того, базовое антивирусное ПО обычно прекрасно справлялось с большинством таких атак.

От хулиганства к серьезным преступлениям

В последние годы молодые компьютерные гики предпочитают проявлять свое мастерство в онлайн-играх. В то же

время, что более важно, постоянный рост объема осуществляемых через Интернет бизнес-процессов и финансовых операций существенно усилил нашу зависимость от Интернета и электронной коммерции. Это привлекло внимание преступников. Время относительно безобидного киберхулиганства прошло, и теперь Интернет грозит более серьезными опасностями.

Киберпреступники быстро сообразили, что вредоносное ПО и другие инструменты интернет-мошенничества можно использовать для более серьезных целей, чем шутки и мелкое хулиганство. Современные атаки разрабатываются для кражи информации, денег и других ценностей. Не допускайте ошибок — работают профессионалы. Киберпреступники, обладающие внушительными техническими навыками, непрерывно разрабатывают новые методы нападения на компании. В большинстве случаев это делается ради финансовой прибыли: прямой кражи денег с банковского счета компании, сбора конфиденциальных бизнес-данных, которые можно продать на черном рынке, или незаконного выполнения платежей от имени предприятия.

Кроме того, собирая персональную информацию с ноутбуков, серверов и мобильных устройств компании, киберпреступники могут совершать «кражу личности» и воровать деньги у физических лиц, так или иначе связанных с компанией.

Наша зависимость от компьютеров также упростила возможность нарушения работы бизнес-систем в знак социального или политического протеста (так называемый «хактивизм»).

Знай своего врага и его методы

Вредоносное ПО и угрозы IT-безопасности могут нанести компаниям значительный ущерб. А для небольших предприятий это может быть и вовсе разрушительно. Хотя представленный в этой главе список угроз не является исчерпывающим, он дает представление о некоторых рисках безопасности, к которым компании должны быть готовы.

Вирусы, черви и троянцы

Компьютерные вирусы и черви — это вредоносные программы, которые могут самовоспроизводиться на компьютерах, владельцы которых и не подозревают о заражении. Троянцы выполняют вредоносные действия, не разрешенные пользователем. Троянцы не способны самовоспроизводиться, но благодаря Интернету киберпреступники могут легко их распространять.

Если вредоносная программа атакует вашу сеть, она может стереть или изменить данные, заблокировать к ним доступ, прервать работу компьютеров или украсть конфиденциальную информацию.

Бэкдоры

Бэкдоры позволяют киберпреступникам удаленно управлять инфицированными компьютерами. Обычно взломанные компьютеры становятся частью вредоносной сети, называемой «бот-сетью», которая может использоваться в различных преступных целях.

Клавиатурные шпионы

Клавиатурные шпионы — это вредоносные программы, которые записывают нажатие клавиш на клавиатуре компьютера. Эти программы используются для сбора конфиденциальных данных, таких как логины и пароли,

номера банковских счетов и данные для доступа к ним, реквизиты кредитных карт и другие сведения. Клавиатурные шпионы часто работают в тандеме с бэкдорами.

Спам

Самый безобидный вариант спама — нежелательные сообщения электронной почты. Однако спам может быть очень опасен, когда используется в рамках фишинговых кампаний или содержит ссылки на зараженные веб-сайты, которые загружают вирусы, черви и троянские программы на компьютер жертвы.

Фишинг

Фишинг — это сложная форма атаки, которая состоит в том, что преступники создают поддельную версию легитимного сайта, например службы интернет-банкинга или социальной сети. Когда пользователь посещает поддельный сайт, злоумышленники с помощью методов социальной инженерии завладевают его ценной информацией.

Фишинг часто используется для «кражи личности» и воровства денег с банковских счетов и кредитных карт.

Программы-вымогатели

Троянские программы-вымогатели предназначены для вымогания денег. Обычно такая троянская программа либо шифрует данные на жестком диске компьютера жертвы, делая их недоступными, либо полностью блокирует доступ пользователя к компьютеру. После этого программа-вымогатель требует заплатить выкуп за отмену этих изменений.

Такие программы передаются через фишинговые сообщения электронной почты или при посещении веб-сайта, содержащего вредоносное ПО. Поскольку вредоносными

программами могут быть заражены самые обычные веб-сайты, взломанные киберпреступниками, пострадать от программы-вымогателя можно не только при посещении подозрительных сайтов.

DDoS-атака (отказ в обслуживании)

Применяя DDoS-атаки, киберпреступники делают компьютеры или сети предприятий недоступными для использования по назначению. Цели подобных атак могут быть разными, однако чаще всего они направлены на выведение из строя веб-сайта компании.

Большинство компаний с помощью веб-сайтов привлекают клиентов и взаимодействуют с ними, поэтому неправильная или медленная работа сайта или проблемы с доступом к нему могут нанести бизнесу значительный ущерб.

DDoS-атаки могут принимать различные формы. Например, киберпреступники могут заразить большое количество компьютеров, владельцы которых ни о чем не подозревают, а затем с их помощью направить огромный поток ненужного трафика на веб-сайт определенной компании. Такая атака перегружает серверы, на которых расположен веб-сайт жертвы, и замедляет работу сайта или полностью выводит его из строя.

От каких ошибок страдает компания?

Практически каждая программа и операционная система, используемая вашей компанией, содержит ошибки. Обычно эти ошибки в программном коде не наносят прямого вреда. Однако некоторые из них создают уязвимые места, которыми могут воспользоваться киберпреступники для незаконного получения доступа к вашим компьютерам.

Подобные уязвимости аналогичны открытым дверям офиса, с той разницей, что они позволяют злоумышленникам не просто проникнуть в приемную, но и попасть в самое сердце компании через компьютерную сеть. Сейчас такой способ атак очень распространен, поэтому необходимо устанавливать обновления и исправления безопасности для приложений (не игнорируйте эти надоедающие напоминания о необходимости обновления ПО и не откладывайте его на потом).

Некоторые решения для обеспечения безопасности содержат функции, позволяющие выявлять и закрывать уязвимости в приложениях и операционных системах, установленных в сети компании, предотвращая их использование киберпреступниками.

Другие риски безопасности

Помимо определенных типов атак, которые мы рассматривали в предыдущем разделе, вашей компании необходимо остерегаться и других опасностей.

Риски при использовании общедоступных сетей Wi-Fi

Благодаря тому, что гостиницы, аэропорты и рестораны предоставляют своим клиентам бесплатный доступ к сетям Wi-Fi, сейчас стало удобно проверять электронную почту на ходу. Однако это также позволяет киберпреступникам следить за общедоступными сетями Wi-Fi и перехватывать информацию, которую вы отправляете или получаете. А это значит, что киберпреступники могут получить прямой доступ к вашим корпоративным почтовым ящикам и компьютерной сети, а также паролям для проведения финансовых операций.

Интернет-банкинг и необходимость в дополнительной защите

Интернет-банкинг стал для многих компаний незаменимым инструментом. Он очень удобен и экономит время. Однако при выполнении финансовых интернет-операций вы подвергаетесь серьезной опасности.

Киберпреступники следят за компьютерами и мобильными устройствами жертв, чтобы определить, когда пользователь посещает веб-сайт банка или сервиса интернет-платежей. А затем специальные программы, так называемые «клавиатурные шпионы», перехватывают информацию, которую вы вводите. Это означает, что киберпреступник может незаметно украсть ваш пароль, а затем войти в вашу учетную запись и перевести средства с вашего счета на свой – а вы ничего не будете подозревать.

К счастью, некоторые защитные программные продукты включают в себя технологии, обеспечивающие дополнительные уровни защиты при выполнении вами финансовых операций в Интернете.

Целевые фишинг-атаки

Целевая фишинг-атака — это еще одна сложная форма нападения. Киберпреступники стремятся получить личную информацию пользователей, например, шпионя за общедоступными сетями Wi-Fi. Затем с ее помощью они создают на первый взгляд правдоподобное (так называемое «фишинговое») сообщение электронной почты с целью взломать систему безопасности компании.

Например, киберпреступник может прочитать запись одного из ваших сотрудников в социальной сети и узнать о том, как он провел отпуск, а затем использовать эту информацию в фишинговом сообщении. Когда сотрудник получит от имени своего коллеги сообщение, которое будет содержать сведения о его отпуске, он поверит в его подлинность. А если в сообщении сотруднику будет предложено перейти по ссылке и подтвердить доступ к корпоративной сети, киберпреступник сможет получить необходимый для доступа пароль.

Потерянные ноутбуки

Все мы слышали истории о ноутбуках, забытых в такси, поездах или ресторанах. При этом вероятность попадания конфиденциальной информации в руки преступников просто ужасает. Обычная невнимательность может нанести серьезный ущерб деловой репутации компании и привести к большим штрафам.

Отчасти решить эту проблему позволяет решение безопасности, которое шифрует бизнес-информацию. Таким образом, даже в случае потери или кражи ноутбука киберпреступники не смогут получить доступ к данным, хранящимся на жестком диске устройства.

Что такое шифрование

Шифрование — это способ защиты, позволяющий победить киберпреступника в его же игре. Вы видели, как шпионы в фильмах кодируют сообщения таким образом, что их могут прочитать только знающие код получатели? Аналогично шифрование позволяет закодировать конфиденциальную информацию компании, так что ее удастся раскодировать только с помощью специального шифра.

Это означает, что если злоумышленники завладеют какими-либо конфиденциальными данными компании, они не смогут просмотреть их в доступном для понимания формате без вашего секретного ключа.

Когда применяется шифрование данных, то в случае, если один из ваших сотрудников потеряет ноутбук или флешку с конфиденциальными сведениями, вы можете не беспокоиться об утечке конфиденциальной бизнес-информации.

Мобильные угрозы

Отдельные пользователи и целые компании могут опрометчиво полагать, что смартфон или iPhone — это всего лишь телефон. Но это не так: подобные устройства являются мощными компьютерами, способными хранить большие объемы конфиденциальных данных. Поэтому кража или потеря мобильного устройства может привести к серьезным проблемам безопасности. Если потерянный или украденный смартфон не защищен PIN-кодом (или, еще лучше, более длинным и сложным паролем), любой другой человек, взяв устройство в руки, сможет без труда войти в любую учетную запись, которая на нем использовалась.

Однако некоторые решения для обеспечения безопасности предлагают функции удаленного управления, позволяющие связаться с потерянным или украденным телефоном и стереть с него все данные.

Если выбранное вами защитное решение включает возможность шифрования данных, вы получаете дополнительный уровень защиты. Даже если преступник найдет ваш телефон раньше, чем вы узнаете о его исчезновении и сможете стереть с него информацию, шифрование позволит гарантировать, что ваши конфиденциальные данные не будут прочитаны.

Более того, поскольку современные смартфоны и планшеты — это, по сути, компьютеры, они, как и обычные ноутбуки и настольные компьютеры, подвержены постоянно растущему риску хакерских атак и заражения вредоносным ПО, а также спаму и фишингу. Поэтому необходимо защищать мобильные устройства с помощью специального программного обеспечения (чтобы узнать об этом подробнее, бесплатно скачайте книгу *Безопасность мобильных устройств для «ЧАЙНИКОВ»* на веб-сайте `www.kaspersky.ru/business`).

Глава 4

Планирование повышения уровня информационной безопасности

В этой главе

- Польза от простой оценки бизнес-рисков
- Информирование сотрудников о рисках безопасности
- Как облачные технологии могут повлиять на безопасность
- Оценка поставщиков облачных служб

Когда дело доходит до IT-безопасности, некоторые думают: «Все это слишком сложно. Скрещу пальцы и буду надеяться, что меня это не коснется». Нам остается только пожелать подобным людям удачи. Но когда клиенты и бизнес-партнеры такой компании подают на нее судебный иск в связи с утерей данных, компании нечего сказать в свою защиту. Итак, в этой главе мы рассмотрим несколько простых мер безопасности, которые не требуют затрат на программное обеспечение или оборудование, а также поговорим о том, как облачные технологии могут повлиять на стратегию безопасности компании.

Рискованный бизнес?

Многим кажется, что оценка риска — это очень сложная задача, которую лучше оставить умникам в очках и белых халатах. Но если вы все-таки хотите повысить уровень информационной безопасности, в этом разделе мы поделимся несколькими простыми идеями, которые можно взять за основу при оценке рисков для вашего бизнеса.

Для начала задайте себе несколько базовых вопросов:

- Где хранится наша бизнес-информация?
- Какова ее ценность для компании и потенциального взломщика?
  - Какими будут последствия для компании, если конфиденциальная информация попадет в руки преступников?
  - Как утечка информации скажется на отношениях компании с клиентами, сотрудниками и бизнес-партнерами?
  - Насколько серьезен ущерб деловой репутации в этом случае?
- Какие меры предпринимает компания для защиты конфиденциальной информации?
- Достаточны ли средства защиты моей бизнес-информации?
  - Насколько эти меры соответствуют принятым нормам для моего сектора рынка и размера компании? (Не забывайте, что по мере развития бизнеса вам, скорее всего, понадобится внедрить средства защиты информации более высокого уровня.)
  - Согласится ли суд, что в моей компании применяются надлежащие меры безопасности? (Честный

ответ на этот вопрос может кардинально изменить отношение к безопасности у компаний, которые предпочитают не задумываться о защите информации и уверены, что у них и так все хорошо.)

- Какова вероятность того, что моя компания пострадает от утечки конфиденциальной информации? (Помните, что это может произойти даже при потере ноутбука или смартфона. Возможно, лично вы ведете себя предельно осмотрительно, но насколько осторожны ваши сотрудники?)

Ответы на эти вопросы помогут вам определить, в каком направлении следует улучшать информационную безопасность своей компании.

Обучение сотрудников приемам IT-безопасности

Когда речь идет о защите ценной информации, работает правило «предупрежден — значит вооружен». Поэтому очень важно, чтобы вы и ваши сотрудники были готовы ко всем возможным рискам безопасности и знали, как их избежать.

Просто удивительно, как много компаний пренебрегают обучением своих сотрудников элементарным правилам безопасности. Ведь рассказать людям о возможных рисках и методах борьбы с ними — самый простой и дешевый способ противостоять киберпреступникам.

Привлечь сотрудников на свою сторону в борьбе за безопасность компании совсем несложно.

- Проанализируйте все угрожающие вашей компании риски, связанные с вредоносным ПО и киберпреступлениями, и определите, как ваши сотрудники способны помочь вам их избежать. Несмотря на всю

замысловатость современных угроз, многие атаки начинаются с того, что сотрудника тем или иным способом вынуждают выполнить простое действие, ставящее под угрозу безопасность компании – например, нажать на ссылку в фишинговом сообщении.

- Разработайте и распространите среди сотрудников политику IT-безопасности, которая четко определяет требования к их поведению, необходимые для поддержания безопасности и предотвращения рисков.
- Регулярно проводите для сотрудников разъяснительные собрания. Привлекайте их внимание к ключевым вопросам, таким как:
  - необходимость использовать различные пароли для разных приложений и учетных записей;
  - риски использования общедоступных сетей Wi-Fi и способы их предотвращения;
  - выявление целевых фишинговых атак;
  - последствия потери мобильного устройства для безопасности компании.
- Обеспечьте выполнение политики безопасности, например примите меры, чтобы гарантировать использование надежных паролей для защиты доступа к бизнес-информации, банковским счетам и др.
- Пересматривайте политику безопасности при появлении новых рисков и внедрении новых рабочих процессов.
- Регулярно проводите обучающие курсы, чтобы освежить в памяти сотрудников правила IT-безопасности.
- Обязательно проводите разъяснительные беседы с новыми сотрудниками при введении их в курс дела.

Какой пароль можно считать надежным?

Если в основе пароля лежит легко запоминающееся слово или простая последовательность цифр, киберпреступник его легко угадает. Надежный пароль должен содержать комбинацию из прописных и строчных букв, цифр и специальных знаков и быть не короче восьми символов.

Нельзя использовать один и тот же пароль для нескольких разных приложений или учетных записей. Если киберпреступник узнает пароль сотрудника к учетной записи Facebook, нельзя допустить, чтобы с его помощью он мог получить доступ к корпоративной электронной почте.

В облаках

В последние годы ведется все больше разговоров об облачных технологиях. Компании любого типа и размера оценивают, насколько облака способны упростить хранение информации и сократить затраты.

Иногда небольшие организации перенимают новые бизнес-стратегии быстрее, чем крупные. В то же время небольшие компании часто острее ощущают необходимость сконцентрироваться на своей основной деятельности, не имея возможности уделять достаточно времени IT-безопасности. Поэтому приветствуется любая возможность поручить задачи IT, которые не относятся к основной деятельности компании, внешним специалистам.

В облаке или нет, сохранность вашей информации — это ваша ответственность

Если вы планируете перенести в облако часть бизнес-информации и некоторые или все приложения, помните, что это не освободит вашу компанию от ответственности за их безопасность. Кроме того, это не означает, что ваша конфиденциальная бизнес-информация будет полностью защищена. Независимо от места хранения, эта информация все равно принадлежит вашей компании. Поэтому ответственность за ее защиту по-прежнему несете вы — именно такие обязанности возлагает на вас закон.

Подумайте и о том, как вы будете ежедневно получать доступ к этой информации. Даже если ваш поставщик облачных услуг обладает безупречной репутацией и строго соблюдает все меры безопасности, все равно вам будет необходимо обеспечить надлежащую защиту каждого устройства компании, которое используется для доступа к информации. Вам потребуется по отдельности установить и настроить решение для защиты каждого настольного компьютера, ноутбука, сервера и мобильного устройства.

Никогда не теряйте бдительность

При использовании облачного решения вам и вашим сотрудникам по-прежнему необходимо придерживаться всех стандартных защитных мер, которые определены в вашей политике безопасности. Например, нужно как и раньше использовать надежные пароли для предотвращения несанкционированного доступа к данным, а сотрудники должны принимать меры к тому, чтобы не терять мобильные устройства.

Необходимо также оценить все потенциальные риски безопасности данных и информировать ваш персонал о простых защитных мерах. На самом деле, использование

облачного сервиса вносит единственное отличие: ваша информация хранится удаленно сторонним провайдером.

Будьте внимательны к условиям использования облачных хранилищ

На рынке облачных услуг представлены самые разные решения. Однако многие облачные хранилища предназначены в большей степени для домашних пользователей. При разработке некоторых из них безопасность не являлась первостепенной задачей, поэтому для бизнес-целей они могут быть недостаточно надежны.

Выбирая поставщика, выясните следующее:

- Кому будет принадлежать ваша бизнес-информация при хранении в облаке?
- Что произойдет, если провайдер облачного хранилища прекратит свою деятельность?
  - Будет ли информация по-прежнему вам доступна?
  - Столкнется ли компания с периодом простоя из-за перемещения информации в хранилище другого поставщика услуг?
  - Останутся ли у первого поставщика копии вашей информации, и есть ли способ гарантировать, что они будут удалены?
- Каким образом можно расторгнуть контракт?
  - Если вы решите расторгнуть контракт, как можно будет переместить вашу бизнес-информацию?
- Насколько надежны компьютеры, на которых хранится ваша информация, и коммуникационные системы поставщика, через которые вы будете получать к ней доступ?

- Гарантирует ли поставщик постоянный доступ к вашей информации: будет ли важная информация доступна всегда, когда она нужна, и не придется ли вам сталкиваться с ее недоступностью из-за различных неполадок?
- Внедрены ли у поставщика надлежащие технологии, которые обеспечат быстрое восстановление после серьезных аварий или атак на компьютерные системы, не влияя на безопасность и доступность вашей информации?
- Какой уровень защиты информации от потери и несанкционированного доступа обеспечивает поставщик? (При этом помните, что вам также необходимо использовать защитное программное обеспечение на всех компьютерах и мобильных устройствах, которые используются для доступа к этой информации.)

✔ Где будет храниться ваша информация?

- Не запрещают ли нормативные и правовые требования хранить информацию за пределами страны?

Вы никогда не поручите заботу о своем ребенке кому-то, в ком вы не можете быть полностью уверены. Аналогично, если вы беспокоитесь о безопасности своего детища — вашей компании, необходимо потратить немного времени, чтобы оценить потенциального провайдера облачного хранилища. Это позволит гарантировать, что ваши конфиденциальные и персональные данные находятся в надежных руках.

Аргументы в пользу переноса информации и приложений в облачное хранилище могут быть очень убедительными.

Однако этот шаг нужно делать со всей осторожностью. Несмотря на то, что облачные вычисления могут упростить некоторые аспекты вашей работы с информацией, они могут также добавить дополнительный уровень сложности при работе с ней.

Применение облачных технологий не освобождает вас от ответственности за безопасность конфиденциальной информации. Защита деловой информации — это ваша обязанность, и именно вы будете нести ответственность в случае появления проблем, вызванных отсутствием надлежащих мер безопасности облачного хранилища.

Глава 5

Выбор подходящего защитного решения

В этой главе

- Выбор оптимального поставщика защитного ПО
- Обеспечение необходимой поддержки
- Как могут измениться потребности компании в информационной безопасности
- Выбор оптимального уровня защиты

Итак, вы оценили риски безопасности для своей компании и поговорили с персоналом о важности защиты информации (если вы и есть весь персонал компании, значит, стороны достигли полного взаимопонимания ☺). Осталось выбрать защитное программное решение, которое сможет наилучшим образом обезопасить вашу компанию.

Выбор правильного поставщика

Из всего разнообразия представленных на рынке программных продуктов для защиты IT постарайтесь выбрать решение, способное адаптироваться к изменениям потребностей компании, возникающим по мере ее развития.

Поддержка нужна всем

Выясняйте у поставщиков, на какую поддержку вы сможете рассчитывать, если возникнут проблемы с работой ПО или компания станет жертвой атаки или взлома компьютеров. Возможность сразу же позвонить и получить помощь в сложной ситуации не только очень обнадеживает и успокаивает, но и помогает сэкономить много времени и максимально быстро восстановить работу компьютеров и бизнес-процессов.

Если же поставщик предлагает самостоятельно искать решение проблемы в его базе знаний в Интернете, готовьтесь к тому, что вам придется надолго отвлекаться от важных бизнес-задач. Все прекрасно знают, что подобные технические проблемы всегда возникают в самый ответственный момент — например, в последний день подачи детального предложения по самой важной сделке вашей жизни!

Постарайтесь выбрать поставщика, который оказывает локальную поддержку на вашем языке в вашем часовом поясе.

В процессе выбора защитного решения очень важно найти поставщика, готового предоставить надлежащую поддержку. На рынке есть несколько отличных пакетных решений для обеспечения безопасности, включающих широкий спектр технологий по борьбе с вредоносными программами и интернет-угрозами. Но подумайте, что вы будете делать, когда ваша компания «перерастет» приобретенный пакет.

- Сможет ли выбранный вами поставщик предложить другой пакет с расширенным функционалом?
- Позволяет ли продукт добавлять функции для защиты новых элементов компьютерной сети, например виртуальных серверов, не изменяя продукт и не прибегая к экспертной помощи для выполнения интеграции, требующей много времени?

Сейчас эти вопросы могут казаться не такими уж важными. Однако по мере расширения компании они способны уберечь вас от простоев в работе и затрат, связанных с необходимостью менять поставщика продуктов для обеспечения безопасности.

Достигайте большего за меньшее время

Каждой компании важно, чтобы программные решения, с которыми она работает, были просты в использовании. Кто захочет тратить бесконечные часы на настройку и управление защитным ПО, когда более совершенный продукт позволяет автоматизировать многие процессы защиты и сэкономить драгоценное время для решения других задач?!

Простота в использовании чрезвычайно важна, особенно если у вас нет штатных IT-специалистов. Но даже если ваша компания будет расширяться, и вы наймете сотрудников, отвечающих за IT и безопасность, простое в использовании защитное ПО поможет повысить производительность их труда.

Упрощение управления безопасностью

Пользовательский интерфейс защитного ПО часто называют *консолью управления*. Подобно различным датчикам, указателям и переключателям на приборной панели автомобиля, консоль управления должна обеспечивать быстрый доступ к просмотру информации о работе продукта, сигнализировать о проблемах и позволять менять настройки. Звучит просто, однако многие поставщики программного обеспечения не слишком заботятся об удобстве использования своего продукта.

В некотором защитном ПО пользователю приходится переключаться между несколькими консолями, чтобы управлять различными технологиями защиты, представленными в продукте. Часто это

объясняется тем, что поставщик приобрел различные технологии за счет покупки других компаний-разработчиков защитных продуктов. Какой бы ни была причина, необходимость использовать несколько консолей управления затрудняет работу администратора и требует больше времени.

Другие решения для обеспечения безопасности, напротив, позволяют просматривать и настраивать политики для всех технологий защитного решения в единой унифицированной консоли управления. Это означает, что нужно освоить всего один интерфейс, в котором ясно представлены все технологии защиты, используемые в вашей компьютерной сети.

Если вы собираетесь управлять защитным ПО лично, то благодаря удобству использования и управления у вас останется больше времени на решение более важных бизнес-задач. Но даже если вы поручили заниматься защитным ПО штатному или внешнему специалисту, единая простая консоль управления поможет сократить затраты и повысить эффективность его работы.

Полезные отчеты

Продукт, способный гибко создавать разные виды отчетов о состоянии безопасности и уязвимых местах вашей IT-инфраструктуры, включая мобильные устройства (в том числе используемые в рамках BYOD), позволяет вам быстрее и намного глубже разобраться в любой возникшей проблеме в сфере IT-безопасности.

Амбициозная компания или маленькое семейное дело: определите нужный вам уровень защиты

Иногда стоит не пожалеть немного времени на то, чтобы подумать о перспективах своей компании и откровенно ответить на вопрос, какие цели вы перед собой ставите. Без сомнения, приятно представлять, что однажды ваше предприятие превратится в международную корпорацию, конкурирующую с самыми влиятельными игроками мирового рынка. Однако не каждый владелец компании рассчитывает на такое будущее.

Конечно, есть масса примеров того, как скромные начинания, зародившиеся в гараже или на кухне, со временем превратились в компании мирового уровня.

Но если главная цель вашего бизнеса — просто обеспечить себе и своей семье достойный уровень жизни, не стоит этого стесняться. Определив, что вам действительно необходимо, вы сможете сделать оптимальный выбор относительно инвестиций в безопасность и IT.

Вам нужно всего лишь ответить на следующие вопросы:

- К какому типу принадлежит ваша компания?
- Какой вы видите свою компанию через год и в более долгосрочной перспективе?

Вооружившись этой информацией, вы сможете точнее определить, как могут измениться потребности вашей компании в области защиты информации. Это позволит вам выбрать защитный программный продукт, который наилучшим образом подходит для вашей компании сегодня и обладает необходимой гибкостью и масштабируемостью для адаптации к ее дальнейшим изменениям.

Выбор неправильного решения для обеспечения безопасности, возможно, не станет катастрофой, но может привести к дополнительным затратам и потере времени сейчас или в будущем.

От безопасности домашнего компьютера до защиты бизнеса

Существуют программные продукты для защиты компаний любого размера. Выбор нужного вам решения зависит от ряда факторов.

Продукты для защиты домашних компьютеров

Если в момент создания вашей компании все ее информационные ресурсы были представлены вашим личным ноутбуком, вполне вероятно, что вы использовали одно из многочисленных решений для защиты персональных компьютеров. Многие продукты, предназначенные для домашних пользователей, совмещают в себе технологии защиты от вредоносного ПО и инновационные разработки в области борьбы с интернет-угрозами. А некоторые решения даже предлагают дополнительную защиту операций интернет-банкинга и других финансовых онлайн-транзакций.

Если в компании работают всего несколько человек, защитный продукт для домашнего компьютера может быть идеальным выбором. Однако на рынке представлено множество подобных решений, поэтому нужно уделить немного времени сравнению их функций и возможностей. Решение, обеспечивающее только антивирусную защиту, не справится со всеми современными угрозами.

Как правило, защитное ПО для домашнего использования хорошо подходит компаниям, в которых работают не более

четырех человек. Конечно, это верно только при условии, что лицензия такого продукта разрешает его коммерческое использование. Однако большинством решений для домашних пользователей сложно управлять, когда их используют пять и более сотрудников компании. Такие продукты обычно не позволяют просто и быстро применить настройки и параметры безопасности на всех ноутбуках, настольных компьютерах и мобильных устройствах предприятия.

Если вы планируете значительное расширение бизнеса, ваша IT-инфраструктура, скорее всего, также будет существенно разрастаться и усложняться. Выбрав решение для домашнего использования, не способное расти вместе с вашей компанией, будьте готовы к тому, что когда в развитии компании наступит переломный момент, вам придется перейти на новый защитный продукт. Такой переход потребует финансовых затрат и нарушит привычную работу компании.

Бесплатное антивирусное ПО

Если вы применяете бесплатное антивирусное программное обеспечение, вероятно, вы захотите продолжить его использование, когда компания начнет расширяться. Хотя таким образом можно решить определенные вопросы защиты, стоит разобраться, какими возможностями бесплатное ПО обладает, а какими — нет.

Предлагает ли оно все технологии, необходимые для защиты от новых угроз и изощренных методов кражи ценной информации? Если продукт включает только антивирусные функции и несколько дополнительных компонентов для защиты от интернет-угроз, вероятно, он не сможет оградить вас от всех современных рисков.

Многие бесплатные программные пакеты не предназначены для компаний: часто лицензионные условия таких продуктов запрещают их коммерческое использование. Поэтому применение некоторых бесплатных защитных решений в бизнесе может быть незаконным. Иногда поставщик бесплатного ПО может взимать за его коммерческое использование штраф.

Бесплатный щенок в хорошие руки...

Отличное предложение! Вам всегда хотелось завести верную овчарку, и сейчас вы можете сделать это, не платя большую сумму собаководам. Ну ладно, это дворняга, зато это *ваша* дворняга – и главное, совершенно бесплатная.

Бесплатная... если не считать всех хлопот, беспорядка (раз уж завели любимца, будьте добры убирать за ним!) и расходов. Да, вы учли затраты на прививки и посещения ветеринара, но подумали ли вы о том, сколько ценных вещей сгрызет растущий щенок?

На самом деле, в жизни редко что-то бывает полностью бесплатным. Подобно бесплатному щенку, бесплатное защитное ПО может приводить к неочевидным на первый взгляд затратам. Например, оно может показывать рекламу сторонних продуктов или настойчиво предлагать купить платную «премиум-версию». Эти назойливые баннеры и оповещения отвлекают внимание, поэтому они могут снижать производительность труда ваших сотрудников. Даже если программное обеспечение не использует подобные методы, поддержка такого продукта его поставщиком может оказаться очень дорогостоящей.

Защитные решения для крупных компаний

Осознав все существующие опасности, вы, возможно, решите пойти радикальным путем и приобрести самое многофункциональное решение на рынке.

Многие компании не осознают, что для большинства программных продуктов действует обратная связь между функциональностью и простотой использования. Продукты, в которых имеются функции, необходимые только крупным компаниям, могут быть намного более сложными в настройке и управлении по сравнению с продуктами, предназначенными для малого бизнеса.

Поэтому небольшие компании, решившие пойти простым путем и выбрать самый многофункциональный программный продукт, могут довольно сильно усложнить себе жизнь. Ведь до того момента, когда компания наконец «дорастет» до выбранного защитного ПО, может пройти немало лет! С другой стороны, выбранный вами поставщик может помогать решать задачи безопасности, возникающие по мере развития компании, без необходимости удалять текущий продукт и начинать все с начала.

Защитные решения для крупных компаний могут содержать продвинутые технологии для обеспечения безопасности сложных сред. Однако если ваша IT-сеть относительно проста и вы не планируете ее расширять, то приобретая такое решение, вы платите за функции, которыми, возможно, никогда не воспользуетесь. Более того, слишком сложное решение для обеспечения безопасности может быть и намного более сложным в использовании. Начиная с первой настройки и заканчивая ежедневным управлением – решение корпоративного уровня может требовать времени и навыков, которыми небольшие компании обычно не располагают. Проще говоря, решения корпоративного уровня предполагают наличие в компании соответствующих ресурсов и квалифицированных штатных IT-специалистов.

Безопасность уровня просьюмеров

Безопасность для просьюмеров? Да, это новый термин, введенный маркетологами в модных костюмах. Но что же он означает? (Кстати, если вы руководите маркетинговым агентством... ваш костюм вам очень идет! ☺)

Просьюмеры (от англ. prosumer) – это так называемые «продвинутые» пользователи, которым в силу различных причин приходится выполнять на работе функции IT-администраторов.

Эффективные и удобные в управлении решения для просьюмеров заполняют пробел между совсем простыми в использовании продуктами для домашних пользователей и корпоративными решениями, которые предлагают расширенные возможности, но требуют сложной настройки и управления.

Таким образом, продукты для просьюмеров объединяют в себе необходимый для бизнеса функционал с простотой использования, столь важной для компаний, в штате которых нет специалистов по IT-безопасности. Если производителям удается достичь этого баланса, защитные продукты для просьюмеров являются оптимальным решением для большинства небольших компаний.

Существует заметная разница между продуктами, специально разработанными для малого бизнеса, и корпоративными решениями. Если производитель всего лишь изменил упаковку своего корпоративного решения, и теперь продает его как продукт для просьюмеров, использование такого решения будет по-прежнему сложным и потребует больших временны́х затрат.

Независимо от размера вашей компании, выбирайте поставщика, который учел уникальные требования организаций вашего типа и разработал программное решение, оптимизированное для них.

Корпоративные решения для просьюмеров

На самом деле все еще сложнее. Некоторые продукты, предназначенные для крупных компаний, подходят и для малого бизнеса. Это правда, что продукты, разработанные без учета особенностей небольших компаний, обычно не подходят для организаций, не обладающих внутренними ресурсами для обслуживания системы IT-безопасности. Однако существует класс продуктов для защиты бизнеса, которые основаны на простой модульной архитектуре.

Такие решения могут включать несколько уровней продукта, предлагающих различные комбинации защитных технологий. Самый низкий уровень обеспечивает базовую защиту, которая хорошо подходит для простых IT-сетей, обычно используемых небольшими компаниями. Каждый последующий уровень добавляет новые технологии защиты, а самый высокий уровень предназначен для сложных корпоративных IT-сред и включает поддержку нескольких операционных систем и мобильных платформ, специализированный функционал для обеспечения безопасности виртуальных сред, а также технологии для защиты интернет-шлюзов и почтовых серверов и многие другие возможности.

Такие модульные продукты позволяют небольшим, но амбициозным компаниям использовать защитные решения, которые легко масштабируются по мере расширения бизнеса, не вызывая простоев в работе, которые, как правило, неизбежны при миграции с относительно простого решения для обеспечения безопасности на продукт корпоративного уровня.

Если вам кажется, что вариантов слишком много, помните, что многообразие компаний практически бесконечно, и все они имеют различные требования к IT-безопасности. Поэтому большой выбор — это замечательно! Не пожалейте немного времени на то, чтобы проанализировать различные варианты и взвесить все «за» и «против» — так вы сможете подобрать для своей компании оптимальное защитное решение.

Глава 6

Десять вопросов, которые вам помогут

В этой главе

- Определение требований компании
- Оценка своих правовых обязательств
- Выбор политики безопасности

Эти десять простых вопросов помогут определить, что нужно для защиты вашей компании от кибератак, вредоносного ПО и других рисков IT-безопасности:

- Вы оценили потенциальные риски безопасности для своей компании и определили, какие компьютеры и данные нуждаются в защите?
- Помимо защиты компьютеров, нужно ли защищать мобильные устройства, в том числе используемые в рамках концепции BYOD?
- Знаете ли вы нормативные и правовые обязательства своей компании по защите конфиденциальной информации?
- Вы определили базовые правила безопасности, которые помогут вашей компании защитить информацию, компьютеры и другие устройства?

- Внедрена ли простая обучающая программа, имеющая целью привлечь внимание сотрудников к вопросам защиты информации и мотивировать их к соблюдению правил IT-безопасности?
- Вы проанализировали доступные на рыке защитные программные продукты по следующим критериям: простота использования, предлагаемые уровни защиты и способность адаптироваться к изменению требований безопасности?
- Предлагает ли выбранный вами поставщик защитного ПО необходимый уровень поддержки на вашем языке и в вашем часовом поясе?
- Нужны ли вам функции безопасности для дополнительной защиты интернет-банкинга и финансовых онлайн-операций?
- Если вы планируете использовать облачные хранилища, проверили ли вы условия контракта, в том числе уровень защиты информации?
- Выбрали ли вы программный продукт, способный защитить все компьютеры и мобильные устройства, используемые вашей компанией для доступа к информации, которая хранится в облаке?

Взлом вашей корпоративной сети и кибератаки могут иметь разрушительные последствия. Поэтому убедитесь, что IT-системы вашей компании защищены надежным программным продуктом.

Защитные решения для малого бизнеса

Решения «Лаборатории Касперского» для малого бизнеса позволяют обеспечить безопасность небольших предприятий с минимальными затратами. Продукты «Лаборатории Касперского» – это целый набор инновационных технологий, которые надежно защищают компьютеры, ноутбуки, файловые серверы, а также мобильные устройства и обеспечивают*:

- многоуровневую защиту бизнеса от новейшего вредоносного ПО
- контроль использования программ, устройств и веб-ресурсов
- управление паролями
- защиту ценных данных с помощью технологий шифрования
- управление функциями защиты из единой консоли

Подробнее см. на www.kasperskysmb.ru

**набор функций зависит от продукта и защищаемой платформы*

РАБОТА ВСТАЛА?

Всего один вирус на рабочем компьютере может стереть все ценные данные, украсть деньги с банковского счета и поставить бизнес под угрозу. С решениями «Лаборатории Касперского» ваши данные, финансы и бизнес в безопасности.

БИЗНЕС БЕЗ УГРОЗ

kasperskysmb.ru

KASPERSKY lab

Защита компании от вредоносных программ и кибератак

От стартапов до международных корпораций — компании любого размера все сильнее зависят от компьютеров и мобильных устройств, а значит, они все более уязвимы для атак киберпреступников. В этой книге говорится о том, как эффективно защитить бизнес-информацию, в том числе конфиденциальные данные клиентов компании, и обезопасить ее компьютеры и мобильные устройства от вирусов и другого вредоносного ПО. Наши советы и рекомендации помогут вам тратить меньше времени на безопасность, и больше — на ведение бизнеса.

- ***Узнайте о рисках IT-безопасности — чего надо опасаться вашей компании***
- ***Ознакомьтесь с угрозами — узнайте, как преступники выбирают мишени для нападения***
- ***Спланируйте защиту — избегайте распространенных ошибок***
- ***Защитите свои данные — вооружитесь простым в использовании защитным ПО***

Джорджина Гилмор обладает более чем 20-летним опытом работы в IT-индустрии. Джорджина занимает должность Директора по корпоративным маркетинговым программам и кампаниям «Лаборатории Касперского».
Питер Бирдмор работает в «Лаборатории Касперского» с 2008 г. Обладает обширными практическими знаниями в области IT-маркетинга и управления производством. Питер руководит отделом продуктового маркетинга.

Из этой книги вы узнаете:

- **какие методы атак используют киберпреступники**
- **как обеспечить сохранность ценной информации**
- **как выбрать защитное ПО, подходящее именно вашей компании**

WILEY

ISBN: 9781118848135