



ПЕРСОНАЛЬНЫЕ ДАННЫЕ '08 В РОССИИ

InformationSecurity
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ



ABISS
Association for Banking Information
Security Standards





ВВЕДЕНИЕ	3
КЛЮЧЕВЫЕ ВЫВОДЫ	4
МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ И ПОРТРЕТ РЕСПОНДЕНТА	5
ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИЙСКИХ КОМПАНИЯХ	8
ЗАКОНОДАТЕЛЬНОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ	13
ЗАКЛЮЧЕНИЕ	19
О КОМПАНИИ PERIMETRIX	20
О ПРОЕКТЕ «БАНКИР.РУ»	20
О ПРОЕКТЕ «INFORMATION SECURITY»	21
О СООБЩЕСТВЕ «ABISS»	21

ВВЕДЕНИЕ

Персональные данные (ПД) клиентов, партнеров и сотрудников являются важнейшим активом любой современной компании и в то же время ее серьезной проблемой. Утечка персональных данных не выгодна ни компании (она испытывает масштабные репутационные потери), ни владельцам этой информации (они испытывают как минимум беспокойство, а нередко становятся и жертвами различных афер).

Персональные данные остро нуждаются в специализированной защите от инсайдеров, хакеров и халатных сотрудников. Эта задача является социально важной, и бывший президент РФ Владимир Путин издал для ее решения федеральный закон, который

так и называется: ФЗ «О персональных данных». За первые два года своего существования закон не сумел заработать на практике, однако в последнее время стали наблюдаться активные попытки его возвращения к жизни.

Настоящее исследование призвано выявить текущий уровень защищенности персональных данных в российских компаниях, а также отношение игроков рынка к законодательному регулированию. В рамках исследования будут также приведены прогнозы развития ситуации в течение нескольких ближайших лет и рекомендации для операторов персональных данных.

КЛЮЧЕВЫЕ ВЫВОДЫ

- Защита персональных данных является серьезной проблемой для российских организаций. 52,0% компаний-респондентов обрабатывают более 10 тыс. записей о персональных данных, а 15,3% – более 1 млн. записей.
- В большинстве случаев (57,6%) доступ к массивам персональных данных имеют сотрудники службы безопасности и персонал ИТ-подразделений компаний. Риски утечки персональных данных через ИТ-персонал являются наиболее высокими. Кроме того, в 21,9% случаев компании испытывают риски утечек через топ-менеджеров или руководителей ведущих подразделений.
- Только 64,3% компаний имеют монопольный доступ к обрабатываемым персональным данным, остальные допускают к информации дочерние или материнские структуры либо партнеров. Для 13,1% операторов это зарубежные фирмы.
- Основная трудность в реализации положений Федерального закона «О персональных данных» заключается в неясном характере этих положений (34,7%). Следом располагаются классические проблемы информационной безопасности: бюджетные ограничения (20,6%) и отсутствие квалифицированных кадров (19,0%).
- Практически две трети (65,3%) специалистов предполагают, что требование обязательного разглашения сведений об утечках персональных данных должно быть включено в федеральный закон.

МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ

Данное исследование проводилось в форме онлайн-анкетирования ИТ- и ИБ-специалистов. В период проведения исследования (с 7 июля по 7 сентября) было опрошено 389 респондентов, представляющих компании различных размеров и отраслей. Перед ответами на основные вопросы исследования респондентам предлагалось рассказать о компаниях, в которых они работают.

Распределение компаний-респондентов по размеру (см. рис. 1) оказалось достаточно равномерным – в нем присутствуют компании малого бизнеса, предприятия среднего размера и крупные корпорации, имеющие более 10 тыс. сотрудников.

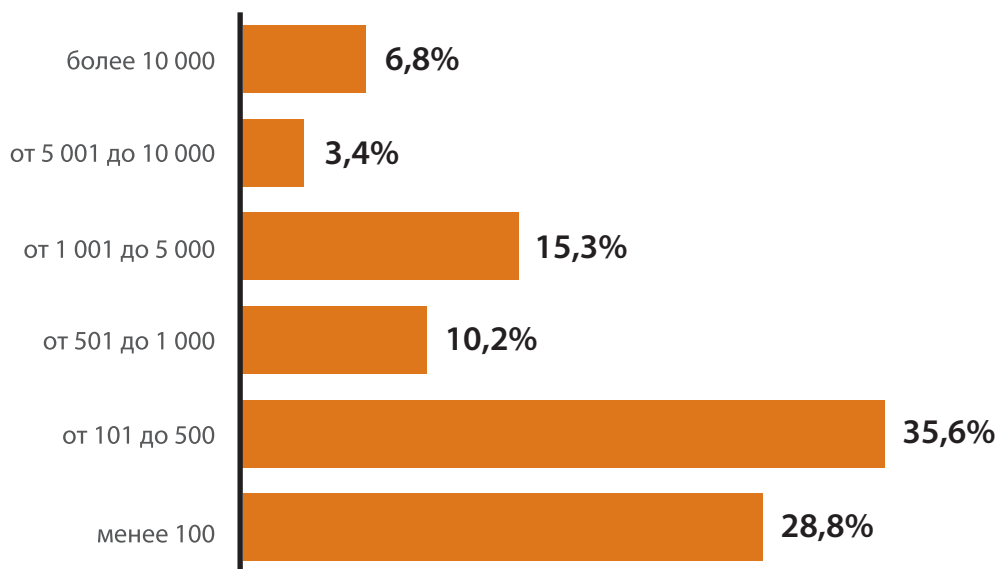


Рис. 1 Количество сотрудников

Отраслевое распределение (см. рис. 2), напротив, является очень специфичным. Практически три четверти (72,5%) респондентов представляют всего лишь два вертикальных рынка: финансовую и телекоммуникационную отрасли. С одной стороны, предприятия этих отраслей обрабатывают максимальное количество персональных данных, с

другой – именно финансовые и телеком-компании всегда являлись пионерами внедрения информационных технологий, а также решений по информационной безопасности. В этом свете совсем не удивителен тот факт, что представители именно таких компаний приняли наиболее активное участие в исследовании.

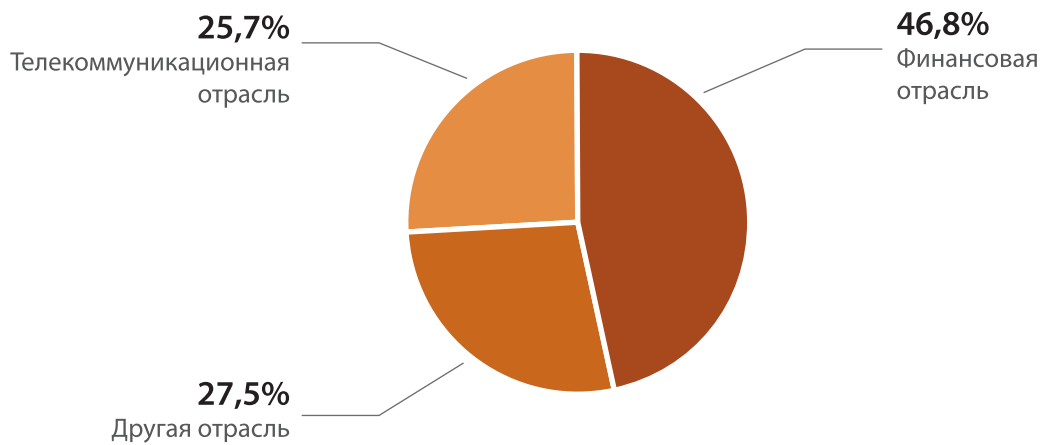


Рис. 2 Сфера деятельности

Из получившегося отраслевого распределения логично сделать два основных вывода. Во-первых, очевидное смещение в сторону финансовых и телекоммуникационных компаний позволяет получить четкое представление о защищенности персональ-

ных данных именно в этих типах организаций. И, во-вторых, оно дает информацию об общих трендах развития отрасли, поскольку финансовая и телекоммуникационная сферы являются ее основными драйверами.

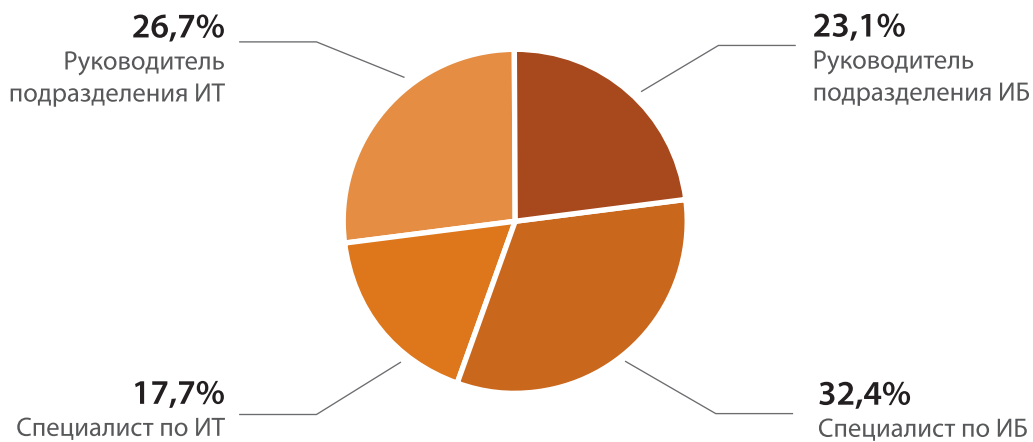


Рис. 3 Должность респондента

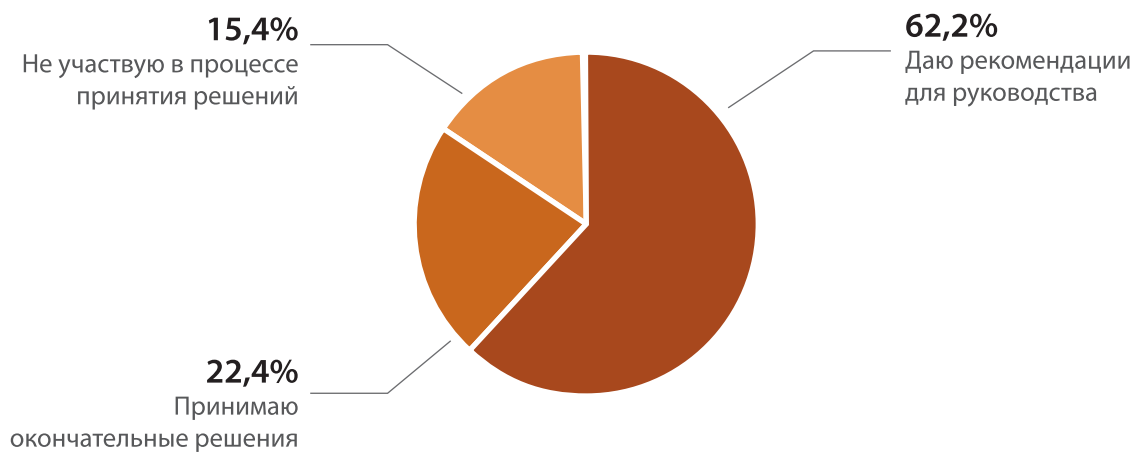


Рис. 4 Ответственность респондента в области информационной безопасности

Профессиональное распределение респондентов показано на рис. 3 и 4. В рамках исследования были учтены ответы только сотрудников департаментов информационных технологий и информационной безопасности различных организаций. Это означает,

что все участники опроса так или иначе задействованы в процессах обработки и защиты персональных данных. Отметим, что подавляющее большинство респондентов (84,6%) участвуют в процессах принятия решений в области информационной безопасности.

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИЙСКИХ КОМПАНИЯХ

Все вопросы, которые задавались респондентам в рамках исследования, можно разделить на две основные части. В первой части участникам опроса предлагалось рассказать об использовании ПД в своих компаниях, а вторая часть была посвящена влиянию различных нормативных актов на степень безопасности персональных данных. В обоих случаях респондентам задавались лишь косвенные и максимально конкретные вопросы, поскольку прямые и комплексные формулировки («Насколько защищены ПД в вашей организации?», «Как влияет федеральный закон на защищенность ПД?» и т.д.) не дают представления об истинном положении вещей и побуждают специалистов давать не всегда объективную оценку. Проблема в том, что каждый конкретный специалист имеет собственное мнение о безопасности, и сравнивать эти мнения друг с другом по дифференцированным критериям технически невозможно.

Внимание каждой компании к проблеме защиты персональных данных напрямую зависит от цело-

го ряда факторов. Первым фактором этого списка является масштаб проблемы – то есть количество обрабатываемых записей персональных данных. С ростом количества персональных записей растут и риски компании, которые с этими записями связаны. Как следствие, чем больше записей обрабатывает компания – тем большую ответственность она несет за их защиту.

Из ответов на следующий вопрос (см. рис. 5) следует, что более чем половина респондентов (52,0%) преодолели «психологическую» отметку в 10 тыс. записей персональных данных. Утечку такого объема информации уже нельзя назвать локальным инцидентом, поскольку она затрагивает количество людей, сравнимое с населением небольшого города. Всем пострадавшим в результате утечки такого масштаба крайне трудно предоставить адекватную защиту, а значит – реальные последствия инцидента практически невозможно проконтролировать.

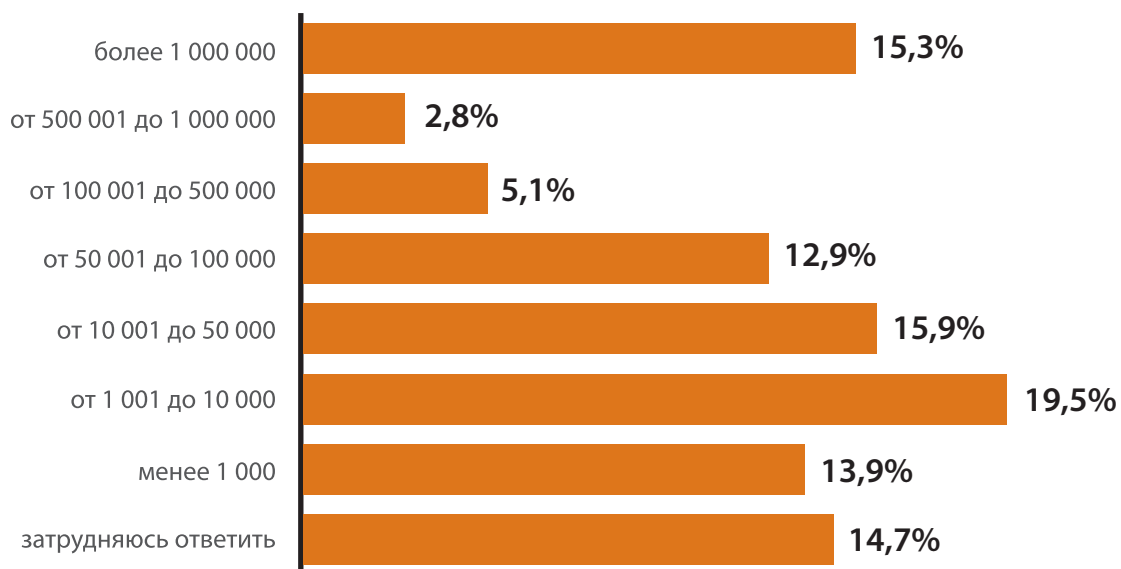


Рис. 5 Количество записей ПД в российских компаниях

В особую группу риска попадают организации, обрабатывающие огромные объемы персональных данных, которые измеряются миллионами записей. Таких предприятий в России тоже хватает – их представляют более 15% участников опроса. И если компания, хранящая сведения десятков тысяч людей, еще как-то может полагаться «на авось», не заботясь об адекватной защите, то для крупных компаний такой подход абсолютно неприемлем. Когда становится известным об утечке миллионного масштаба, различные медиаагентства быстро тиражируют новость и распространяют подробности инцидента. Репутация небрежной компании начинает резко падать вниз, что неизбежно приводит к мгновенному падению стоимости акций и долгосрочным потерям в будущем.

Каким образом могут «утекать» персональные данные? По данным мировой статистики по инцидентам, около 90% всех происходящих утечек так или иначе связаны с действиями персонала. В данном случае речь идет не только о спланированном инсайде (то есть краже информации), хотя и эта проблема является достаточно серьезной. Кроме инсайда, существует масса других сценариев утечки, большая часть из которых связана с банальной халатностью сотрудников либо с бездействием службы безопасности. Аналитический центр Perimetrix выделяет пять наиболее стандартных сценариев утечки персональных данных:

- Кража или потеря носителей (ноутбуков) с персональными данными;
- Web-утечка: случайная публикация персональных данных в общедоступных местах (Интернете или интранете);
- Спланированный инсайд: умышленная кража информации сотрудником, имеющим легальный доступ к ней;
- Бумажная утечка: печать и распространение персональных данных на бумажных носителях;
- Внешний взлом корпоративной сети.

Полученное распределение показывает, что примерно половина отечественных специалистов работает в компаниях, которые уязвимы перед утечками персональных данных. Другими словами, защита этих персональных данных является весьма масштабной проблемой, которая пронизывает все сферы отечественного бизнеса.

Первые четыре сценария являются внутренними угрозами информационной безопасности. Таким образом, риски утечек персональных данных напрямую зависят от количества людей, имеющих доступ к массивам этой информации (см. рис. б).

В идеале доступ к персональным данным должны иметь только сотрудники службы безопасности. На практике такая ситуация встречается очень редко (5,1%) – в большинстве случаев доступ к информации (57,6%) имеет и ИТ-персонал организации. Таким образом, риски возможной утечки информации значительно увеличиваются, поскольку численность персонала ИТ-департамента заметно выше, а истории про «обиженных сисадминов» давно перестали быть основой для анекдотов и переместились во вполне реальную плоскость.

Впрочем, ИТ-персонал является далеко не единственной угрозой безопасности персональных данных. Достаточно часто (21,9%) доступ к этой информации предоставляется топ-менеджерам, действия которых всегда отличаются повышенным уровнем халатности. Но на практике отсутствие доступа к любым корпоративным сведениям вызывает негодование со стороны руководителей. И, избегая конфликтных ситуаций, ИТ- и ИБ-специалисты нередко предоставляют начальникам полный доступ. Кроме того, определенные опасения вызывают сотрудники аналитических служб, имеющие доступ к персональным данным в 18,5% случаев. Тогда как для данной категории работников, в большинстве случаев, вполне достаточно было бы обезличенных статистических выборок.

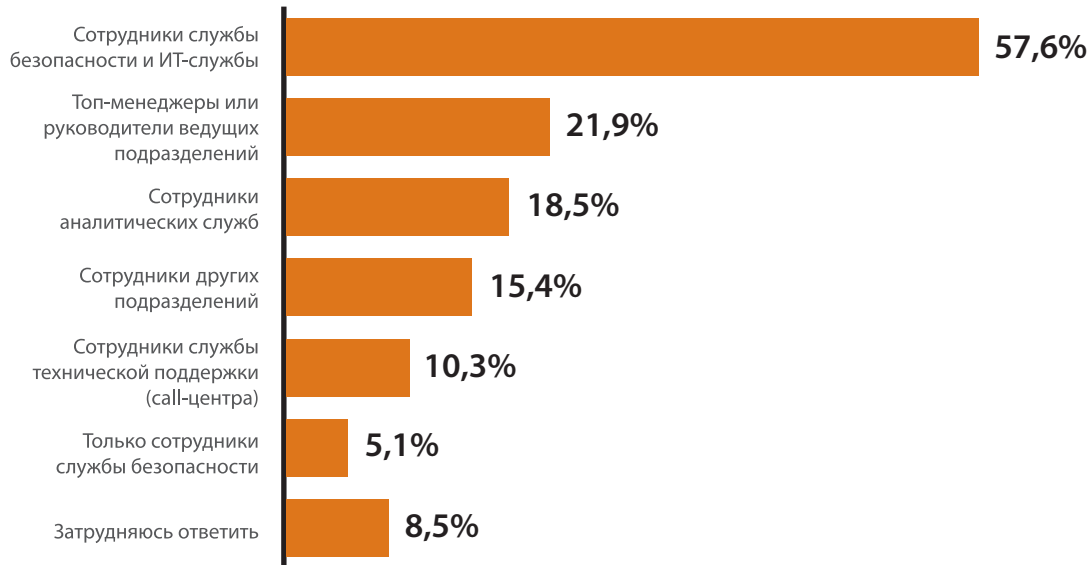


Рис. 6 Кто имеет доступ к массивам ПД¹?

Отдельного внимания заслуживают службы технической поддержки и контактные центры. Эти подразделения, как правило, комплектуются не самыми квалифицированными сотрудниками и обладают высоким уровнем текучки кадров. При этом операторы контактных центров практически всегда имеют доступ к персональным данным, которые необходимы им для обслуживания клиентов.

Исследование показало, что сотрудники технической поддержки и call-центров сравнительно редко (10,3% случаев) получают доступ к массивам персо-

нальных данных. Они могут посмотреть конкретные записи персональных данных «по запросу», но не обладают правами для действий с базами конфиденциальных сведений. Это означает, что угроза утечки из контактного центра все же существует, однако не является слишком опасной - украсть большое количество информации посредством единичных запросов весьма проблематично (хотя и такие случаи известны). В данном случае уместнее говорить не об угрозе утечек персональных сведений, а о возможной слежке за конкретными людьми и предоставлении информации о них за определенную плату.

¹ Сумма долей больше 100%, поскольку респонденты могли выбрать несколько вариантов ответа

Защищенность персональных данных (см. рис. 7) практически идентична защищенности информации, которая составляет коммерческую тайну. Из этого тезиса можно сделать два вывода: с одной стороны, российские компании осознают важность защиты персональных данных, с другой – осозна-

ние этого факта отнюдь не равноценно качественной системе безопасности. В большинстве современных предприятий защищенность персональных данных и защищенность сведений, которые составляют коммерческую тайну, находятся на одинаково низком уровне.

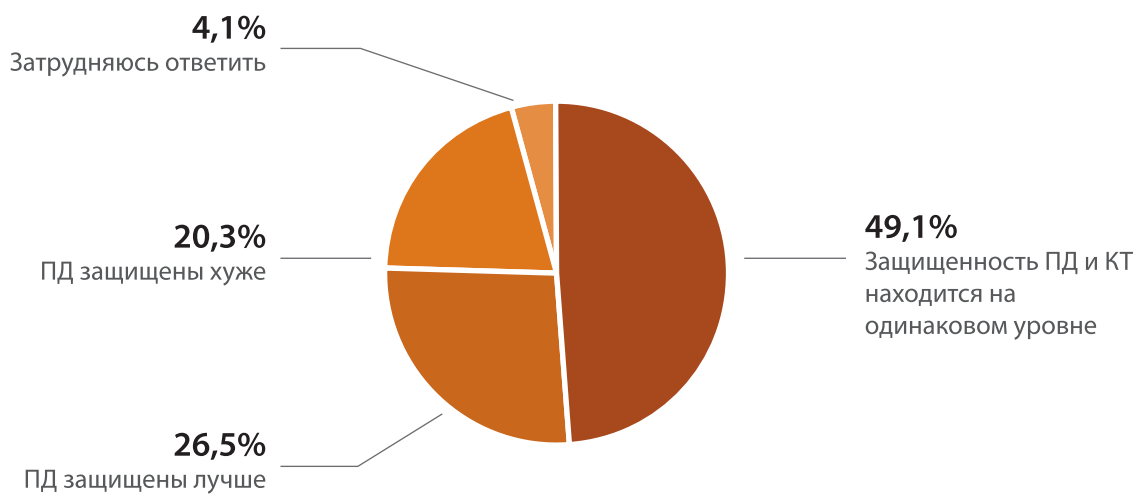


Рис. 7 Защищенность ПД в сравнении с защищенностью сведений, составляющих коммерческую тайну

Действительно, по данным другого исследования Perimetrix («Инсайдерские угрозы 2008»), два наиболее действенных класса систем защиты – решения для шифрования данных в местах хранения и комплексные продукты по защите от утечек – имеют довольно низкое проникновение на российском рынке (36% и 24% соответственно). Все остальные системы безопасности занимаются защитой исключительно от внешних вторжений и потому не могут ничего поделать с более опасными внутренними угрозами.

В последнее время все большую актуальность стали приобретать так называемые «партнерские утечки» персональных данных, которые допускаются «третьими» компаниями. По данным Ponemon Institute, практически 40% мировых инцидентов возникают в результате ошибочных действий партнеров, аутсорсеров и, что особенно интересно, логистических вендоров. Последние компании довольно часто теряют носители с приватными данными во время транспортировки.

В нашей стране культура аутсорсинга пока еще далека от западной, и потому российская ситуация с партнерскими утечками (см. рис. 8) не так сложна. Две трети (64,3%) отечественных компаний не делятся своими персональными данными

ни с кем и никогда, а еще 24,7% – разделяют информацию только с дочерними и материнскими структурами. И только 11,1% респондентов испытывают риски партнерских утечек по полной программе.

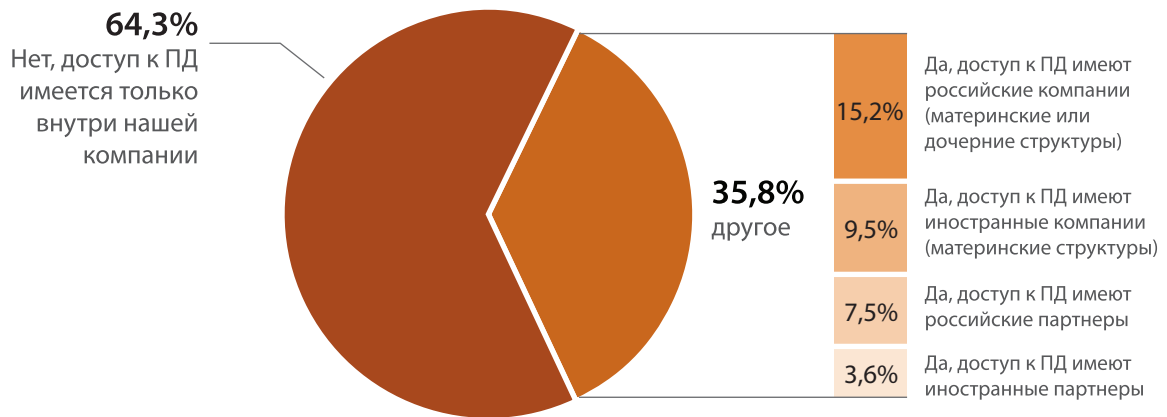


Рис. 8 Сторонние компании, имеющие доступ к ПД

В этом свете было бы логично рассказать о другой проблеме, с которой сталкиваются 13,1% российских организаций. Именно эта часть компании делится персональными данными с иностранными организациями – материнскими компаниями или обычными партнерами. Вместе с тем согласно Федеральному закону «О персональных данных» делать это можно лишь с согласия владельцев информации, которое технически невозможно получить.

Как следствие, перед иностранными компаниями возникают масштабные ограничения на трансграничную передачу персональных данных. Согласно букве закона, они не могут послать аудитора для проверки деятельности дочерней структуры, по-

скольку тот неизбежно получит доступ к персональной информации российских граждан. Они не могут создавать общие дата-центры консолидированного хранения российских персональных данных и информации жителей из других стран. Наконец, они не могут обслуживать российских клиентов за границей, поскольку не имеют доступа к их персональной информации.

Получается типичный правовой коллапс – ограничения закона оказываются невыполнимыми, и потому они фактически не выполняются. При этом перед всеми иностранными компаниями возникают масштабные правовые и репутационные риски, которые в теории могут привести к сворачиванию бизнеса в России.

ЗАКОНОДАТЕЛЬНОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

С точки зрения российского законодательства использование персональных данных в отечественных организациях жестко зарегулировано. Основным документом, регламентирующим меры защиты персональных данных, является одноименный федеральный закон, вступивший в действие 30 января 2007 года. За время, прошедшее с этого момента, закон практически не применялся на практике, однако в настоящее время наблюдаются серьезные предпосылки к изменению сложившейся ситуации. Итак, что же представляет собой Федеральный закон «О персональных данных»? По сути, он является высокоуровневым набором концептуальных требований к защите персональной информации. Отдельно подчеркнем, что под действие федерального закона попадают фактически все компании, которые имеют в своем составе хотя бы отдел кадров и бухгалтерию.

В области защиты информации закон выдвигает самые общие требования, не опускаясь до конкретных деталей. Например, норматив гласит, что «оператор персональных данных обязан принимать необходимые организационные и технические меры... для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий». Конкретики в законе нет, и определять степень необходимости мер фактически должна каждая конкретная организация. Именно поэтому закон в его нынешнем виде почти невозможно применить на практике. Без более детальных требований («методичек») норматив практически теряет смысл, оставаясь лишь набором общих рекомендаций.

В ноябре 2007 года тогдашний премьер-министр России Виктор Зубков подписал специальное распоряжение («Положение об обеспечении безопасности персональных данных при их обработке в ин-

формационных системах персональных данных»), в рамках которого обязал уполномоченные органы (ФСБ и ФСТЭК) написать более детальные нормы к федеральному закону к 18 февраля 2008 году. Нетрудно догадаться, что к обозначенной дате никаких нормативов не появилось.

Тем не менее в июле 2008 года первый документ такого рода все-таки был опубликован правительством РФ. Постановление № 512 содержит конкретизированные требования к «материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных». Конечно, этот документ не может покрыть все случаи, которые регулируются ФЗ, однако его публикацию можно расценивать как безусловный позитивный сдвиг.

Публикация конкретизирующих нормативов является не единственной попыткой правительства оживить фактически мертвый закон. В конце 2007 года стартовала разработка реестра операторов персональных данных, а также был назначен орган, ответственный за этот реестр (Россвязькомнадзор). Спустя четыре месяца представители регулятора объявили о создании реестра и призвали все российские компании внести туда свою информацию. На момент подготовки этого исследования в реестре содержались сведения о 17 тыс. операторов персональных данных.

Так или иначе, в течение последних 12 месяцев правительство наконец-то стало проявлять хотя бы какую-то активность. Конечно, пока эта активность недостаточна для реального применения закона на практике, однако сама тенденция заставляет задуматься. По мнению экспертов аналитического центра Perimetrix, существует достаточно высокая вероятность резкого усиления нормативного пресинга уже в ближайшие полтора-два года.

Рост озабоченности российских компаний влиянием федерального закона косвенно подтверждается собранной статистикой. Абсолютное большинство (79,7%) специалистов (см. рис. 9) уже пытались вни-

кать в положения ФЗ и задумывались о его возможном влиянии на бизнес. Оставшиеся 20,3% респондентов имеют о законе смутное представление либо вовсе с ним не знакомы.

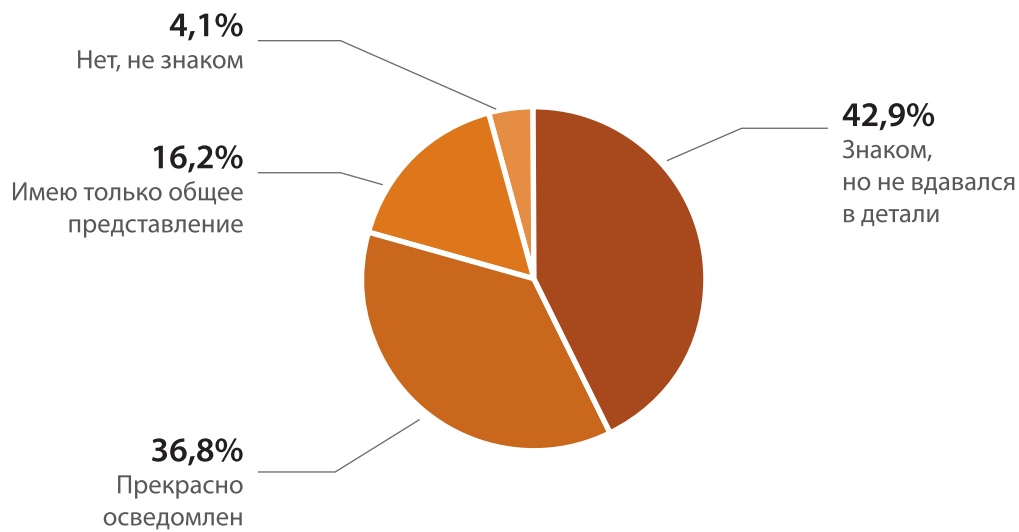


Рис. 9 Осведомленность специалистов о ФЗ «О персональных данных»

Пятая часть (20,3%) респондентов предполагает (рис. 10), что их компания полностью удовлетворяет требованиям закона. Весьма смелое утверждение, особенно если учесть туманность и размытость этих требований. В каждом конкретном случае трактовка положений ФЗ может производиться по-разному и до появления конкретизирующих нормативов заявлять о полном соответствии почти бессмысленно.

Вместе с тем более половины специалистов честно признают, что их компании выполняют не все требования закона (46,3%) либо не выполняют их вовсе (11,1%). Для достижения соответствия этим компаниям придется инвестировать средства в развитие системы информационной безопасности.

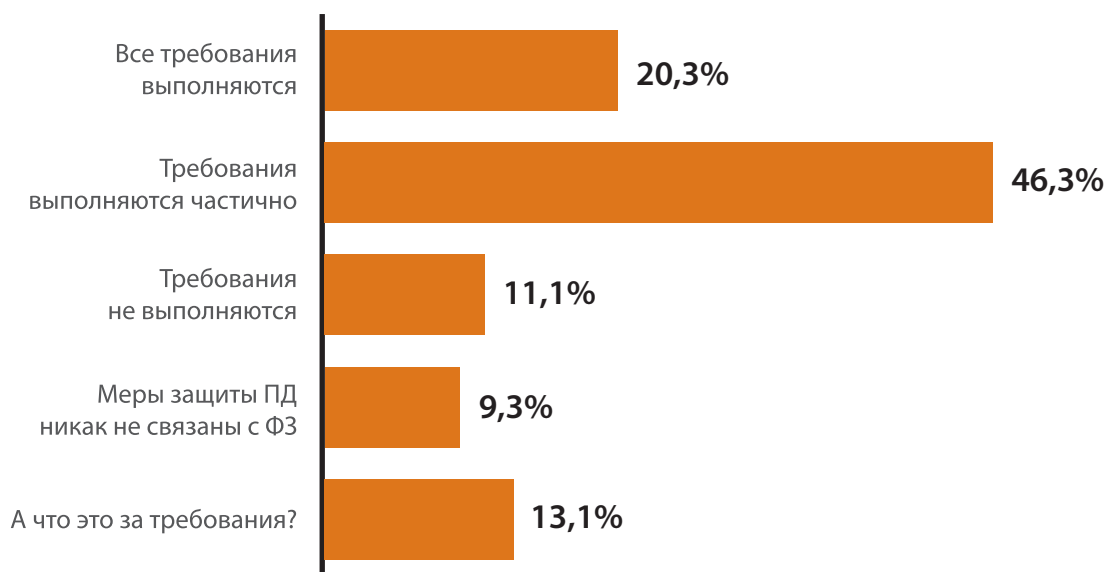


Рис. 10 Соответствие требованиям ФЗ «О персональных данных»

Основным препятствием на пути соответствия закону (см. рис. 11) является нечеткость и размытость его положений – эту проблему отметили почти 35% респондентов. Как и всегда, весьма актуальными трудностями являются бюджетные ограничения, а также отсутствие квалифицированных специалистов – каждый из этих пунктов набрал примерно по 20% голосов. Остальные сдерживающие факторы, по-видимому, не являются серьезной проблемой для большинства организаций.

В общем и целом, операторы персональных данных готовы добиться соответствия федеральному закону, однако они не могут понять, как именно это можно сделать. Медлительность чиновников оказывает негативное влияние и на вендоров систем защиты, которые теряют ориентиры при разработке защитных продуктов. Можно с уверенностью утверждать, что работающий федеральный закон нужен не только для защиты владельцев ПД, но и для развития рынка информационной безопасности в целом.

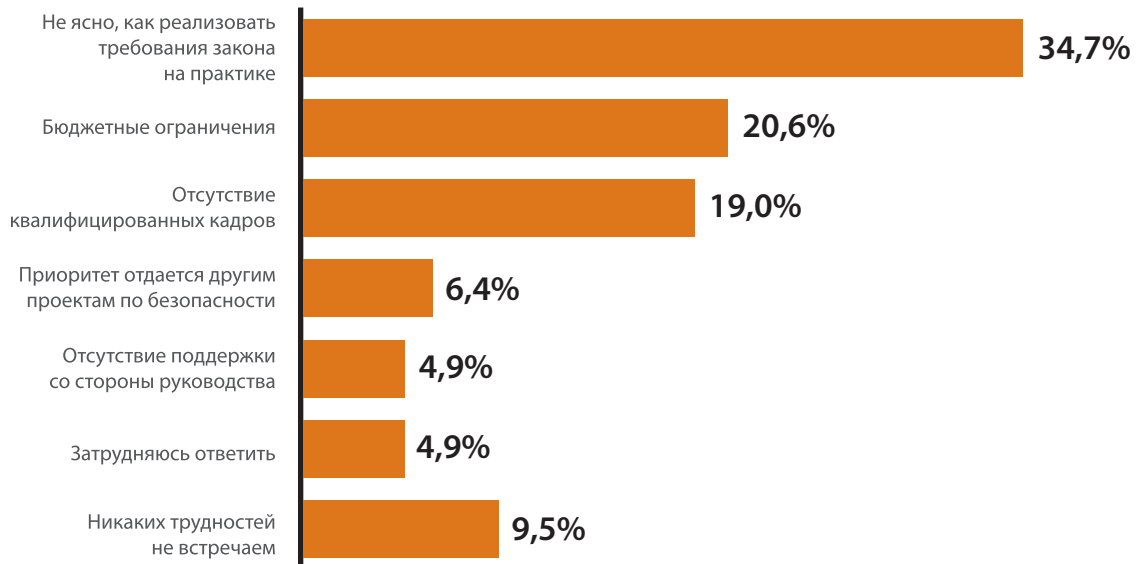


Рис. 11 Осведомленность специалистов о ФЗ «О персональных данных»

Более того, участники рынка считают важным не только выполнять положения ФЗ в их нынешнем виде (при условии публикации конкретизирующих документов), но и даже усиливать их в целях защиты владельцев персональных данных. В частности, практически две трети (65,3%) респондентов уверены (см. рис. 12), что требование об обязательном разглашении информации об утечках ПД должно быть включено в федеральный закон. Такое требование, уже прописанное в законодательствах ряда развитых западных странах, значительно увеличит ущерб компаний в результате каждой утечки информации. А значит – заставит уделять безопасности большее внимание и повысит роль подразделений, которые за нее отвечают.

В таком разрезе полученные результаты не удивляют – любой специалист хочет увеличить свое влияние и значимость в жизни компании. Это означает, что требование «обязательного разглашения» рано или поздно появится в федеральном законе. Фактически оно выгодно всем участникам рынка – и регулятору (усиление нормативного прессинга), и специалистам по безопасности (усиление внутрикорпоративной роли), и непосредственным владельцам персональных данных (усиление защищенности). Оно невыгодно лишь владельцам и инвесторам компаний, однако лагерь противников достаточно немногочисленен.

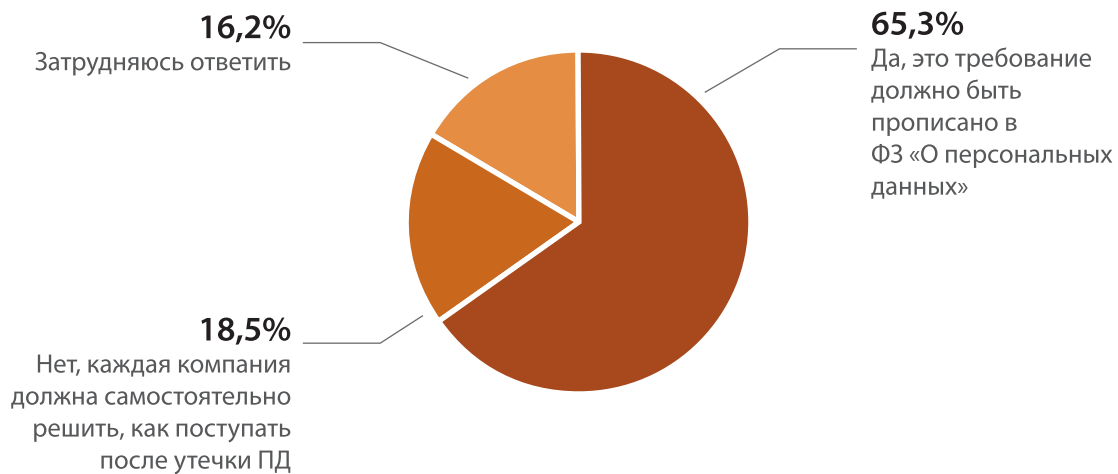


Рис. 12 Должны ли компании разглашать сведения об утечках ПД?

Резюмируя все вышесказанное, легко прийти к выводу о растущем влиянии федерального закона в сравнении с другими регулируемыми документами. Этот закон уже сейчас (рис. 13) является более

значимым документом, чем все остальные нормативные акты, и в том числе и отраслевые стандарты. В будущем, по мере конкретизации требований закона, его влияние на бизнес только увеличится.

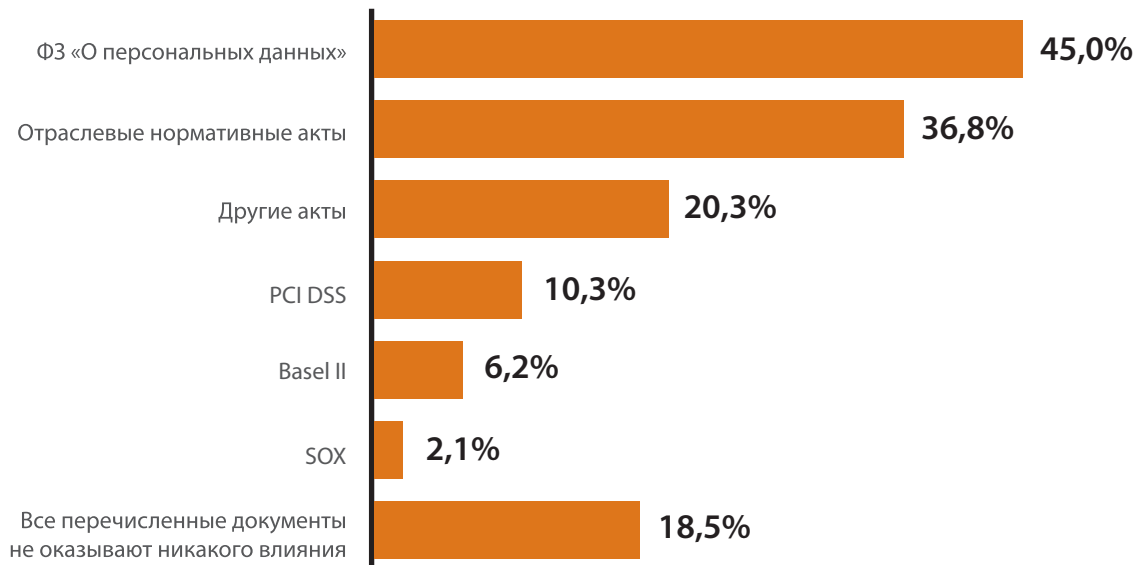


Рис. 13 Степень влияния различных нормативных актов на защищенность персональных данных¹

Впрочем, преуменьшать значение других документов также не стоит. В отличие от федерального закона (под действия которого подпадают едва ли не все организации) они имеют ограниченную область применения и иногда – необязательный характер. Однако требования таких нормативов как, «Базо-

вый уровень операторов связи», стандарт Банка России «СТО БР ИББС» или стандарт PCI DSS, можно реализовать уже сегодня. Как следствие, некоторые компании рассматривают именно эти документы в качестве дорожной карты для создания корпоративной системы безопасности.

¹ Сумма долей больше 100%, поскольку респонденты могли выбрать несколько вариантов ответа

ЗАКЛЮЧЕНИЕ

Исследование «Персональные данные в России 2008» показало чрезвычайную важность и растущую актуальность защиты персональных данных. На сегодняшний день российские компании обрабатывают огромное количество персональных данных, доступ к которым имеет целый ряд корпоративных подразделений и департаментов. В большинстве случаев этот доступ никак не контролируется, что приводит к высоким рискам утечки.

Законодательное регулирование защиты ПД до сих пор практически не работает, а основной норматив – ФЗ «О персональных данных» - по-прежнему выдвигает слишком общие и неконкретные требования. Каждая компания трактует эти требования исходя из собственных соображений, а иногда просто их игнорирует. Правоприменительная практика в отношении ФЗ отсутствует, контроль над исполнением закона де-факто не производится.

Вместе с тем российское правительство пытается (хотя и не слишком активно) реанимировать федеральный закон и получить хотя бы какой-то контроль над операторами персональных данных. Несколько, казалось бы, незначительных шагов, которые были предприняты в течение последнего года, наглядно показали общественности, что государство не собирается отказываться от своих замыслов. От этих действий закон «О персональных данных» не стал понятнее, однако он приобрел некую новую актуальность, которая со временем будет только расти.

Поскольку ФЗ уже давно вступил в силу, российские компании должны быть готовы к публикации конкретизирующих документов и появлению контроля над исполнением закона. Конечно, это событие не может произойти в один момент, однако и реализация комплекса защитных мер требует времени. Задумываться о защите персональных данных необходимо уже сегодня, внедряя защиту – завтра, а послезавтра – спокойно наблюдать за схваткой государства и менее дальновидных компаний.

О ПРОЕКТЕ «INFORMATION SECURITY/ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

- Журнал «Информационная безопасность», который выходит тиражом 10 тыс. экземпляров 8 раз в год и распространяется по схеме B2B среди руководителей и владельцев IT-компаний и компаний-потребителей, начальников IT-отделов и технических специалистов;
- ежегодный каталог «IT-Security. Системы и средства защиты информации», предназначенный для руководителей и специалистов, отвечающих за закупки продуктов, систем и услуг в области информационной безопасности;
- еженедельная электронная газета «Information Security», аудитория которой – более 4 тыс. постоянных подписчиков;
- конференции серии «профессиональный диалог», организуемые на высоком уровне для тщательно отобранной аудитории потребителей;
- отраслевой портал www.itsec.ru, ежедневную аудиторию которого составляют более 700 профессионалов.

О ПРОЕКТЕ «БАНКИР.РУ»

Главное направление деятельности Банкир.Ру – активное участие в развитии банковского бизнеса в России, улучшение качества и расширение спектра финансовых услуг клиентам российских банков. Мы считаем, что банковская система РФ должна и может быть конкурентоспособна по отношению к ведущим мировым финансовым системам. Наша цель – продвижение и развитие банковского дела в России, повышение квалификации банковского персонала.

Развитие банковского рынка зависит не только от деятельности государственных органов управления и Центрального банка РФ, но и не в последнюю очередь от самих кредитных организаций, от их понимания законов развития бизнеса, от намерений

расширения деятельности. Коммерческие банки, банковские ассоциации и союзы, Центральный банк РФ должны объединить усилия для достижения общих целей, наладить конструктивный диалог, способствовать профессиональному росту специалистов банковского дела.

На сайте Банкир.Ру любой посетитель найдет ответ на интересующий его вопрос по банковской деятельности и не только; познакомится с последними новостями, аналитическими материалами и интересными людьми; узнает много нового и интересно о действующих кредитных организациях; сможет найти новое место работы или подобрать квалифицированного специалиста для работы в банке.

О СООБЩЕСТВЕ ABISS

Сообщество пользователей стандартов Центрального банка Российской Федерации (далее по тексту Банк России) по обеспечению информационной безопасности организаций банковской системы Российской Федерации (далее по тексту сообщество ABISS – [Association for Banking Information Security Standards]) – это сообщество организаций, деятельность которых направлена на развитие и продвижение Стандарта Банка России

СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения», его последующих версий и дополнений, а также других стандартов, положений и методических указаний Банка России, регламентирующих вопросы информационной безопасности организаций банковской системы Российской Федерации.

О КОМПАНИИ PERIMETRIX

Компания Perimetrix разрабатывает уникальные решения для реализации режима секретности конфиденциальности данных. В отличие от конкурентов Perimetrix концентрирует свой потенциал, инновационный подход и уникальный опыт на создании корпоративной платформы внутренней информационной безопасности и интеграции с актуальными бизнес-процессами, организационной и технологической инфраструктурой заказчика. Наша цель – повышение стоимости бизнеса заказчиков за счёт поддержания непрерывности бизнес-процессов, минимизации риска утечки, повышения конкурентоспособности, а также установления плодотворных отношений с инвесторами и партнерами, соответствия государственным требованиям.

Благодаря реализации революционной концепции Secret Documents Lifecycle™ Perimetrix обеспечивает защиту секретных документов на всех этапах жизненного цикла, мониторинг каналов коммуникаций и аудит электронных операций. Технологическая основа системы – знание объекта защиты, контроль доступа и действий пользователей с целью предотвращения нарушения корпоративной политики.

Компания основана в 2007 году командой профессионалов, стоявших у истоков создания современных систем защиты от внутренних угроз информационной безопасности, и входит в Группу компаний «КомпьюЛинк» – лидирующий альянс на российском рынке информационных технологий.



Штаб-квартира Perimetrix

Российская Федерация,
119607, Москва,
Мичуринский проспект, д. 45

Телефон: +7 495 737 99 91
Факс: +7 495 737 99 92

info@perimetrix.com
www.perimetrix.com

**Штаб-квартира Information Security/
Информационная безопасность**

Российская Федерация,
123007, Москва,
3-я Магистральная улица, д. 30

Телефон + 7 495 609 32 31
www.itsec.ru

Почтовый адрес:
123007, Москва, а/я 82