ЗИ

АКАДЕМИЯ
СОВРЕМЕННЫХ
ИНФОКОММУНИКАЦИОННЫХ
ТЕХНОЛОГИЙ

ЗИ **Защита информации**

ЗИ.4 Защита данных в российских компаниях
(количество частей – 1, число страниц - 17)

ЗИ.4

Исследование Zecurion и HeadHunter

Защита данных в российских компаниях

ZECURION

Резюме

Аналитический центр Zecurion Analytics представляет результаты опроса по организации информационной безопасности в российских компаниях, проведенного совместно с компанией HeadHunter среди руководителей ИТ-подразделений. Интерес к этой теме был вызван наблюдениями за процессом развития рынка ИБ: объем спроса на нем не соответствует темпам роста предложения. Несмотря на стабильный рост рынка ИБ, усилия вендоров и поставщиков, обилие отраслевых мероприятий и насыщенность информационного поля сообщениями на тему защиты данных, проблемы информационной безопасности остаются неосознанными во многих российских компаниях.

Цель опроса Zecurion Analytics — составить общую картину организации ИБ в российских компаниях. В задачи исследования не входило выявление причинно-следственных связей, однако многие выводы о взаимозависимости различных аспектов ИБ напрашиваются сами собой. Так, например, из результатов опроса становится ясно, что специальные меры по защите информации принимаются преимущественно в тех компаниях, которые имеют в своем составе подразделения по информационной безопасности. В 93 % таких организаций есть положение о конфиденциальной информации, а DLP-системы есть в 43 % этих компаний против 9% организаций, не имеющих в штате ИБ-специалистов.

Более трети компаний возлагают задачи по защите информации на сотрудников ИТ-отделов. Эта практика является распространенной, особенно в компаниях малого и среднего размера. Очевидно, что руководство считает целесообразным экономить на специалистах и специализированных системах защиты, недооценивая вероятный ущерб от возможных утечек информации или взлома информационной сети.

Защита информации ожидаемо лучше организована в компаниях крупного бизнеса. В этом же сегменте чаще всего применяются DLP-системы. Однако результаты опроса демонстрируют активный рост интереса к защите информации со стороны сектора SMB: уже сейчас DLP есть в 17 % компаний малого бизнеса, и еще 17 % таковых планируют внедрение систем защиты от утечек в ближайший год. Неудовлетворенный спрос SMB на DLP-решения, обсуждаемый в ИБ-отрасли не первый год, пока остается «непаханым полем» в ожидании предложения, адекватного возможностям и потребностям небольших компаний.

Среди типов конфиденциальной информации самыми защищенными оказались персональные данные клиентов, что заставляет в очередной раз задуматься о неоднозначной роли регулирования в области информационной безопасности. С одной стороны, закон 152-ФЗ «О персональных данных» заставил многих впервые предпринять какие-либо меры по защите конфиденциальной информации. С другой — качество соответствующего законодательства дает необозримый простор для спекуляций поставщиков и интеграторов. В результате многие операторы персданных сосредоточились на задачах соответствия требованиям регуляторов, не уделяя должного внимания реальным потребностям ИБ. Так, внутренняя конфиденциальная информация, кража которой несет в себе гораздо более серьезные риски, в большинстве компаний защищается в последнюю очередь.

Ситуация вокруг информационной безопасности в российских компаниях имеет тенденцию к улучшению, однако демонстрирует явные проблемы, вызванные как историческим ходом развития рынка, так и вновь возникающими сторонними факторами. Мы надеемся, что подготовленные Zecurion Analytics данные заставят задуматься об очевидных и скрытых проблемах организации ИБ руководителей бизнеса, а также покажут производителям, поставщикам и экспертам по ИБ на тревожные тенденции рынка, требующие их вмешательства.

Методология

Данные исследования основаны на результатах опроса, проведенного Службой исследований HeadHunter с помощью собственных инструментов сегментации и анализа. Целевую аудиторию опроса составили руководители подразделений по информационным технологиям компаний всех отраслей. Всего в исследовании были обработаны ответы 192 респондентов. Приведенные данные взяты только со слов опрошенных специалистов и могут содержать погрешность, связанную с субъективным восприятием вопросов респондентами.

Результаты опроса были обработаны и представлены в настоящем исследовании Аналитическим центром Zecurion Analytics. Ответы опрошенных сотрудников были сгруппированы в трех тематических разделах. Первый раздел посвящен организации информационной безопасности в компаниях и содержит сведения о кадровой структуре, разделении полномочий и документальной регламентации ИБ. Второй раздел содержит сведения о защите от утечек информации в российских компаниях, применяемых средствах и защищаемых каналах.

Суммарные показатели по некоторым вопросам были также разделены по дополнительному критерию — размеру компаний, в которых работают опрошенные сотрудники. Это позволило составить отдельные картины о защите информации в малом, среднем и крупном бизнесе. Результаты такой группировки представлены в третьем разделе.

Представленным результатам исследования дали свою оценку независимые эксперты рынка информационной безопасности: Сергей Гордейчик (Positive Technologies), Илья Шабанов (Anti-Malware) и Алексей Лукацкий (Cisco). Комментарии экспертов представлены в конце каждой главы, содержат субъективные экспертные оценки, могут не совпадать друг с другом или с позицией авторов исследования.

Организация ИБ в российских компаниях

Организационные показатели — структурные, кадровые, документальные — служат практически прямым отражением озабоченности компании вопросами информационной безопасности. Так, например, наличие в компании специализированного подразделения по защите информации позволяет говорить о том, что задачи ИБ серьезно осознаются на высшем уровне руководства и воплощаются в реальных действиях по защите информации. При этом, однако, в российских компаниях распространена и часто оправдана практика реализации задач ИБ силами сотрудников ИТ-отдела и, реже, других подразделений. Такая ситуация подразумевает под собой два варианта: либо масштаб компании и объем защищаемых данных достаточно невелик для защиты средствами, которые может обслуживать сотрудник без ИБ-квалификации, либо руководство недооценивает значение информационной безопасности.

Как видно на диаграмме 1, половину российских компаний (51 %) можно отнести к первой категории «ИБ-ответственных» — в их составе есть специализированные подразделения по защите информации. Причем в большинстве случаев такое подразделение включает несколько сотрудников: от 2 до 5 (43 %) и даже более 5 человек (28 %). В 13 % компаний, имеющих отделы по защите информации, за ИБ отвечает лишь один сотрудник (см. диаграмму 2).

44 % опрошенных заявили, что в их компаниях нет подразделений по информационной безопасности, при этом лишь 2 % компаний готовы в ближайший год нанять специальных сотрудников для реализации ИБ-задач (см. диаграмму 1).

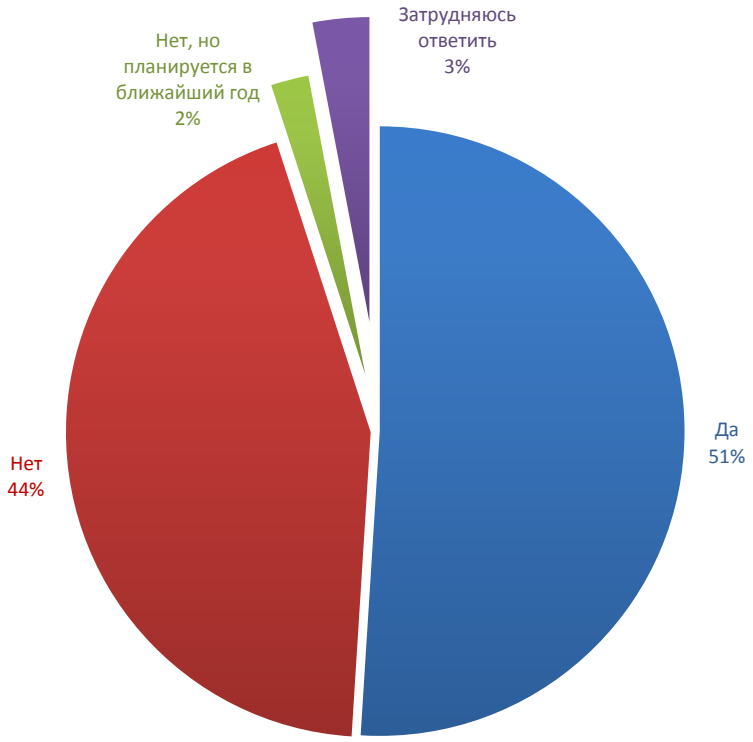

Диаграмма 1. Есть ли у Вас в компании специализированное подразделение по защите информации?

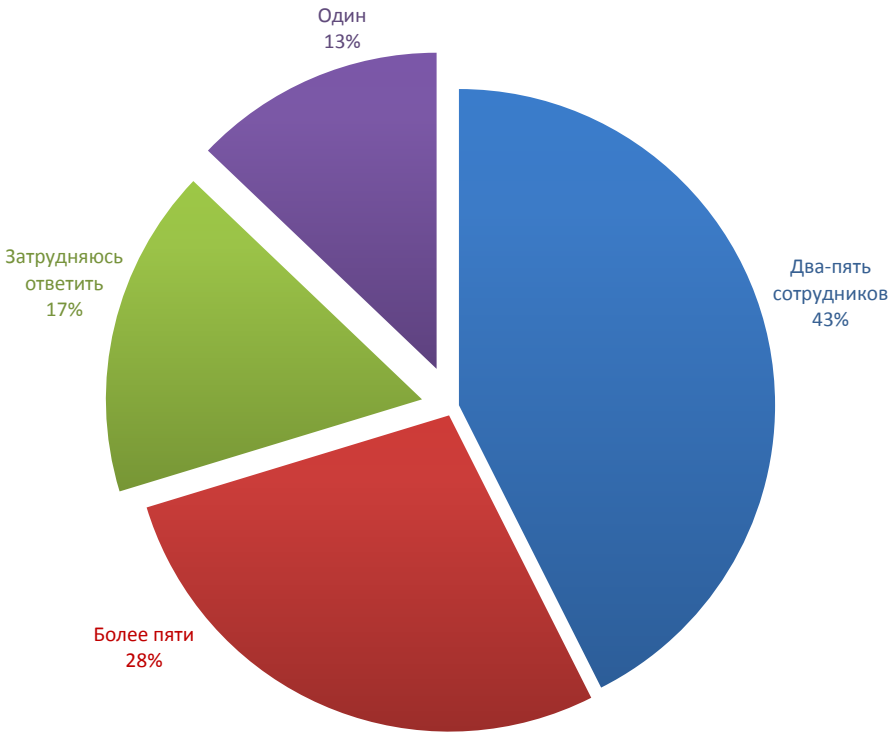

Диаграмма 2. Сколько сотрудников работают в этом подразделении?

Сергей ГОРДЕЙЧИК

Технический директор Positive Technologies

Структура подразделений, отвечающих за ИБ, в большой степени зависит от размера компании, степени зрелости и зависимости бизнеса от информационных технологий. Например, в холдинговых структурах при наличии централизованной политики информационной безопасности задачи ИБ могут координироваться в компании одним человеком, менеджером по ИБ, который использует ресурсы разных подразделений для выполнения своих задач. В этом случае важным моментом является наличие у менеджера по ИБ необходимых полномочий, что обычно реализуется путем назначения одного из топ-менеджеров компании куратором, отвечающим за проектную и операционную деятельность в этой области. Но вне зависимости от организации, наличие специалистов, имеющих знания и навыки обеспечения реальной защищенности является необходимым условием для эффективной защиты бизнеса.

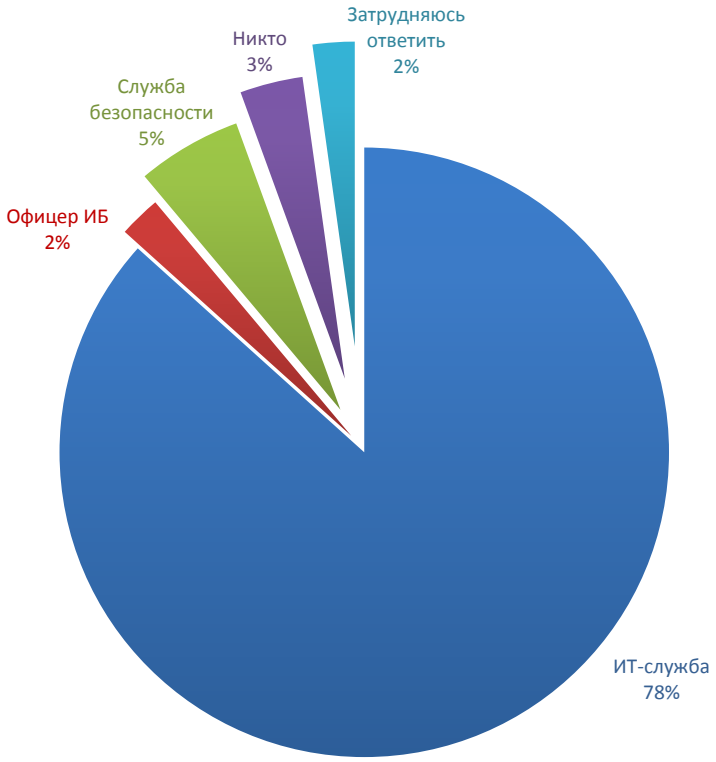

Диаграмма 3. Кто в Вашей компании отвечает за защиту информации? (Если нет специального подразделения по ИБ.)

В 85 % компаний, не имеющих специализированных подразделений по защите информации, вопросы информационной безопасности всё же решают сотрудники других отделов. В подавляющем большинстве случаев (78 %) эту функцию выполняет ИТ-служба, еще в 2 % — отдельный ИБ-специалист (см. диаграмму 3). Очевидно, ИТ-специалисты обладают более широкими компетенциями в вопросах технического обеспечения информационной безопасности, чем сотрудники других отделов. Однако следует понимать, что респонденты могут понимать под защитой информации как специальные системы, так и такие базовые меры, как установка фаервола и антивируса, доступные любому квалифицированному системному администратору.

Илья ШАБАНОВ
Управляющий партнер Anti-Malware.ru

Далеко не во всех компаниях пришли к пониманию необходимости серьезно заниматься вопросами защиты информации. Многие по-прежнему не до конца осознают критичность для бизнеса, например, утечки конфиденциальных данных, включая персональные данные сотрудников или клиентов. В таких компаниях вопросами ИБ занимается ИТ-департамент, чья работа в этом направлении ограничивается в лучшем случае установкой и настройкой необходимого набора программ и аппаратных устройств (антивируса, фаервола, антиспам, VPN и т. д.).

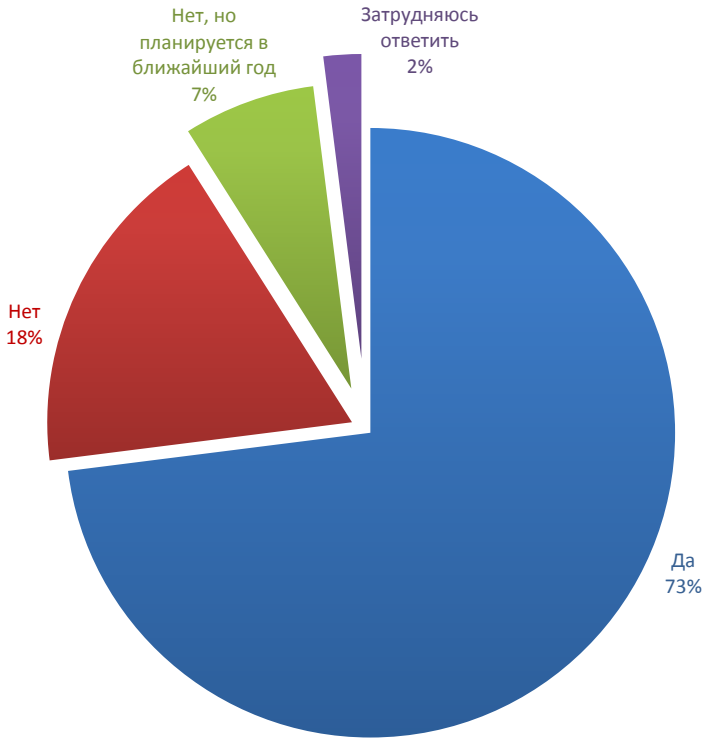

Диаграмма 4. Есть ли в Вашей организации положения о защите конфиденциальной информации?

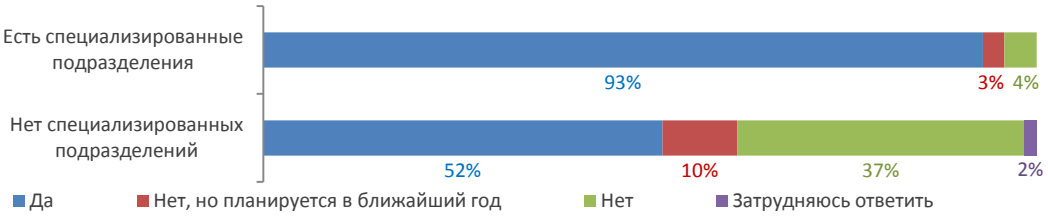

Диаграмма 5. Есть ли в Вашей организации положения о защите конфиденциальной информации?

В большинстве компаний (73 %) правила защиты конфиденциальной информации документированы в специальных положениях (см. диаграмму 4). Причем такие положения существуют или будут создаваться в ближайшее время практически во всех компаниях, где есть специализированные подразделения по информационной безопасности (см. диаграмму 5). Создание политик и правил работы с конфиденциальными данными, как правило, входит в основные обязанности ИБ-специалистов. Однако положения о конфиденциальной информации создаются не только по инициативе ИБ-отделов: более половины опрошенных работников (52 %), чьи компании не имеют специализированного подразделения, отмечают, что положения по защите информации тем не менее существуют.

Такие документы могут регламентировать отдельные участки работы с конфиденциальными данными, но при этом не иметь отношения к технической защите информации. Например, положение о неразглашении коммерческой тайны чаще всего подписывается сотрудниками вместе с трудовым договором и остается в ведении HR-отдела или службы безопасности.

Защита от утечек

Согласно результатам опроса, в 28 % компаний для защиты от утечек информации используются DLP-системы (см. диаграмму 6). Несмотря на оптимистичность этой цифры, еще более примечательными выглядят планы опрошенных: 9 % из них готовы внедрить DLP в следующем году. Следует отметить, что DLP-системы встречаются заметно чаще в организациях, имеющих отдел ИБ: 43 % против 9 % компаний, не имеющих подразделений по защите информации (см. диаграмму 7). С одной стороны, это говорит о высокой роли «безопасников» в выборе и продвижении внутри компании специализированных средств защиты. С другой — свидетельствует об определенном необходимом уровне квалификации персонала, обслуживающего систему: хотя сотрудники ИТ и других отделов, отвечающие за ИБ, и знают о существовании DLP-систем, брать на себя ответственность по их внедрению и обслуживанию они не решаются. Напротив, среди сотрудников компаний, в которых отдел ИБ есть, 33 % опрошенных затруднились определить наличие в их информационной системе DLP. Скорее это указывает не на их неосведомленность, а на распространенную вопреки усилиям вендоров проблему неоднозначной трактовки термина DLP и размытости границ продуктов этого класса.

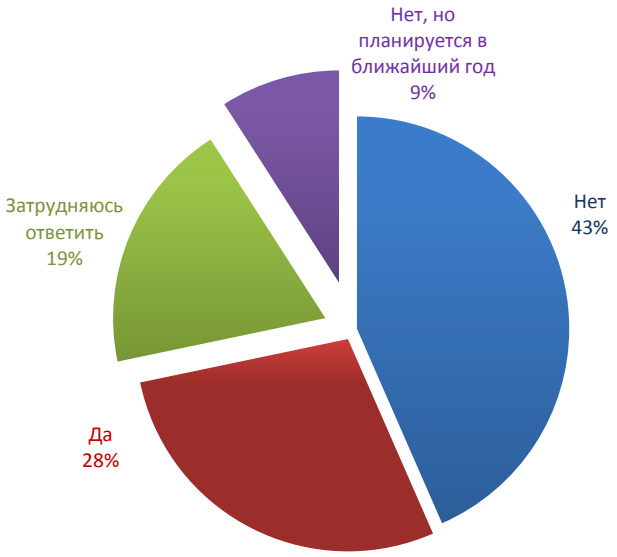

Диаграмма 6. Используются ли в Вашей организации специализированные DLP-системы для защиты от утечек информации?

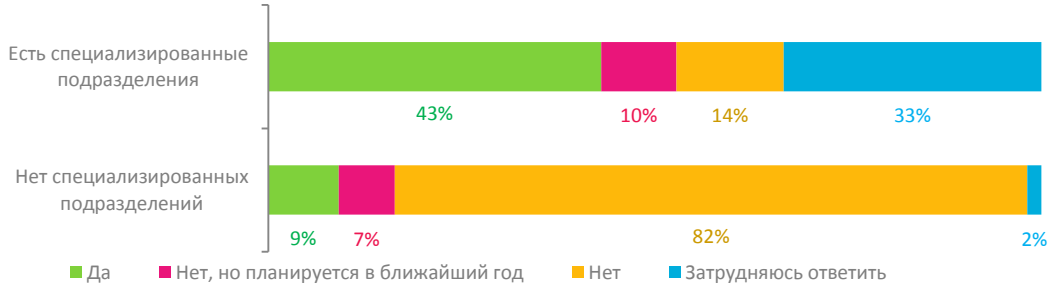

Диаграмма 7. Используются ли Вашей организации специализированные DLP-системы для защиты от утечек информации?

Илья ШАБАНОВ
Управляющий партнер Anti-Malware.ru

Цифры проникновения DLP-систем на рынке следует трактовать с осторожностью. Дело в том, что зачастую понятие DLP сильно размыто и трактуется недобросовестными производителями в выгодном для себя варианте. Таким образом, к DLP-системам очень часто относят банальный контроль внешних устройств или системы мониторинга действий сотрудников на рабочем месте, что категорически неверно. Но если смотреть на относительные показатели, то очень радует большой процент тех, кто планирует внедрять у себя на предприятии DLP-системы в том или ином виде.

В списке защищаемых данных с большим отрывом лидируют персональные данные — их защищают в 68 % компаний (см. диаграмму 8). Более половины (57 %) работников утверждают, что в их компаниях защищают критически важные базы данных, в первую очередь списки клиентов и поставщиков. Таким образом, наибольшее внимание в российских компаниях уделяют защите информации, относящейся к внешним агентам. Компрометация такой информация приводит к прямым убыткам из-за потери клиентов, необходимости возмещать ущерб пострадавшим и платить штрафы за несоблюдение законодательства, регулирующего защиту персональных данных.

Внутренняя информация компаний: схемы бизнес-процессов, интеллектуальная собственность, стратегические планы — защищаются значительно реже. Информация об архитектуре информационной сети находится под защитой всего в 32 % компаний, несмотря на то что только этой информации может быть достаточно, чтобы злоумышленник извне проник в корпоративную сеть и получил доступ к любой нужной ему конфиденциальной информации.

Диаграмма 8. Какая информация защищается в первую очередь?

Основной канал, который подвергается контролю, — корпоративная электронная почта — об этом заявили 70 % респондентов (см. диаграмму 9). В 56 % компаний защищаются данные при хранении на серверах, рабочих станциях, в ЦОДах. Более половины опрошенных (55 %) также заявили, что в их компаниях контролируется использование сотрудниками интернет-ресурсов: сервисов веб-почты, социальных сетей, блогов и других веб-сайтов. Однако при этом переписка в IM-программах контролируется заметно реже — только в 45 % случаев. Использование сотрудниками USB-накопителей и других съемных устройств контролируется почти в половине компаний (48 %), а печать на корпоративных принтерах — в 33 % случаев.

Диаграмма 9. Какие каналы утечки контролируются?

Алексей ЛУКАЦКИЙ

Бизнес-консультант Cisco

Лидерство персональных данных говорит не о важности этой темы и не о размерах убытков от нарушения законодательства. Скорее это результат спекуляций на тему Федерального Закона «О персональных данных», который не сходит с повестки дня специализированных СМИ и конференций, и постоянного подливания масла в огонь производителями средств защиты, консультантами и интеграторами, а также регуляторами. Реального ущерба субъектам от утечки их персональных данных практически не происходит. Да и новой тему защиты персданных не назовешь — она возникла не вчера, и абсолютное большинство компаний ее давно и успешно решили.

Гораздо интереснее другие цифры: наиболее важная для злоумышленников информация (бизнес-планы, ноу-хау, маркетинговая информация и т. д.) реже подлежит защите. И причина тут кроется в технократичности служб ИБ. Они зачастую не знают, что надо защищать на самом деле, а если знают, то не осведомлены о том, где эта информация хранится. И даже если они осведомлены об этом, то у них отсутствуют технические решения для контроля этой информации. Это классическая проблема оторванности служб ИБ от бизнеса и его реальных потребностей.

Эту же проблему отражает и диаграмма 9, согласно которой службы ИБ защищают не те каналы, которые обрабатывают конфиденциальные данные (базы данных, видеоконференции, голосовые соединения, технологии взаимодействия Web 2.0 и т. д.), а те, для которых существуют коробочные продукты, которые легко купить и так же легко проинсталлировать.

Защита данных в компаниях малого, среднего и крупного бизнеса

Ситуация с организацией информационной безопасности в компаниях малого, среднего и крупного бизнеса ожидаемо существенно различается. На вопросы о наличии подразделения ИБ, положений о конфиденциальной информации и специализированных DLP-систем наибольшее число положительных ответов поступило от сотрудников крупных организаций (см. таблицы 1, 2, 3). Тем не менее, полученные показатели далеки от 100 %: при общей численности штата более 500 сотрудников в 29 % крупных организаций отдела по защите информации нет.

Чуть меньшую организованность в вопросах ИБ показали предприятия численностью от 250 до 500 человек, в разных странах классифицируемые как средний или крупный бизнес. Специализированные подразделения по ИБ есть в 52 %, а положения о конфиденциальной информации — в 65 % таких компаний. Регламентировать защиту информации планируют в ближайший год во многих компаниях вне зависимости от размера (10 % компаний до 500 сотрудников и 4 % крупных компаний).

Что касается использования для защиты от утечек специализированных решений, то в этом вопросе малый бизнес демонстрирует неожиданное оживление интереса к DLP-системам. Хотя на сегодняшний момент DLP функционирует только в 17 % малых предприятий, еще столько же планируют внедрение DLP в следующем году. Если этот прогноз оправдается и число внедрений в небольших компаниях удвоится, то процент малого бизнеса, защищенного с помощью DLP, превысит аналогичную долю предприятий среднего бизнеса.

Таблица 1. Есть ли в Вашей организации специализированное подразделение по защите конфиденциальной информации?

	Да	Нет, но планируется в ближайший год	Нет	Затрудняюсь ответить
До 50 сотрудников	38 %	0 %	62 %	0 %
От 50 до 250 сотрудников	32 %	0 %	68 %	0 %
От 250 до 500 сотрудников	52 %	5 %	33 %	10 %
Более 500 сотрудников	67 %	4 %	25 %	4 %

Таблица 2. Есть ли в Вашей организации положения о защите конфиденциальной информации?

	Да	Нет, но планируется в ближайший год	Нет	Затрудняюсь ответить
До 50 сотрудников	52 %	10 %	38 %	0 %
От 50 до 250 сотрудников	65 %	10 %	25 %	0 %
От 250 до 500 сотрудников	76 %	10 %	14 %	0 %
Более 500 сотрудников	84 %	4 %	8 %	4 %

Таблиц 3. Используются ли в Вашей организации специализированные DLP-системы для защиты от утечек информации?

	Да	Нет, но планируется в ближайший год	Нет	Затрудняюсь ответить
До 50 сотрудников	17 %	17 %	66 %	0%
От 50 до 250 сотрудников	24 %	8 %	63 %	5 %
От 250 до 500 сотрудников	26 %	5 %	42 %	26 %
Более 500 сотрудников	39 %	8 %	22 %	31 %

Сергей ГОРДЕЙЧИК

Технический директор Positive Technologies

Желание малого бизнеса и сегмента SME использовать решения DLP для контроля конфиденциальной информации понятно. Как правило, такие компании не располагают ресурсами, необходимыми для построения многоуровневой системы защиты, разграничения доступа и контроля. В этом случае DLP может рассматриваться в качестве «серебряной пули», позволяющей обнаруживать и предотвращать серьезные инциденты. В крупных компаниях, как правило, используется комплекс организационных и технических средств защиты и DLP является лишь одним из эшелонов, позволяющих обнаруживать недостатки или сбои в работе других уровней обеспечения конфиденциальности информации.

Алексей ЛУКАЦКИЙ

Бизнес-консультант Cisco

В целом вывод о том, что малые предприятия меньше уделяют внимания своей информационной безопасности, верен. И это очевидно. Нехватка ресурсов не позволяет малому бизнесу тратить их на неявные и непрофильные процессы, к которым и относится информационная безопасность. Обычно малые предприятия стараются убить одним выстрелом двух зайцев: нанять специалистов, одновременно подкованных в области и ИТ, и ИБ, а также приобрести продукты, объединяющие в себе функционал и ИТ, и ИБ. Но вот к результатам, показанным в таблицах, у меня отношение скептическое. Я не верю, что на 38 % малых предприятий с числом сотрудников менее 50 человек существует отдельное подразделение по информационной безопасности. Также как и не верю в наличие на таких предприятиях отдельного положения по защите конфиденциальной информации. Скорее всего, респонденты имели ввиду какие-нибудь рамочные соглашения или даже отдельные разделы/пункты в трудовых договорах со своими сотрудниками.

Илья ШАБАНОВ

Управляющий партнер Anti-Malware.ru

Реально возможность содержать отдел ИБ и всерьез заниматься защитой конфиденциальной информации обратно пропорциональна размеру бизнеса компании. Небольшая компания едва ли может позволить себе выделенного на эту область специалиста. Поэтому высокий процент ответивших, что имеет специальное подразделение для таких целей, вызывает большие сомнения. Скорее всего, респонденты выдавали желаемое за действительное или попросту не знали реальную ситуацию на предприятии. С другой стороны, данные по проникновению DLP-систем в зависимости от размера компании выглядят, на мой взгляд, вполне достоверно.

Очень интересен факт наличия неудовлетворенного спроса на DLP-системы в сегменте малого бизнеса, т. е. количество тех, кто заинтересован во внедрении таких систем. По сути, этот сегмент рынка ждет адекватного предложения, как по стоимости, так и составу нужной для них функциональности.

Выводы

- Организация информационной безопасности в российских компаниях остается на среднем уровне и не демонстрирует явной тенденции к значительному улучшению в ближайшем будущем.
- Отделы или сотрудники, специализирующиеся на информационной безопасности, есть примерно в половине компаний, большинство которых относятся к крупному бизнесу. Отделы по ИБ как правило достаточно многочисленны и в четверти случаев включают более 5 человек.
- Во многих компаниях принята практика совмещения полномочий по поддержке информационных систем и защите информации сотрудниками ИТ-отделов.
- Положение о защите конфиденциальной информации есть в подавляющем большинстве компаний, в которых информационной безопасностью занимаются отдельные специалисты.
- Использование DLP-систем для защиты информации довольно распространено в российских компаниях пропорционально их размеру и демонстрирует тенденцию к росту в следующем году на 9%. Особенно заметно созревание интереса к внедрению DLP-решений в среде малого бизнеса.
- Выбор защищаемых данных проводится под влиянием внешних факторов (регуляторов и поставщиков), а не в соответствии с реальными рисками и потребностями бизнеса. Поэтому в первую очередь защищаются персональные данные и списки клиентов, а в последнюю — внутренняя конфиденциальная информация компании.
- Контроль каналов распределяется примерно равномерно между сетевым трафиком, съемными устройствами и местами хранения информации. Однако чаще всего контролю подвергается корпоративная электронная почта.

Александр КОВАЛЕВ

Директор по маркетингу Zecurion

Мы как разработчики DLP с осторожностью относимся к цифрам, касающимся систем защиты от утечек. Действительно, как сказал Илья, под DLP часто понимают не полноценные системы защиты от утечек, а отдельные их части или вовсе использование каких-то базовых политик ИБ. Например, иногда приходится слышать от руководителей ИТ-отделов: «Мы защищаемся от утечек — у нас на межсетевом экране запрещены „Одноклассники" и почта Mail.Ru». Конечно, и так можно частично снизить риски, но лишь в какой-то степени.

Отсутствие широкого распространения DLP-систем является следствием кадровой ситуации: в большей части компаний нет достаточного штата ИБ-специалистов или вовсе функции обеспечения безопасности перекладываются на сотрудников по ИТ. Очевидно, что для полноценного использования DLP, например, составления отчётов по действиям подозрительных сотрудников на основе данных архива трафика и печати, требуются определённые человеческие ресурсы. В итоге в условиях нехватки человеческих ресурсов, к сожалению, не всегда внедрённая DLP-система реально работает хотя бы на 25 % своих возможностей.

Всё это позволяет предположить, что в ближайшее время большим спросом будут пользоваться DLP-системы «на потребу», то есть требующие минимального участия человека в процессе защиты от утечек и просто обслуживании самого софта. Пока их появлению мешает даже не сложность реализации «коробочных DLP», к которым уже можно отнести некоторые продукты на рынке, а отсутствие полноценной нормативной базы. Дело в том что, если говорить о минимальном участии специалистов ИБ, когда система должна принимать большую часть решений сама, необходимо как-то определить базовые, стандартные настройки. Если на Западе в общем-то существует сравнительно неплохое законодательство и часто указывается, какую информацию, в каких случаях и от чего защищать, то у нас, наоборот, больше описываются требования к процессам контроля, причём часто на уровне 20-летней давности. В такой ситуации трудно создать действительно коробочный продукт с универсальными правилами, именно это, по нашему мнению, и сдерживает реальный рост внедрений в SMB-секторе.

Эксперты

Сергей ГОРДЕЙЧИК

Технический директор Positive Technologies

Основными направлениями деятельности Сергея являются развитие системы контроля защищенности и соответствия стандартам MaxPatrol, внедрение процессов контроля соответствия стандартам информационной безопасности, руководство крупнейшей в России группой профессиональных этических хакеров. Кроме основной деятельности, Сергей разрабатывает и преподает курсы по информационной безопасности, среди которых «Безопасность беспроводных сетей», «Анализ и оценка защищенности Web-приложений».

Сергей опубликовал несколько десятков статей в отраслевых изданиях, автор книги «Безопасность беспроводных сетей», участник международного проекта Web Application Security Consortium (WASC), научный редактор специализированного портала SecurityLab.ru, популярный докладчик на отраслевых мероприятиях. Имеет профессиональные звания и сертификаты: MCSE, CWNA, MCT, MVP in Enterprise Security, CISSP.

Илья ШАБАНОВ

Управляющий партнер Anti-Malware.ru

Окончил Московский Физико-Технический Институт (МФТИ). С 2000 года работает в области интернет-технологий, информационной безопасности и маркетинга. В 2005 году основал портал Anti-Malware.ru, занимает должность Управляющего партнера. С 2010 года входит в административный совет портала VirusInfo.info.

Сфера компетенции и экспертных знаний включает широкий спектр задач от аналитики и стратегического маркетинга до информационной безопасности и антивирусных исследований. В 2007—2010 годах удостаивался награды «Microsoft Most Valuable Professional in Windows Security» как один из наиболее влиятельных независимых экспертов по информационной безопасности. Автор многих публикаций и тестов на Anti-Malware.ru.

Алексей ЛУКАЦКИЙ

Бизнес-консультант Cisco

Окончил Московский институт радиотехники, электроники и автоматики (МИРЭА) по специальности «Прикладная математика» (специализация – «Защита информации»). В области информационной безопасности работает с 1992 года. Прошёл путь, начиная от программиста средств шифрования и администратора и заканчивая аналитиком и менеджером по развитию бизнеса в области информационной безопасности.

Опубликовал около 400 печатных работ в различных изданиях: «Информкурьерсвязь», «CIO», «Национальный банковский журнал», «ПРАЙМ-ТАСС», «Information Security», «CNews», «LAN Magazine», «Системы безопасности, связи и телекоммуникаций», «PCWeek/RE», «Банковские системы», «Аналитический банковский журнал», «Business Online», «Мир связи. Connect» и т.д.

В 2005 году был удостоен награды Ассоциации документальной электросвязи «За развитие инфокоммуникаций в России», а в 2006 — награды Инфофорума в номинации «Публикация года». В январе 2007 года Алексей Лукацкий был включён в рейтинг 100 персон российского ИТ-рынка.

Авторы исследования

Аналитический центр компании Zecurion

Zecurion (до ребрендинга 2012 года — SECURIT) — ведущий разработчик систем защиты информации от внутренних угроз. Продукты компании позволяют минимизировать риски умышленной и случайной утечки корпоративной информации.

Компания Zecurion 10 лет профессионально занимается вопросами информационной безопасности. С 2001 года Zecurion является лидером в области шифрования данных, а с 2006 года разрабатывает инновационные DLP-решения для защиты от утечек информации. Среди современных продуктов, представленных на рынке DLP, решения Zecurion признаны самыми технологичными (по версии аналитического центра Anti-Malware.ru).

Линейка продуктов Zecurion реализует полный спектр защиты информации от инсайдеров: контроль всех потенциальных каналов утечки, ведение архива действий сотрудников, защиту данных в процессе использования и хранения, а также управление доступом пользователей к корпоративной сети, приложениям и конфиденциальной информации. Использование DLP-решений компании обеспечивает комплексную защиту информации от утечек на протяжении всего ее жизненного цикла — от создания до записи в архив или удаления.

Служба исследований компании HeadHunter

Группа компаний HeadHunter (hh.ru) работает на рынке интернет-рекрутмента с 2000 года. На данный момент сайт hh.ru является одним из лучших онлайновых ресурсов для поиска работы и найма персонала. Бизнес-модель HeadHunter построена на продаже информации из базы данных резюме. Стратегия компании — инвестиции в новые технологии и постоянное совершенствование нашего сервиса.

Служба исследований HeadHunter проводит более 100 исследований в год, анализируя различные аспекты рынка труда. Результаты отчетов строятся как на собственных статистических данных, так и на опросах пользователей.

Контактная информация

Zecurion

109316 Российская Федерация, Москва
Волгоградский просп., дом 42 корпус 8
Телефон: +7 (495) 221-21-60
market@zecurion.ru
www.zecurion.ru

HeadHunter

129085 Российская Федерация, Москва
ул. Годовикова, дом 9, стр. 10
Телефон: +7 (495) 974-64-27
pr@hh.ru
www.hh.ru