Евгений Преображенский,
генеральный директор, компания Perimetrix

ИНСАЙДЕР: ВАРИАНТ С ЗАКЛЕИВАНИЕМ USB-ПОРТА НЕ ПОМОЖЕТ

Ни для кого не секрет, что информация сейчас занимает первое место в конкурентной борьбе, и соответственно, утечка информации за пределы компании может нанести непоправимый ущерб ее репутации и финансовому положению. Понятие «инсайдер» в различных источниках имеет разную трактовку. Давайте разберемся: кто же такой «инсайдер»? Какие ситуации не подпадают под определение «угрозы инсайдеров»?

— Классическое определение этого термина трактует инсайдера, как члена ограниченного круга людей, имеющих доступ к закрытой информации. Дальнейшие смысловые поиски размывают это понятие и трактуют по-разному не только с учетом функциональной специфики, но и эмоционального оттенка. Например, с точки зрения регуляторов финансового рынка, инсайдер — злоумышленник, использующий свои знания об эмитентах ценных бумаг для игры на фондовой бирже. Правоохранительные органы считают инсайдером отважного оперативника или агента, внедренного в преступные круги для сбора доказательной базы. В быту — это человек, который знает больше, чем знают все, к мнению которого нужно прислушиваться.

Представьте себе, что в сказке Петра Ершова про Конька-Горбунка это самое мифическое создание было не кем иным, как Ивановым инсайдером.

Впрочем, вернемся к существу вопроса.

Для специалистов по информационной безопасности, которых мы имеем честь представлять на страницах этого уважаемого издания, инсайдер — сотрудник компании, имеющий доступ к конфиденциальным данным, размещенным в компьютерной сети предприятия. Причем под это определение может попасть как секретарша, по ошибке переславшая «не то и не туда», так и злоумышленник, внедренный специально для кражи данных. Определение упрощенное, но оно позволяет понять природу явления с точки зрения защиты информации.

ИНСАЙДЕР – СОТРУДНИК КОМПАНИИ, ИМЕЮЩИЙ ДОСТУП К КОНФИДЕНЦИАЛЬНЫМ ДАННЫМ

Какую корректировку внесла российская действительность в данное определение?

— Перефразирую слова известной поговорки: «Инсайдер — он и в Африке инсайдер». Действительно, недостатки человеческой натуры качественно не меняются в зависимости от места проживания. Редко кто сможет устоять перед соблазном заработать на эксклюзивном доступе к данным. И, наоборот, ошибку может совершить и швед, и русский, и якут.

Правда, все же не стоит недооценивать силу российской действительности. Она наложила свой отпечаток хоть и не на определение инсайдеров, но на их деятельность. Например, у нас значительно чаще уволенные сотрудники забирают с собой оперативную рабочую информацию — контакты, сведения о бизнес-планах, персональные данные, финансовые отчеты. В России предприятия меньше знают о такого рода инцидентах, а узнав, стараются «замять», дабы не выносить сор из избы. Впрочем, корни такой ситуации не в национальной черте, а, скорее, в ощущении безнаказанности. Например, наши исследования показывают, что в отечественных компаниях судебное преследование грозит лишь 9% злонамеренных инсайдеров. Для сравнения: в США всех внутренних нарушителей такого типа рано или поздно постигнет крупный штраф и/или тюремное заключение.

В чем опасность инсайдеров?

— Эта пятая колонна может доставить предприятию целый спектр неприятностей. Давайте опустим порчу нервных клеток, переживания, срыв сделок, ущерб репутации и т.п. Это, все же бо-

лее-менее восполнимые ресурсы. Их главная опасность в другом — прямой угрозе бизнесу. Трактуя опасность на межгосударственном уровне, можно утверждать, что инсайдеры угрожают даже национальной безопасности.

РЕДКО КТО СМОЖЕТ УСТОЯТЬ ПЕРЕД СОБЛАЗНОМ ЗАРАБОТАТЬ НА ЭКСКЛЮЗИВНОМ ДОСТУПЕ К ДАННЫМ

Известна формула, согласно которой утечка всего 20% корпоративных секретов в 60% случаев приводит фирму к банкротству. Например, летом 2005 г. американский процессинговый центр CardSystems Solutions допустил утечку номеров 40 млн. кредитных карт. В течение месяца от работы с ним отказались крупнейшие клиенты, государство наложило крупный штраф, а в декабре бывшая преуспевающая компания была куплена за символическую цену небольшим конкурентом. При этом практика имеет много подтверждений того, что 20% — это даже много.

Каков психологический портрет инсайдера?

— Логичный вопрос. Для успешной борьбы нужно, прежде всего, знать врага в лицо.

Существует несколько подходов к классификации внутренних нарушителей. Компания Perimetrix придерживается следующего: экосистема инсайдеров имеет четыре уровня: «граждане», «нарушители», «отступники», «предатели».

Верхний уровень составляют «граждане» — лояльные служащие, которые очень редко (если вообще когда-нибудь) нарушают корпоративные политики и в основном не являются угрозой безопасности. Чуть ниже находятся «нарушители», составляющие большую часть «населения» корпорации. Эти сотрудники позволяют себе небольшие фамильярности, работают с персональной веб-почтой, играют в компьютерные игры и совершают онлайн-покупки. Представители данного слоя представляют угрозу ИТ-безопасности, но сопутствующие им инциденты являются случайными и неумышленными. На следующей ступени находятся «отступники» — работники, которые проводят большую часть дня, делая то, что они делать не должны. Эти служащие злоупотребляют своими привилегиями по доступу к Интернету, самовольно устанавливают и используют P2P-клиенты и IM-приложения. Более того, такие сотрудники могут отсылать конфиденциальную информацию компании внешним адресатам, заинтересованным в ней. Таким образом, «отступники» представляют серьезную угрозу ИТ-безопасности. Наконец, на самом нижнем уровне находятся «предатели». Это служащие, умышленно и регулярно подвергающие конфиденциальную информацию компании опасности. Обычно за финансовое вознаграждение от заинтересованной стороны. Такие сотрудники представляют самую опасную угрозу. Одновременно, их сложнее всего поймать.

Не вызывает сомнений, что корпоративная ИБ-стратегия должна учитывать опасность, исходящую от всех перечисленных типов. Например, кажущаяся невинность «граждан», наоборот, сегодня представляет собой главную угрозу: 80-90% всех зарегистрированных утечек данных были следствием неосторожности или безалаберности сотрудников. И лишь незначительная часть инцидентов была вызвана злонамеренными инсайдерами: «отступниками» и «предателями».

Какие предприятия особо чувствительны к инсайдерским атакам?

— Для ответа на этот вопрос необходимо понять, что же, собственно, интересует инсайдеров? Наши исследования показывают, что это персональные данные, финансовые отчеты, детали конкретных сделок, интеллектуальная собственность и бизнес-планы. Таким образом, «под колпаком», несомненно, находятся все отрасли. Однако угроза нарушения конфиденциальности данных растет пропорционально приближению организации к «живым» деньгам и персональным данным. В этой связи в зону повышенного риска попадают, прежде всего, банки, другие финансовые организации, телекоммуникационные операторы, крупный бизнес, основанный на многомиллиардных контрактах, государственные учреждения.

В ОТЕЧЕСТВЕННЫХ КОМПАНИЯХ СУДЕБНОЕ ПРЕСЛЕДОВАНИЕ ГРОЗИТ ЛИШЬ 9% ЗЛОНАМЕРЕННЫХ ИНСАЙДЕРОВ

Впрочем, нельзя недооценивать опасность и для среднего и малого бизнеса. Скажем, вынос перешедшим к конкуренту сотрудником списка клиентов небольшого дистрибутора будет означать, минимум, многократное снижение продаж, а максимум — банкротство организации.

Резюмируя, можно уверенно сказать, что проблема защиты данных от внутренних нарушителей — это проблема универсаль-

ная с точки зрения географии, размера бизнеса и его отраслевой специфики.

По мировой статистике, утечка всего 20% коммерческих секретов фирмы в 60% случаев приводит к банкротству. А как обстоят дела у нас?

— Действительно, еще одна национальная особенность инсайда. Прямой ответ на этот вопрос — никак. Высокая степень латентности подобных преступлений выносит на суд общественности лишь редкие и скудные новостные заметки. При этом, насколько мне известно, ни одну компанию ни разу в таких случаях не постигло банкротство.

УТЕЧКА ВСЕГО 20% КОРПОРАТИВНЫХ СЕКРЕТОВ В 60% СЛУЧАЕВ ПРИВОДИТ ФИРМУ К БАНКРОТСТВУ

По данным американского центра исследований, относительно преступлений, связанных с хищениями персональных данных (Identity Theft Resource Center, ITRC), в прошлом году на территории США произошло, как минимум, 656 публичных утечек информации. Это значение на 47% превосходит показатели позапрошлого года и более чем в четыре раза — данные за 2005 год. Если темпы роста количества утечек сохранятся и в нынешнем году (а пока предпосылок к их снижению не наблюдается), то общее количество публичных инцидентов может приблизиться к психологической отметке в 1 000 случаев за год. И это только вершина айсберга: компаниям свойственно замалчивать утечки в надежде защитить публичный имидж, а некоторые просто не в состоянии учитывать утечки вовсе. Наши исследования показывают, что в 2008 г. 42% российских организаций затруднились назвать хотя бы приблизительное количество подобных инцидентов.

На данный момент существуют две основные группы причин, из-за которых компании скрывают информацию об инцидентах. Во-первых, это нежелание нести дополнительные расходы на ликвидацию последствий утечек, оповещение пострадавших и возмещение понесенного ими ущерба. Зачастую организации полагаются «на авось», считая, что утечку никто не заметит. При этом они неизбежно испытывают риски, связанные с возможными последствиями инцидента.

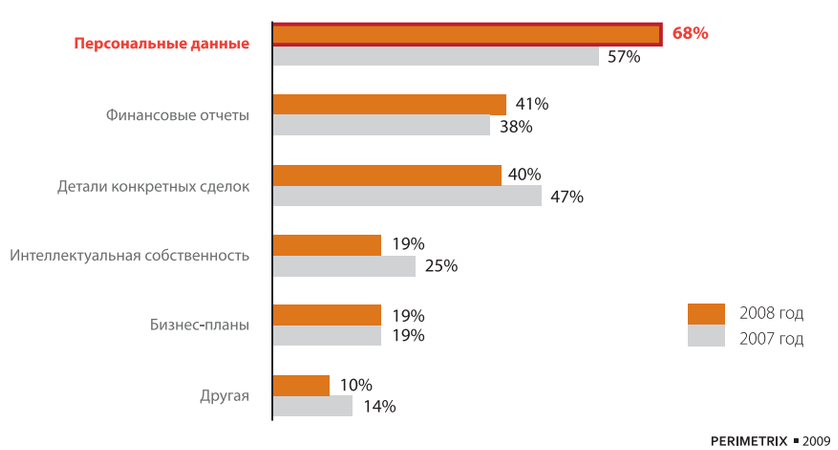
Однако еще большую важность имеет вторая группа причин, смысл которой заключается в том, что информация о случившихся инцидентах часто не доходит до руководства. Всего лишь одна потерянная флешка или письмо, отправленное по чужому адресу, может привести компанию к невосполнимым финансовым потерям. При этом персонал по безопасности и ИТ часто просто игнорирует такого рода инциденты, опасаясь санкций со стороны начальства или просто не принимая их всерьез. Кроме инцидентов, которые хоть как-то обнаруживаются внутри компаний, существуют еще и утечки-фантомы, о которых никто ничего не знает. Доля таких утечек особенно велика для внутренних инцидентов по безопасности, поскольку далеко не все компании имеют средства для выявления данных проблем.

Для понимания масштаба потерь приведем оценку ущерба от публичных утечек персональных данных только для США: эта сумма составляет астрономические $24 млрд. за 2008 г. При этом учитываются только публичные утечки, только этого специфического типа данных и только в США. Общий же ущерб мировой экономики может составлять $1-1,2 трлн.

Какая информация чаще всего «утекает» из российских компаний?

— По нашей статистике, инсайдеров больше всего интересуют персональные данные: 68% респондентов исследования «Инсайдерские угрозы в России 2009» указали, что именно этот тип информации становится объектом нездорового внимания сотрудников. Весьма показательно, что по сравнению с прошлым годом мы зафиксировали 11% (sic!) рост

Информация, наиболее подверженная утечке
(можно выбрать до двух вариантов)



показателя. Я далек от мысли, что персональные данные приносят криминальным элементам больше прибыли, чем, скажем, детали финансовых отчетов, конкретных сделок, интеллектуальная собственность или бизнес-планы. Причина такого положения вещей, пожалуй, в степени защиты. К сожалению, несмотря на бурную законотворческую деятельность, российские предприятия еще очень далеки от практической реализации эффективной системы защиты персональных данных.

Для справки. По нашим подсчетам порядок работы с персональными данными в России регулируют более 30 законов (в том числе федеральных), указов, постановлений, приказов и распоряжений. Излишне говорить, что разобраться в этом нормативном буйстве очень сложно даже профессионалу. Тем более, приблизительно 7 миллионам юридических лиц и ИП, которые согласно ФЗ «О Персональных данных» оперируют ПД и обязаны соответствовать его требованиям.

Недавние новости на этом направлении подлили масла в огонь. 15.09 Правительство выпустило постановление № 687, которое вступило в противоречие со всеми ранее выпущенными нормативными актами. В частности, постановление определяло за оператором выбор средств защиты персональных данных и их реализацию.

Наконец, нельзя не обратить внимание и на количественные характеристики реализации ФЗ «О персональных данных». Из упомянутых 7 миллионов подзаконных лиц сегодня зарегистрировались операторами только… немногим больше 24 тыс. (sic!).

Какие каналы можно назвать наиболее опасными?

— В последние годы мы наблюдаем любопытную тенденцию. Занимавшая долгое время лидерские позиции в рейтинге самых опасных каналов утечки электронная почта сегодня сдала свои позиции. На первое место по популярности вышли мобильные накопители. Крошечные запоминающие устройства, способные вмещать десятки гигабайтов данных, объем, сравнимый с возможностями жестких дисков. Их вместимость, мобильность и простота подключения — главные причины распространения как оружия инсайдеров. С другой стороны, за электронной почтой на большинстве предприятий зорко наблюдает служба безопасности. Да и, прямо скажем, сложно таким образом переслать большой массив данных.

Действительно, мобильные накопители стали своего рода enfant terrible (несносный ребенок), постоянной головной болью владельцев бизнеса. И ведь не запретишь их — очень часто «флэшки» требуются по производственной необходимости. Что-то вроде кухонного ножа: с одной стороны — самое распространенное орудие бытовых убийств, а с другой — незаменимый помощник в хозяйстве. Так что вариант с заклеиванием USB-порта эпоксидным клеем здесь неуместен. Впрочем, сегодня уже есть широкий выбор специализированного ПО, способного предотвратить утечку программным способом, без таких экзотических средств.

80–90% ВСЕХ ЗАРЕГИСТРИРОВАННЫХ СЛУЧАЕВ УТЕЧЕК ДАННЫХ БЫЛИ СЛЕДСТВИЕМ НЕОСТОРОЖНОСТИ ИЛИ БЕЗАЛАБЕРНОСТИ СОТРУДНИКОВ

Финансирование вопросов безопасности. На чем нельзя экономить?

— В России средний уровень расходов на ИБ составляет всего лишь 3% (мировой показатель — 7%) от общего ИТ-бюджета, поэтому даже при сокращении расходов сэкономить не удастся. Более того, в условиях кризиса и массовой миграции сотрудников

Самые популярные каналы утечки
(можно выбрать до двух вариантов)

PERIMETRIX ■ 2009

между компаниями вопрос защиты конфиденциальности данных многократно возрастает. Естественно, что для повышения своей стоимости работник будет стремиться аккумулировать как можно

ВСЕГО ЛИШЬ ОДНА ПОТЕРЯННАЯ ФЛЕШКА ИЛИ ПИСЬМО, ОТПРАВЛЕННОЕ ПО ЧУЖОМУ АДРЕСУ, МОЖЕТ ПРИВЕСТИ КОМПАНИЮ К НЕВОСПОЛНИМЫМ ФИНАНСОВЫМ ПОТЕРЯМ

больше стратегической и тактической информации своего предыдущего работодателя.

В частности, обращу внимание на следующую цифру: 73,3% респондентов считают, что несмотря ни на какие кризисы ИБ является важнейшим приоритетом организации. В период кризиса значение ИБ даже возрастает.

Назовите самые популярные средства информационной безопасности (плюсы-минусы).

— Три кита, на которых покоится эффективная защита конфиденциальности данных — это комбинация технических, административных и организационных мер. Однако не стоит углубляться в технологический нарциссизм. Прежде всего, нужно понять, что и от чего необходимо защитить. Знание природы бизнеса предприятия, особенностей бизнес-процессов, а также того самого «врага» — самый важный шаг внедрения системы нейтрализации инсайдерской угрозы.

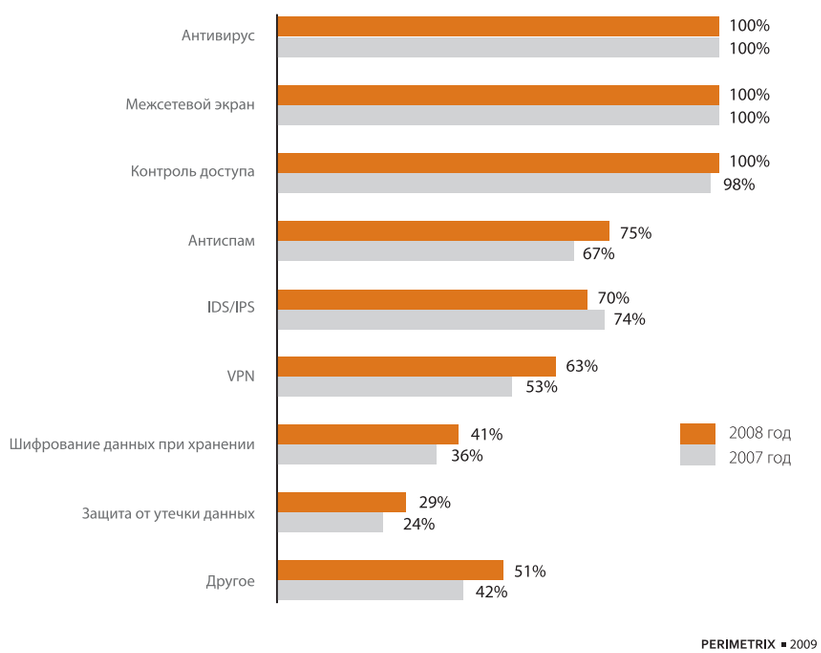
Традиционно защита была сферой компетенции ИБ/ИТ-служб, которые зачастую выступали инициаторами, внедренцами и эксплуатирующей инстанцией таких проектов. Это, в свою очередь, наложило на проекты сильный отпечаток технократического подхода, слабо увязывавшего защиту с бизнесом организации. С точки зрения эффективности защиты и инвестиций, необходимо отталкиваться не от контроля информационной инфраструктуры и сетей передачи данных, а от контроля только критических бизнес-процессов. В рамках каждого внедрения системы нужно проводить глубокий предварительный анализ, призванный определить наиболее критичные, с точки зрения безопасности, бизнес-сценарии.

Важно заметить, что в процессе практической реализации ИБ-стратегии компании питают слабость к точечным мерам, напоминающим пожаротушение. Например, «заткнуть» интернет-пейджеры или фильтровать электронную почту. Однако инсайд подобен газу под давлением — он всегда найдет выход через альтернативные каналы. Из этого следует очевидный вывод — защита от утечек может быть или всеобъемлющей, пронизывающей все бизнес-процессы и тесно интегрирующейся с КИС, или никакой. Стоит ли инвестировать в технологии, которые все равно не смогут решить проблему?

Замечу один важный недостаток. Склонность использовать технологию контентной фильтрации как фундамент защиты. Его смысл состоит в фильтрации потока сетевых данных и выявлении конфиденциальной информации на основе вероятностных методов. Его единственное достоинство — простота внедрения. Однако эффективность — ниже всякой критики. Альтернатива — использование детерминистских методов, которые предполагают разметку всех конфиденциальных документов и постоянный контроль над их использованием. В таких условиях контентная фильтрация становится дополнительной технологией, позволяющей автоматически категоризировать новые, не размеченные документы.

Итак, мы снова возвращаемся к

Самые популярные средства ИБ
(можно выбрать неограниченное число вариантов)



постулату о том, что защита может быть либо всеобъемлющей, либо никакой.

Что будет происходить в ближайший год на рынке внутренней безопасности?

— Парадоксально, но факт. Утечки данных занимают первую строчку в рейтинге критических угроз бизнесу, но на практике лишь 29% российских компаний используют специализированные системы защиты.

Анализ динамики проникновения специализированных систем защиты от внутренних ИТ-угроз демонстрирует противоречивую ситуацию. В прошлогоднем исследовании 34% участников заявили о планах внедрения таких систем. Однако свежие данные показали, что это желание реализовали на практике лишь 5%. Безусловно, частично причиной этой разницы можно назвать трудоемкость внедрения технологий класса PCKД или DLP (иногда этот процесс занимает несколько лет), неясность законодательных актов и отсутствие четких стандартов. Однако неоспорим факт, что в российских компаниях слово все еще ощутимо расходится с делом.

Впрочем, налицо и положительная тенденция. На 14% (с 49% до 35%) снизилась доля респондентов, считающих специализированные системы защиты неэффективными. В целом можно констатировать, что в ближайший год рынок внутренней безопасности продолжит свой рост, однако он вряд ли окажется слишком быстрым. Прорыва следует ожидать в среднесрочной перспективе, по мере стабилизации финансовой ситуации: 46% респондентов назвали бюджетные ограничения главным сдерживающим фактором.

МОБИЛЬНЫЕ НАКОПИТЕЛИ СТАЛИ СВОЕГО РОДА ENFANT TERRIBLE, ПОСТОЯННОЙ ГОЛОВНОЙ БОЛЬЮ ВЛАДЕЛЬЦЕВ БИЗНЕСА

По признанию экспертов, человек — самое слабое звено в системе безопасности, но и самое важное! Как избежать в работе службы безопасности соблазна тотальной слежки всех за всеми и сохранить в компании здоровый моральный климат?

— На мой взгляд, здесь нет универсального рецепта. Мне известны организации, где обстановка тотальной слежки и подозрительности и есть торжество

порядка. При этом они продолжают нормально функционировать и демонстрировать приемлемые показатели эффективности работы. В других организациях вполне логично делается упор на образование сотрудников, воспитание в них корпоративного духа, самосознания, чувства единения со стратегическими целями и задачами.

Согласны ли Вы с мнением, что сегодня технические средства обеспечивают лишь «защиту от дурака» и доказательную базу для разбора произошедших инцидентов. Не предусматривается никаких превентивных мер по предотвращению утечек данных, вероятных в результате действий злоумышленников-инсайдеров.

— Увы, наш мир не совершенен, и это ни для кого не секрет. Невозможно создать абсолютную защиту от всех и навсегда. Противостояние меча и щита — это непрекращающийся процесс совершенствования.

Впрочем, уже сейчас можно сказать, что индустрия разработки сделала большой шаг вперед по сравнению с концепцией «защиты от дурака». С Вашего позволения сделаю небольшой экскурс в историю развития систем защиты от инсайдеров.

Первые попытки решить проблему относятся к рубежу веков. В конце 90-х годов появились системы (DLP — Data Leakage Prevention), способные фильтровать сетевой трафик, выявлять и с некоторой долей вероятности блокировать запрещенные слова и выражения. Традиционно, такие системы базировались на антиспам-технологиях и, прямо скажем, к проблеме защиты от инсайдеров были «притянуты за уши». Они унаследовали недостатки «предков» — низкую эффективность, высокий уровень ложных срабатываний и, правда, годились только для «защиты от дурака».

НА ПРАКТИКЕ ЛИШЬ 29% РОССИЙСКИХ КОМПАНИЙ ИСПОЛЬЗУЮТ СПЕЦИАЛИЗИРОВАННЫЕ СИСТЕМЫ ЗАЩИТЫ

Через несколько лет разработчики представили системы, основанные на детерминистской технологии контроля над движением конфиденциальных данных. На каждом компьютере размещалась программа, следившая за правильностью использования помеченных документов.

Недавно начали появляться системы класса РСКД (Режим секретности конфиденциальных данных), которые объединили оба подхода и добились реализации практически 100% защиты для классифицированных данных. Пожалуй, только недостаточное знакомство с развитием отрасли может позволить сделать вывод о низкой эффективности современных технологий защиты. Да, разработчикам еще предстоит предпринять много усилий не только для совершенствования своих решений, но и информирования потенциальных заказчиков.

СОВРЕМЕННЫЙ ИБ-РУКОВОДИТЕЛЬ ДОЛЖЕН БЫТЬ БЛИЖЕ К БИЗНЕСУ

При каких условиях работа специалиста по безопасности может быть эффективной?

— Опущу общеизвестные фразы по поводу профессионализма, образованности, способности работать в команде и т.д. С моей точки зрения, современный ИБ-руководитель должен быть ближе к бизнесу. Не нужно зацикливаться на технологических особенностях систем защиты, но смотреть на проблему с точки зрения эффективности инвестиций, непрерывности бизнес-процессов, соответствия основополагающим целям организации. Это, в свою очередь, возможно, только если в организации существует соответствующая корпоративная культура, предполагающая вовлечение руководителей в стратегическое планирование и управление.

Расскажите о себе.

— Я окончил Дальневосточный политехнический университет по специальности «инженер-геофизик» и Академию Министерства финансов. С 1995 года работаю в области управления и корпоративных продаж в ведущих ИТ-компаниях. В частности, отвечал за стратегические поставки ИТ-решений в нефтегазовую, добывающую и перерабатывающую промышленности. С 2001 года руководил департаментом корпоративных решений «Лаборатории Касперского». В мои обязанности входило обеспечение разработки и реализации политики корпоративных продаж на международном уровне, а также создание и развитие отношений компании со стратегическими партнерами и заказчиками. В 2004 году стал одним из основателей и генеральным директором компании InfoWatch. А с 2007 года — генеральный директор Perimetrix.

Спасибо.