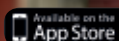


Директор

информационной службы

Скачайте
мобильную
версию



Сергей Прадедов,
заместитель вице-
президента по
безопасности, CISO
компании «МТС», —
о борьбе
с мошенничеством
и защите от других
киберугроз

ТЕМА НОМЕРА:
ЭНЕРГЕТИКА И ЖКХ
ГЛАВНЫЙ ПО «ЦИФРЕ»
ЧЕГО ЖДУТ ОТ CHIEF DIGITAL
OFFICER

ПОДНЯТЬСЯ В МЕНТАЛИТЕТЕ
КАКИХ КОМПЕТЕНЦИЙ
НЕ ХВАТАЕТ СІО

ЧТО ЗНАЕТ ИТ-СЛУЖБА
УПРАВЛЕНИЕ ЗНАНИЯМИ
ВНУТРИ ИТ

АДЕКВАТНАЯ ЗАЩИТА



Рассеивание в облаке

На фоне всеобщего увлечения пользователей публичными облачными сервисами вызывает беспокойство то, что ИТ-руководители постепенно теряют контроль не только над приобретением ИТ бизнес-подразделениями, но и над тем, как сами ИТ-специалисты используют различный инструментарий в своей работе.

Бизнес-подразделения все чаще приобретают ИТ-решения и услуги в обход департаментов по информационным технологиям. В частности, приобретение программных решений как сервисов (SaaS) в ряде случаев представляется бизнесу настолько простым делом, что его можно осуществить самостоятельно. Полагаю, тут сказывается ослепление «легкостью бытия», навеянное консьюмеризацией всего, что только можно: сотрудники привыкают самостоятельно выбирать себе инструменты для выполнения служебных обязанностей — от мобильных устройств, которые покупают за свои деньги и для забавы, и для работы, до браузеров, офисных приложений и прочих ИТ-средств и сервисов.

Вряд ли ИТ-руководители смогут полностью искоренить использование для работы с корпоративными информационными ресурсами технологий, не санкционированных ИТ-службой. Следовательно, им нужно возглавить этот процесс, чтобы сделать его управляемым. И едва ли здесь помогут только жесткие регламенты и запреты. Пользователей самых разных уровней придется убедить в том, что ИТ-средства и сервисы, которые предоставляет или рекомендует ИТ-департамент, в самом деле лучше, чем те, что им порекомендовали друзья или навесили рекламные баннеры. Но прежде ИТ-департаменту нужно убедиться в том, что эти средства и сервисы подходят именно для данной организации.

Вопросы, которые больше всего беспокоят ИТ-руководство, — это распределение расходов на ИТ и информационная безопасность. Особенно много вопросов возникает в области ИБ. Как убедиться в том, что выбранные пользователями средства и сервисы не шпионят за организацией и не выполняют скрытно какие-то вредоносные действия? Как предотвратить утечки информации в результате разгильдяйства? Как выявить и пресечь деятельность инсайдеров? И прочее.

Все эти вопросы ИБ перерастают в проблемы, когда речь заходит о штатных сотрудниках ИТ-департаментов, ведь и их компетенция в области ИТ, как правило, на порядок, а то и два выше, чем у простых пользователей, а возможности доступа к информации и всевозможным ИТ-ресурсам неизмеримо шире. Недавнее исследование, проведенное Frost & Sullivan и McAfee, показало: 80% ИТ-специалистов, похоже, считают оправданным продолжать пользоваться несанкционированными сервисами без соблюдения политик безопасности.



Не думаю, что тотальный контроль или жесткая регламентация использования ИТ-средств и сервисов ИТ-специалистами позволят полностью устранить проблему. На мой взгляд, ее решение следует искать не в сфере технологий, а в области человеческих отношений: придется пересмотреть кадровую политику ИТ-департамента — в частности, принципы отбора специалистов, адаптации их к работе в компании, а также систему мотивации и механизмы управления лояльностью ИТ-сотрудников. Есть основания полагать, что лояльные ИТ-специалисты (если, конечно, штат укомплектован людьми с достаточно высокими нравственными принципами) будут более scrupulously соблюдать правила и регламенты, касающиеся информационной безопасности, и окажутся менее «зловредными» в отношении своего работодателя.

В спорах вокруг «теневых» ИТ внутри самого ИТ-департамента есть еще один интересный аспект: получается, что «главный по ИТ» в эпоху облачных и мобильных вычислений не сможет толком проконтролировать своих собственных сотрудников и добиться, чтобы они пользовались исключительно теми ИТ, которые разрешены ИТ-департаментом. Возникает болезненный вопрос: если директор по ИТ не имеет реальной власти над деятельностью своих сотрудников, то может ли он претендовать на дополнительные полномочия, «роли» и «миссии», которые ему делегирует бизнес? Полагаю, что ответ зависит от раскрытия лидерских качеств ИТ-руководителя. Только будучи ярким лидером, он сможет реально управлять и своими подчиненными, и всем, что имеет отношение к информационным технологиям.

Михаил Зырянов



18 Тема номера 28 Технологии для бизнеса 42 Управление

В каждом номере:

- 4 **ИТ**ого
- 63 **МонИТ**ор
- 64 **хИТ**ы

ТЕМА НОМЕРА | ЭНЕРГЕТИКА И ЖКХ

18 Электроэнергетика и ЖКХ: эффективность и ИТ

Марина Полякова

Стремясь следовать международным концепциям развития энергетики, таким как Smart Grid, российские энергокомпании внедряют интеллектуальные приборы учета электроэнергии, модернизируют инфраструктуру и автоматизируют свою деятельность.

24 Энергичные документы

Дмитрий Капралов

Внедрение юридически значимого электронного документооборота позволяет «Учетно-финансовому сервису» «КЭС-Холдинга» сократить «бумажные издержки», повысить эффективность взаимодействия с компаниями холдинга, ускорить внутренние бизнес-процессы.

ТЕХНОЛОГИИ ДЛЯ БИЗНЕСА

ИТ-ИНФРАСТРУКТУРА

28 Крылья для Service Desk

Наталья Дубова

Модернизацию службы Service Desk в международном аэропорту Шереметьево можно было бы отнести к вполне рядовым ITSM-проектам. Однако значимость управления инцидентами для ИТ-среды, от работоспособности которой часто напрямую зависит нормальное функционирование ведущего российского аэропорта, заставляет пристальней присмотреться к этому опыту.

32 Облако про запас

Михаил Зырянов

Создавать собственный резервный ЦОД или приобретать ресурсы для резервирования ИТ как услуги? В компании «Аэрофлот» предпочли создать собственный ЦОД с виртуализованной инфраструктурой.

ИНТЕРВЬЮ

12 Адекватная защита

Михаил Зырянов

Сергей Прадедов, заместитель вице-президента по безопасности, директор департамента информационной безопасности компании «МТС», — о ключевых подходах к защите от киберугроз.

ПРАКТИКА

35 Документальная история

Ирина Шеян

Компании «Газпром комплектация» удалось резко повысить скорость согласования спецификаций с помощью системы электронного документооборота, а затем интегрировать СЭД с ERP-системой.

38 Бухгалтерская первичка в электронном виде

Вячеслав Вейгандт

Внедрение электронного документооборота для первичных бухгалтерских документов помогло Челябинскому металлургическому комбинату ускорить технологический процесс, упорядочить документооборот и снизить налоговые риски.

ИТ-УНИВЕРСИТЕТ

40 Сделать печать прозрачной

Николай Смирнов

Расходы на печать занимают третье место в операционных ИТ-бюджетах после зарплат сотрудников и услуг связи. Между тем офисная печать не дает никаких конкурентных преимуществ большинству компаний, поэтому следует серьезно задуматься о ее оптимизации.

УПРАВЛЕНИЕ

КАРЬЕРА И МЕНЕДЖМЕНТ

42 Два в одном

Ирина Шеян

Молодая и все еще формирующаяся профессия ИТ-директора — это яркое воплощение конвергенции компетенций. Помимо ИТ, менеджмента и набора смежных с ними дисциплин, СІО должен прекрасно разби-

Главный редактор
 Михаил Зырянов mikez@osp.ru

Ответственный редактор
 Яна Абрамова

Редакторы
 Марина Полякова,
 Ирина Шеян,
 Николай Смирнов

Литературный редактор
 Нина Михеева

Фотографии
 Игорь Лапшин
 Дмитрий Демчев

Иллюстрации
 Анна Арианова

Дизайн и верстка
 Марина Романчук

Директор по рекламе
 Юлия Ломино lomino@osp.ru

Менеджер по рекламе
 Ирина Смирнова

Адрес редакции: Россия, 127254, Москва,
 ул. Руставели, д.12а, стр.2

www.cio.ru

Адрес для корреспонденции:
 127254, Москва, а/я 42

Телефоны: (495) 725-4780 (издательство)
 Факс: (495) 725-4783

Комментарии к статьям
 направляйте по адресу: cio@osp.ru

Подписные индексы:

64112 (дополнение к каталогу «Пресса России», стр. 22)
 38695, 80478 (каталог агентства «Роспечать»)
 99486 (каталог «Почта России»)

Реклама

ООО «Рекламное агентство «Чемпион»
 Телефон: (499) 750-0467

Распространение

ООО «ОСП-Курьер», тел.: (495) 725-4785
 Отпечатано в ООО «Богородский полиграфический
 комбинат», 142400, Московская область, г. Ногинск,
 ул. Индустриальная, д. 40 б
 Тел.: (495) 783-9366, (49651) 73179

© 2013 Издательство «Открытые системы»
 © 2002–2013 International Data Group, Inc.

Издание зарегистрировано в Министерстве РФ по
 делам печати, телерадиовещания и средств массовых
 коммуникаций за № ПИ 77-7291 от 19.02.2001

Цена свободная

**ОТКРЫТЫЕ
 СИСТЕМЫ**
 Open Systems Publications
 Открыты для вас. 20 лет

Учредитель и издатель:

ЗАО «Издательство «Открытые системы»

Адрес издательства: Россия, 123056, Москва,
 Электрический переулок, дом 8, строение 3

Президент: Михаил Борисов

Генеральный директор: Галина Герасина

Директор ИТ-направления: Павел Христов

Коммерческий директор: Татьяна Филина

Тираж 7500 экз.

Журнал выходит ежемесячно

Подписано в печать: 19.12.2013

Редакция не несет ответственности за содержание
 рекламных материалов.

Все права на материалы, опубликованные в номере,
 принадлежат журналу «Директор информационной
 службы» (CIO.RU). В номере использованы иллюстрации
 и фотографии «Издательства «Открытые системы»,
 International Data Group, PressFoto, Пресс-служба
 «Аэрофлот», «Шереметьево», «КЭС».

Перепечатка материалов без разрешения редакции
 запрещена.

При использовании материалов ссылка на «Директор
 информационной службы» (CIO.RU) обязательна.

Мобильная версия журнала



ратся в специфике отрасли, где
 ему довелось трудиться. И если
 раньше он добирал недостающие
 знания предметной области глав-
 ным образом на практике, то се-
 годня наблюдается тенденция пе-
 рехода от эмпирических знаний
 к фундаментальному образованию
 в двух областях.

46 Почему роль Chief Digital Officer становится все актуальнее?

Рич Хейн

Современным организациям
 приходится сталкиваться с тех-
 нологиями буквально на каждом
 шагу: социальные сети, мобиль-
 ные инструменты, Большие Дан-
 ные, аналитические механизмы,
 средства составления отчетов,
 инфраструктура, системы хра-
 нения и прочее, прочее, прочее.
 Как старым «традиционным»
 предприятиям конкурировать в
 цифровом мире с новыми компа-
 ниями, рожденными уже в циф-
 ровой век?

48 Ненаписанного — не существует

Николай Смирнов

Управление знаниями своих со-
 трудников — обязанность любо-
 го руководителя. Однако пере-
 давать информацию «из уст в
 уста» не всегда эффективно и,
 более того, не всегда возможно.
 Создание базы знаний помога-
 ет эффективно решить проблему.
 Главное — верно организовать ее
 наполнение.

УПРАВЛЕНИЕ ИТ- ПОСТАВЩИКАМИ

52 САРЕХ, ОРЕХ и ИТ-аутсорсинг

Сергей Таран

Ответ на вопрос, что лучше — по-
 купать ИТ или брать в аренду, за-
 висит в первую очередь от целей
 бизнеса и от того, на рост каких по-
 казателей компания в данный мо-
 мент ориентирована.

УПРАВЛЕНИЕ ИТ

54 Курс на мобилизацию, или Новейшая история BYOD

Юрий Черкас

Как бы бизнес ни открещивался от
 причастности к внедрению BYOD,
 эта концепция уверенно набирает
 обороты. Можно выделить несколь-
 ко востребованных сценариев, ори-
 ентированных на эффективное ре-
 шение существующих бизнес-задач.

57 Пять изменений в организации технической поддержки в эпоху BYOD

Мэри Брэндел

С ростом популярности концепции
 BYOD возникает резонный вопрос:
 а как будет осуществляться техни-
 ческое обслуживание и поддержка
 этих устройств?

59 COPE против BYOD

Том Канешиге

Работодатели понимают, что оста-
 новить мощный поток потребитель-
 ских устройств, наводняющих ком-
 пании, практически невозможно, но
 в их силах минимизировать послед-
 ствия. Компании восстанавливают
 контроль с помощью совершенство-
 вания моделей организации вычис-
 лений и набирающей популярность
 концепции COPE, которая уже впло-
 не в состоянии соперничать с BYOD.

CSO

61 Неоднозначный урожай регулирования безопасности

Юлия Онищук

Претерпевшее в 2013 году замет-
 ные изменения российское законо-
 дательство по-прежнему несовер-
 шенно, но связанные с ним риски
 достаточно велики и оставлять без
 внимания меры по выполнению
 требований регуляторов в области
 ИБ явно не стоит.

ИТого за Декабрь



Рынок высоких технологий

Операторы ЦОД воюют за клиентов

В последние годы в России заметно росла потребность в услугах ЦОД, обусловленная развитием корпоративных систем и желанием компаний снизить технические риски. До сих пор самой востребованной услугой остается размещение в ЦОД серверов и систем хранения заказчика.

По оценкам польской компании PMR, на российском рынке коммерческих ЦОД присутствуют 80 игроков. При этом 65% их суммарной полезной площади сконцентрировано в Москве и ближнем Подмосковье. Что логично, столичные операторы являются и лидерами по выручке, контролируя 75% рынка.

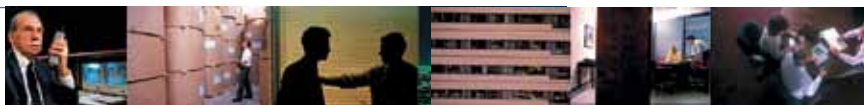
Российский рынок уже несколько лет сохраняет высокие темпы роста. В прошлом году он вырос на 20% по сравнению с 2011 годом и достиг 7,8 млрд руб., а в нынешнем — должен превысить 9 млрд руб. Услуга хостинга серверов (colocation) приносит операторам большую часть доходов. При этом около половины заказчиков составляют финансовые организации, резервирующие свои системы. Компании сегмента SMB обычно приобретают выделенные или виртуальные серверы для поддержки сайтов и приложений.

Среди наиболее значимых тенденций можно выделить снижение цен на размещение серверов, что вынуждает операторов инвестировать в создание

более прибыльных и перспективных решений, в том числе облачных сервисов и комплексных услуг по обеспечению непрерывности бизнеса.

Растущая конкуренция вынуждает прибегать к агрессивным маркетинговым стратегиям. Помимо традиционных кампаний, предлагающих значительные — от 20 до 50% — скидки, некоторые операторы переманивают более выгодными условиями заказчиков у своих конкурентов. Объектами таких целенаправленных атак становятся перспективные клиенты, уже пользующиеся услугами ЦОД на одной из соседних площадок. К подобным методам прибегают, как правило, не крупные провайдеры.

Управление



Специалист по Oracle

Исследовательский центр портала Superjob.ru изучил предложения работодателей на позицию «программист Oracle».

Данные специалисты осуществляют разработку и сопровождение программного обеспечения под СУБД Oracle, конвертирование данных различных форматов в базы Oracle, участвуют во внедрении нового программного обеспечения и в проектировании программных комплексов. Средняя предлагаемая им зарплата составляет 105 тыс. руб. в Москве и 84 тыс. руб. в Санкт-Петербурге.

От соискателей, впервые претендующих на должность программиста Oracle, работодатели ждут уверенных навыков программирования на PL/SQL и опыта разработки под Oracle. Молодые специалисты должны знать английский язык на уровне, достаточном для чтения технической документации. В качестве начинающих програм-

мистов Oracle могут пробовать силы выпускники либо студенты профильных и технических факультетов вузов. Стартовый оклад, на который могут рассчитывать кандидаты без опыта работы, в столице составляет от 50 до 70 тыс. руб.

Рассчитывать на более высокий заработок могут программисты Oracle со стажем работы от одного года. Такие специалисты должны уметь разбираться в чужом программном коде, иметь опыт работы с системами контроля версий и начальные навыки проектирования. Специалистам, соответствующим указанным требованиям, обещают платить до 85 тыс. руб.

Следующий зарплатный диапазон открыт специалистам с опытом программирования под Oracle более двух лет. Кандидатам необходимо иметь законченное высшее образование, знать методологию разработки информационных систем, а также иметь навыки проектирования баз

данных, оптимизации SQL-запросов. Конкурентным преимуществом на рынке труда обладают специалисты с опытом работы в компаниях по профилю деятельности потенциального работодателя. Предлагаемая зарплата для программистов Oracle такого профессионального уровня достигает 115 тыс. руб.

Стаж программирования под Oracle более трех лет, опыт работы с высоконагруженной базой большого объема и навыки оптимизации сложных запросов — таковы ключевые требования к разработчикам, претендующим на максимальный доход. Ярким доказательством профессионализма опытного специалиста будет портфолио завершенных проектов. Дополнительным плюсом послужит свободное владение английским языком. Наиболее высокий доход программистов Oracle составляет 140 тыс. руб. в Москве и 115 тыс. руб. в Северной столице.

Бизнес и технологии



Большие Данные иссякнут?

В течение ближайших пяти лет компании столкнутся с проблемами приобретения клиентских данных. Сейчас их можно раздобыть довольно свободно: достаточно заглянуть в социальные сети. Другое дело, что мало кто всерьез задается такой целью. Однако, как прогнозируют в Ernst & Young, очень скоро клиенты начнут более серьезно относиться к своей персональной информации.

Проведенное исследование показало, что половина людей выкладывает на всеобщее обозрение информацию о себе уже с большей осторожностью, чем несколькими годами ранее, и почти столько же планируют дальнейшее ограничение доступа к персональной информации. Такое поведение может нанести серьезный удар по концепции использования Больших Данных.

Несанкционированное использование персональных данных не на шутку встревожило людей. Особенно их нервирует передача информации от одной компании другой — 75% негативно отзываются о такой практике.

Между тем компании продолжают возлагать большие надежды на накопление и анализ клиентских данных. 62% запустили специальные программы сбора и интерпретации информации о потребителях, причем большинство заявляет о наличии финансового эффекта.

Облачные активы требуют особого управления

Предприятия получают максимальную пользу от облачных вычислений лишь в тех случаях, когда они внедряют проверенные методики управления программными активами (Software Asset Management, SAM). Как подчеркивают в BSA, недостаточно эффективное управление программными активами в облаке способно нивелировать многие преимущества облачных решений. Например, компании не могут снизить издержки или минимизировать свои риски.

Как выяснилось, с внедрением облачных технологий у предприятий не стало меньше забот и переживаний относительно соблюдения условий лицензирования — скорее, добавились новые. Добиться соответствия лицензионным требованиям можно путем эффективного внедрения процессов SAM. И хотя при переходе в облачное окружение цели методологии SAM не изменились, процессы SAM нуждаются в корректировке и адаптации.

При переходе к облаку следует обращать особое внимание на уже существующие, традиционные соглашения о лицензировании программных продуктов для обеспечения соответствия лицензионным требованиям. Концепция потребления программного обеспечения в виде сервиса способна создать определенные трудности, обуслов-

ленные неавторизованным использованием ПО или, наоборот, тем, что приобретаемое программное обеспечение остается невостребованным.

Менеджеров по продажам больше не слушают

Поведение компаний, приобретающих ИТ-продукты, все больше приближается к поведению покупателей обычных потребительских продуктов. Как показали результаты опроса, проведенного Avanade, 61% тех, кто принимает решение об ИТ-инвестициях, больше ориентируется на мнение коллег, аналитические сайты, отзывы партнеров и обсуждения в социальных сетях, чем на информацию, полученную от вендоров.

Консьюмеризация ИТ радикально трансформировала традиционные каналы продаж продуктов и услуг. Поставщики теряют контроль над процессом продаж, и модели B2B и B2C постепенно сближаются.

Это не значит, что профессия менеджера по продажам корпоративных приложений постепенно уходит в прошлое. Напротив, взаимодействие с бизнес-покупателями будет приобретать все более важное значение. Однако место, где это взаимодействие будет происходить, изменится. Вендорам ИТ-систем, как и многим другим, придется идти в мобильные каналы и социальные сети.

Антифрод-терминал

Решение для безопасной работы
с электронной подписью
в недоверенной среде

- Защита от подмены подписываемых документов
- Защита от перехвата управления
- Аутентификация терминала на сервере



ЗАО "Аладдин Р.Д."
Тел.: +7 (495) 223-00-01

aladdin@aladdin-rd.ru
www.aladdin-rd.ru





НЕ
ПРОПУСТИТЕ

«Проект года»

Конкурс
30 января
Москва
Global CIO,
www.globalcio.ru/projectoftheyear

Big Data – 2014

Форум
20 марта
Москва, МИВЦ «ИнфоПространство»
Издательство «Открытые системы»,
www.osp.ru

«Бизнес-Видео – 2014»

Форум
1 апреля
Москва
«Журнал сетевых решений/LAN»,
www.osp.ru/bvideo/

«Встраиваемые технологии — 2014.

Современные программные и аппаратные
решения»
Конференция
16 апреля
Москва
Компания «Кварта Технологии»,
www.embeddeday.ru

«Мобильное предприятие – 2014»

Форум
24 апреля
Москва
Журнал «Открытые системы. СУБД», Агентство
корпоративных коммуникаций OSP-Con,
www.ospcon.ru

«Связь-Экспокомм – 2014»

Выставка
13-16 мая
Москва, ЦВК «Экспоцентр»
«Экспоцентр»,
www.sviaz-expocomm.ru

«МИР ЦОД – 2014»

Форум
Май
Москва
«Журнал сетевых решений/LAN»,
www.osp.ru/dcworld/

11-й IT Management Forum

5 июня
Москва, гостиница «Radisson-Славянская»
Журнал «Открытые системы. СУБД», Агентство
корпоративных коммуникаций OSP-Con,
www.ospcon.ru

на правах рекламы

ИТого

Техника безопасности



Следят и будут следить

Треть работодателей ведут слежку за своими сотрудниками. Как выяснилось в ходе опроса, проведенного Zecurion Analytics, более 30% российских компаний контролируют активность своего персонала и в социальных сетях, и в электронной почте.

48% опрошенных признались, что отслеживают действия сотрудников в социальных сетях «ВКонтакте», Facebook, «Одноклассники», а 68% — в корпоративной электронной почте. На третьем месте в списке контролируемых каналов находятся интернет-пейджеры, и лишь 9% специалистов по безопасности отметили, что в их компаниях контролируются принтеры. Компании уверены, что через бумажные носители крайне сложно потерять информацию в большом объеме. Между тем, по статистике, более 10% всех утечек происходит именно через принтеры.

Стремление компаний к контролю действий своих сотрудников обусловлено тем, что, по результатам исследования, почти 90% из них периодически страдают от утечек информации. Наибольшую ценность для респондентов представляют персональные данные сотрудников и акционеров, списки клиентов, поставщиков и другие данные CRM-систем, а также персональные данные клиентов. Более половины организаций имеют в штате выделенные подразделения по информационной безопасности, еще 17% планируют создать их у себя в течение будущего года.

За утечками не успевают

Каждая вторая компания в России хотя бы раз сталкивалась с утечками информации. Как выяснилось в ходе опроса, проведенного «МФИ Софт», половина из них понесла убытки в результате инсайдерской деятельности. Несмотря на это, специализированные DLP-системы для защиты информации использует лишь каждая пятая компания. Чаще всего утечки информации удается выявлять в Москве — 22% столичных компаний сталкиваются с инсайдерами 3–5 раз в год и более.

Попытки так или иначе защитить свои информационные ресурсы предпринимают все. Однако инфраструктура ряда предприятий достаточно архаична, поэтому процесс перехода на современные технологии защиты

отстает от развития технологий передачи информации.

Наиболее консервативный подход к информационной безопасности характерен для специалистов Нижнего Новгорода, которые чаще остальных прибегают к таким радикальным мерам, как запрет USB-портов, ограничение доступа к интернет-ресурсам и квотирование трафика. По технологическому обеспечению информационной безопасности лидирует Екатеринбург — специализированные системы класса DLP используются здесь в 34% компаний.

Чаще всего специалисты выявляют утечки информации, произошедшие с помощью электронной почты или съемных носителей информации. Вероятно, большое количество выявленных на этих каналах утечек связано с технической простотой их контроля и очевидностью для специалистов. В регионах, активно использующих DLP-системы, более эффективно удается контролировать каналы передачи информации (бумажные носители, портативные и мобильные устройства).

Атакуют всех

В течение нынешнего года ИТ-инфраструктура 95% российских организаций как минимум один раз подверглась внешней атаке. Наиболее частой угрозой является вредоносное ПО и спам-атаки.

Один из ключевых параметров, позволяющих определить значимость ущерба от той или иной атаки, — это факт утечки данных в атакованной компании. В ходе опроса, проведенного B2B International, выяснилось, что для 40% компаний самые частые атаки с использованием вредоносного ПО стали и самыми разрушительными. В 9% случаев они привели к утечке конфиденциальных данных, разглашение которых причинило ущерб бизнесу. Кроме того, к утечкам данных в 13% случаев приводили случаи корпоративного шпионажа, хакерские и фишинговые атаки.

Одной из ключевых тенденций рынка информационной безопасности стало смещение фокуса от точечной защиты к комплексным решениям. Компании понимают, что недостаточно использовать только антивирус или только разграничивать права доступа. Они начинают выстраивать интегрированные системы защиты.