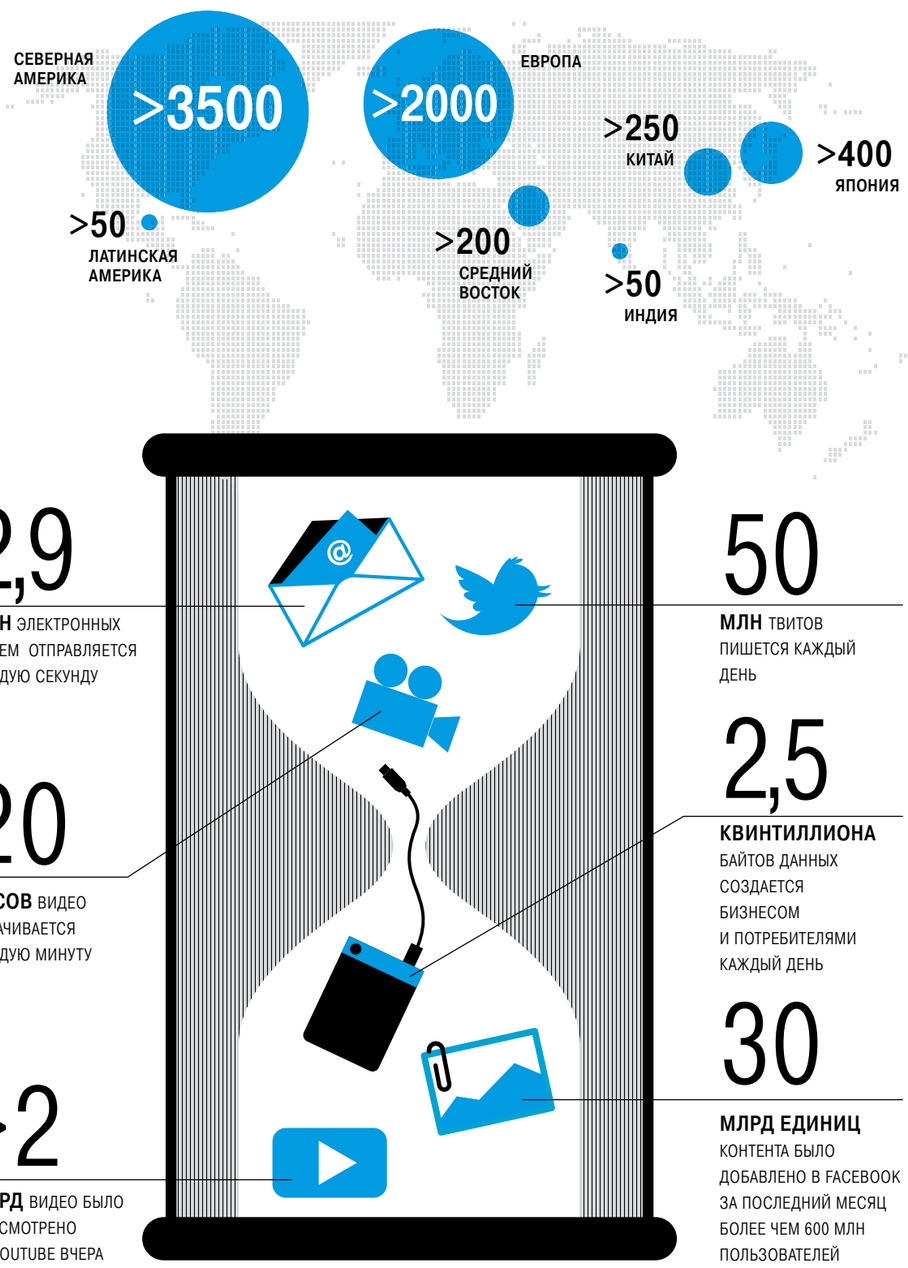
информационные технологии

Большие числа

СОГЛАСНО ЯНВАРСКОМУ ПРОГНОЗУ IDC, МИРОВОЙ РЫНОК ПО ОБРАБОТКЕ БОЛЬШИХ ДАННЫХ (BIG DATA) БУДЕТ РАСТИ НА 31,7% В ГОД И ДОСТИГНЕТ К 2016 ГОДУ ОБЪЕМА $23,8 МЛРД. А САМИ БОЛЬШИЕ ДАННЫЕ БУДУТ АКТИВНО ИСПОЛЬЗОВАТЬСЯ ДАЖЕ В ЗДРАВООХРАНЕНИИ.

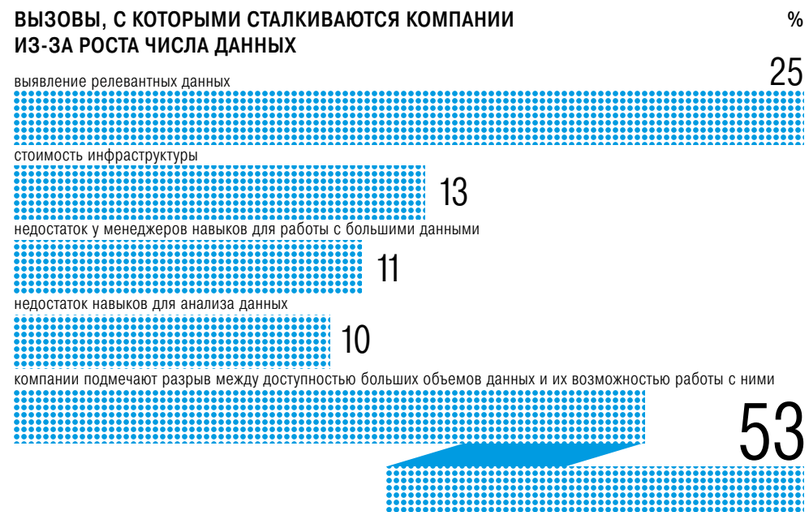
ОБЪЕМ СОХРАНЕННЫХ БОЛЬШИХ ДАННЫХ (ПЕТАБАЙТЫ)



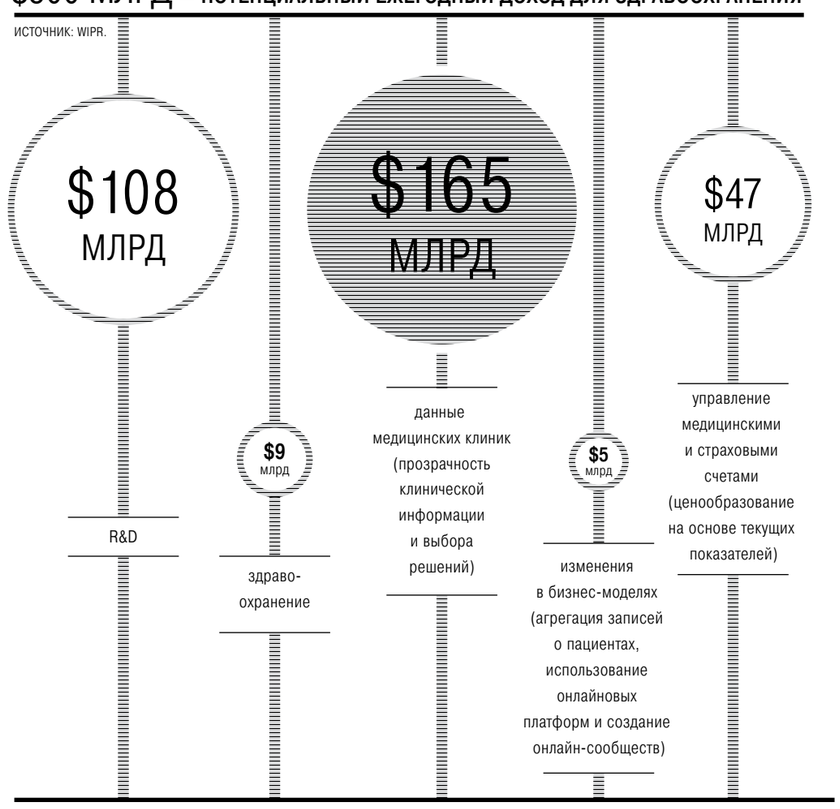
112 000 000

ЗАПИСЕЙ В БЛОГАХ ПОСВЯЩЕНЫ ОБСУЖДЕНИЮ BIG DATA

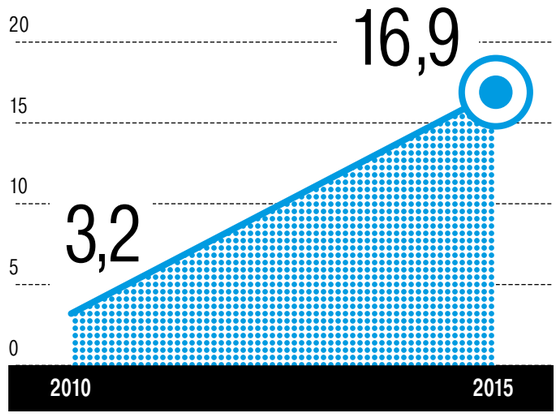
ВЫЗОВЫ, С КОТОРЫМИ СТАЛКИВАЮТСЯ КОМПАНИИ ИЗ-ЗА РОСТА ЧИСЛА ДАННЫХ



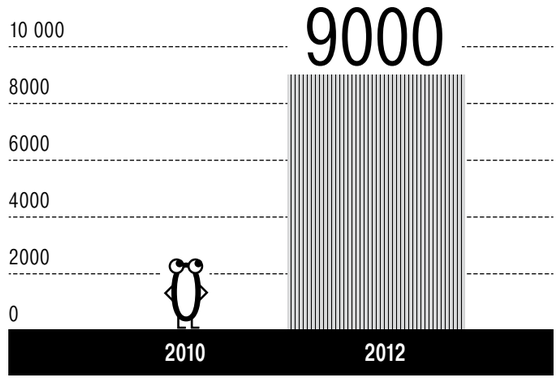
$300 МЛРД – ПОТЕНЦИАЛЬНЫЙ ЕЖЕГОДНЫЙ ДОХОД ДЛЯ ЗДРАВООХРАНЕНИЯ



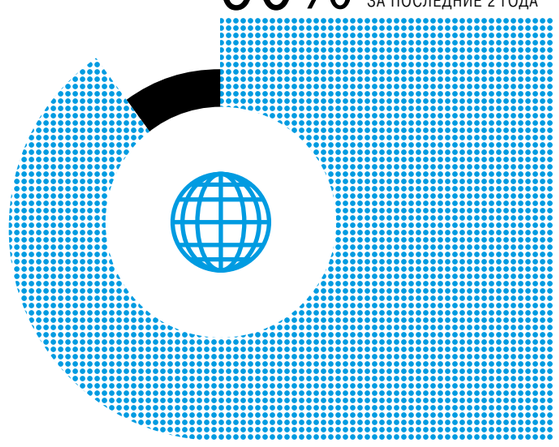
ОБЪЕМ РЫНКА РЕШЕНИЙ ДЛЯ ОБРАБОТКИ BIG DATA ($ МЛРД)



ПОИСК ПО ВАКАНСИИ DATA SCIENTISTS (РЕЗУЛЬТАТЫ)



90% ВСЕХ МИРОВЫХ ДАННЫХ БЫЛО СОЗДАНО ЗА ПОСЛЕДНИЕ 2 ГОДА



Внимание регулировщика

бизнес

(Окончание. Начало на стр. 12)

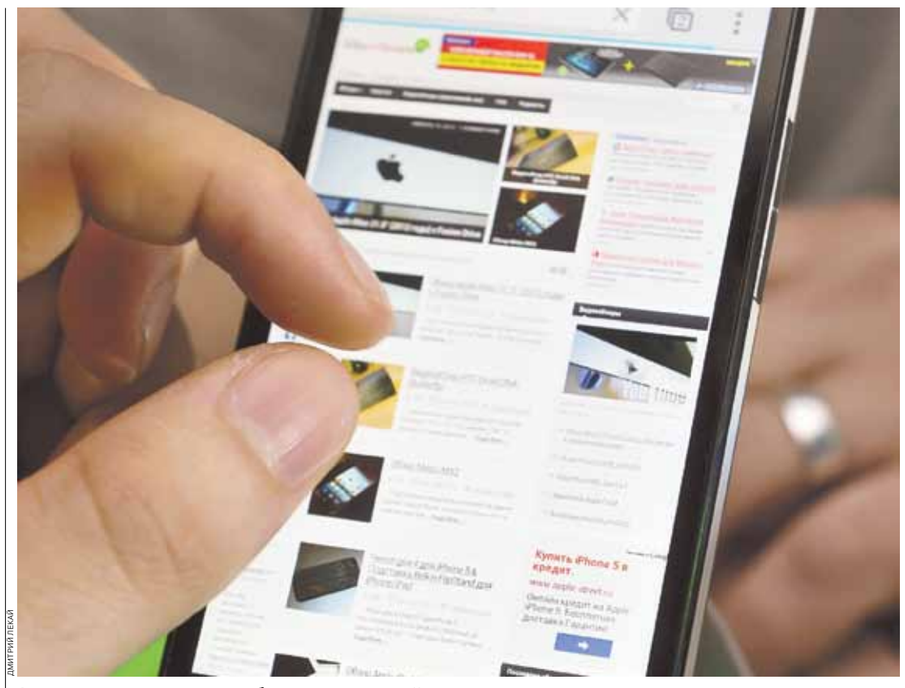
В частности, господин Башлыков подчеркивает, что рынок аудита по информационной безопасности у нас пока находится на этапе становления: нет стандартов, четких прописанных характеристик этой услуги. Под «аудитом по информационной безопасности» каждый понимает что-то свое. «В результате ожидания от таких проектов у заказчиков часто разные. Так что нам каждый раз приходится уточнять, какие именно задачи хочет решить с помощью аудита конкретная компания», — добавляет господин Башлыков.

Виртуализация в фокусе

По мнению Игоря Кораблева, руководителя направления защиты промышленных систем департамента сетевой интеграции ЛАНИТ, в 2012 году на рынок ИБ в России повлияли общемировые тренды, связанные с качественным и количественным ростом возможностей, доступных злоумышленникам. Кибератаки становятся коммерчески эффективным инструментом. При этом область возможного применения этих инструментов значительно расширилась. Сложность и распределенность кибератак показала необходимость создания инструментов глобального мониторинга информационной безопасности. В 2013 году должны быть предприняты шаги по созданию таких систем, как в России, так и в США.

Активное распространение идеологии BYOD (bring your own device) и мобильных приложений в корпоративном секторе спровоцировало интерес злоумышленников к мобильным устройствам, что обусловило рост спроса на решения MDM и мобильной безопасности. Влияние этого тренда в 2013 году будет только усиливаться.

В 2012 году произошел резкий рост количества обнаруженных уязвимостей в программном и аппаратном обеспечении промышленных систем (АСУТП). Многочисленные исследования показали катастрофически низкий уровень обеспечения информационной безопасности АСУТП. С другой стороны, эти же исследования показали неэффективность, а иногда невозможность применения стандартных для корпоративных сетей средств защиты в технологических сетях. В связи с этим на рынке обнаружился недостаток решений для защиты технологических сетей, что дало возможность выхода на рынок новым, нишевым вендорам. В 2013 году ожидается появление новых средств защиты АСУТП преимущественно зарубежных вендоров. Процесс формирования общих методов и требований по обеспечению информационной безопасности АСУТП поднимет спрос на услуги консалтинга в этой области.



ДМИТРИЙ ЛЕКАЯ

Активное распространение мобильных приложений в корпоративном секторе спровоцировало интерес злоумышленников к мобильным устройствам, что обусловило спрос на решения мобильной безопасности

В числе определяющих трендов прошедшего года господин Ляпунов называет переход угроз в сфере ИБ в разряд системных, а также заметный рост числа кибератак. «Последнее связано с тем, что хакерская деятельность стала представлять собой вполне сформировавшуюся индустрию. Хакерское сообщество превратилось в полноценный теневой рынок с годовым оборотом в миллиарды рублей и широчайшим спектром влияния, в который попадают не только бизнес-структуры или государственные организации, но и все население в целом», — объясняет господин Ляпунов. При этом он отмечает значительное снижение объема спама в интернете, что происходит за счет «сужения специализации» хакеров.

Сергей Земков считает, что сегмент антивирусных систем в последние пять-семь лет показывал самые высокие темпы роста среди всего рынка ИБ. Это было связано с несколькими фактами. Во-первых, произошло «обеление» рынка ПО: пользователи активно переходили с нелицензионных продуктов на лицензионные. Второй фактор — это изменение законодательной базы: вступление в силу закона о персональных данных, наличие обязательной сертификации для программных продуктов, защищающих персональные данные, и т. д. Но на сегодняшний день, по словам господина Земкова, эти драйверы исчерпаны или, по крайней мере, основную свою роль уже сыграли. И теперь для производителей антивирусного ПО возможность роста заключается в развитии на внешних рынках.

К числу новых направлений, актуальность которых возросла в 2012 году, господин Ляпунов относит предоставление «облачных» услуг и сервисов виртуализации в сфере ИБ. «Некоторые отечественные интеграторы уже начали предлагать сервисы ИБ из „облака“, но этот подход к оказанию ИБ-услуг пока нельзя назвать массово-популярным. Тем не менее его перспективность на сегодняшний день очень высока», — добавляет он.

Игорь Корчагин, специалист по ИБ компании ИВК, также говорит, что активное внедрение технологий виртуализации в ИТ-инфраструктуру предприятий заметно влияет на рынок ИБ, а кроме того, в тренде использование мобильных устройств (в том числе по схеме BYOD), внедрение портальных решений и систем электронного документооборота. «В ближайшее время в России возможен также всплеск интереса к теме безопасности АСУТП, — рассказывает господин Корчагин. — Однако в настоящее время по указанным трендам на российском рынке ИБ готовых продуктов практически нет, сертифицированных же отечественных решений либо нет вообще, либо их предлагают один-два разработчика, не больше. Такое положение дел характеризует отечественный ИБ-рынок как молодой и исключительно перспективный».

По словам господина Башлыкова, все более изощренными становятся хакерские атаки — отчасти это связано с переходом от массированных атак к направленным, которые довольно дорогие и трудоемкие. Например, создается вирусное ПО, которым с помощью подставного лица заражаются компьютеры организаций. Из-за того что преступники, создавая вирус, ориентируются на особенности ИТ-инфраструктуры конкретной компании, такую атаку крайне сложно обнаружить. А потери компаний в результате могут доходить до десятков миллионов долларов. Решения, которые способны помочь в такой ситуации, уже появились на рынке. Еще один перспективный сегмент — системы мониторинга инцидентов: они помогают не только отследить и устранить брешь в системах защиты, но и провести расследование, найти уязвимые места и не допустить повторения ситуации.

В технологиях мониторинга, а также автоматизации ИБ видит большие перспективы господин Рахметов. «Одной из проблематик, существующих в бизнесе, является многообразие активов, систем, технологий, продуктов, решений, — объясняет он. — Обеспечение ИБ как сервиса всего вышеперечисленного многообразия является неотъемлемой частью бизнеса. Увидеть и управлять своей безопасностью становится потребностью компаний. При этом на сегодня на российском рынке только зарождается культура автоматизации ИБ как процесса. Тем не менее тренд имеет как регуляторную поддержку, начиная от постановлений и заканчивая созданием ситуационных центров на уровне государства, так и соответствие международным практикам».

Михаил Башлыков отмечает, что задач, связанных с безопасностью, становится больше и они усложняются. Отдел по информационной безопасности есть уже в большинстве компаний — многие идут дальше, выделяя его в обособленную организацию. Но постепенно компании переходят к следующему этапу — полному аутсорсингу — и отдают сторонним компаниям как отдельные задачи, связанные с безопасностью, так и целые направления работы.

Регуляторы и ИБ

По мнению экспертов, рынок ИБ вообще сильно подвержен влиянию регуляторов. Александр Санин, коммерческий директор компании «Аванпост», рассказывает, что развитие российского рынка ИБ в последние несколько лет на 80% зависит исключительно от регуляторов в лице ФСТЭК и ФСБ. И прошлый год не стал исключением. Алексей Лукацкий, консультант по безопасности Cisco, подсчитал, что в России за последние два года появляется примерно четырепять нормативных актов по ИБ в месяц, причем три из четырех обязательны для применения.

Федеральный закон N161-ФЗ «О национальной платежной системе», появившийся в прошлом году, значительно повышает требования к банкам, в том числе в части механизмов противодействия мошенничеству. «На данный момент мы также находимся в ожидании нормативных актов и конкретных нормативных требований ФСТЭК и ФСБ России по защите ПДН, — добавляет господин Ляпунов. — Но если оценивать степень давления со стороны регуляторов на рынок ИБ в целом, то в 2012-2013 годах оно значительно ниже, чем ранее, а доля проектов, нацеленных исключительно на выполнение законодательных требований, в среднем сократилась в полтора раза».

Выполнение требований регуляторов, по мнению большинства опрошенных экспертов, один из основных драйверов рынка ИБ. «Общий тренд не изменился, и существенных предпосылок к его изменению нет, — уверен Руслан Рахметов. — Безопасность от „регуляторов рынков“ будет основным трендом как в государственном секторе, так и в коммерческом. Положительная тенденция видится в методичном сокращении разрыва между „безопасностью от регуляторов“ и реальной безопасностью».

Павел Ерошкин, директор департамента информационной безопасности компании «Техносерв», также напоминает о том, как влияют на рынок продолжающиеся изменения в механизме сертификации. «ФСТЭК продолжает идти путем РД БИТ, позаимствованным из европейских common criteria, — рассуждает он. — Выпущены профили защиты для антивирусов и систем обнаружения вторжений, на сайте ФСТЭК лежат проекты профилей для целого ряда решений по информационной безопасности. Вопрос, насколько этот непростой путь целесообразен. Хочу заметить, что одной из особенностей ИБ в России является то, что конкуренция между различными вендорами сводится к войне сертификатов. Более чем за год существования профилей для систем обнаружения вторжений появилось лишь одно сертифицированное решение, которое ранее на российском рынке не было представлено либо было представлено в очень небольшом количестве».

Господин Санин говорит, что в прошлом году немного замедлился рост консалтинговой составляющей рынка, что в целом объяснимо: «Многие компании-заказчики, с которыми мне доводилось говорить об этом, просто устали от постоянной неопределенности в различных вопросах ИБ (все-таки законодательство у нас не на самом высоком уровне) и притормозили консалтинговые проекты до полной ясности». Господин Санин надеется, что в 2013 году эти проекты будут разморожены.

По словам господина Ляпунова, объем поставляемых услуг, их качество и бизнес-модели, характерные для игроков российского рынка ИБ, значительно изменяются. При этом трансформируется и сам рынок. Службы ИБ уже берут на себя новые задачи, обеспечивая реальную безопасность бизнеса и предъявляя все более высокие требования к поставщикам решений. В будущем, по мнению господина Ляпунова, вендоры, в свою очередь, возьмут на себя решение части задач по внедрению и кастомизации своих продуктов. Некоторая часть классических ИБ-интеграторов перейдет в разряд специализированных сервис-провайдеров или отраслевых аутсорсеров и будет предоставлять услуги по обеспечению безопасности, а сложные интеграционные вопросы — решать совместно с вендорами. На долю остальных останется решение задач управления большими федеральными проектами или низкомаржинальная проектная дистрибуция.

Светлана Рагимова