#6–7 (231) 2015

WWW.B-MAG.RU

БИЗНЕС журнал

Самый большой тираж среди деловых журналов России по данным Национальной тиражной службы за 2014 год

ISSN 1819–267X

16+

ЦИФРОВАЯ ПАРТИТУРА

музыкальная индустрия в эпоху digital 42

ПОДОИТЬ ОСЕТРА
хроники рынка черной икры с.10

ХОД КОНЁМ
от создателя «Лошадиной силы» с.16

ТЕХНООККУПАЦИЯ
страшнее зависимости от импорта с.36

ИНФОРМАЦИЯ БЕЗ ОПАСНОСТИ

АНДРЕЙ МОСКАЛЕНКО

Новые технологические тренды — виртуализация, мобильность, облачные технологии — не только открывают перед компаниями новые возможности, но и создают дополнительные угрозы для корпоративных ИТ-систем. О том, что происходит сегодня в российском сегменте средств и услуг в сфере информационной безопасности, «Бизнес-журналу» рассказали ведущие игроки этого рынка.

Информационная безопасность (ИБ) — по-прежнему наиболее динамично развивающийся и кризисоустойчивый сегмент российского ИТ-рынка. Даже по итогам непростого 2014 года, по оценкам J'son & Partners Consulting, он смог вырасти в номинальном рублевом выражении на 13%, до 51 млрд рублей.

«Спад в экономике наш рынок всегда переживал спокойнее других, — говорит управляющий директор «Лаборатории Касперского» в России, странах Закавказья и Средней Азии Сергей Земков. — На информационную безопасность компании продолжают тратить даже в самые трудные времена, поскольку экономия в этом вопросе может стать причиной инцидентов с тяжелыми последствиями для деятельности компании. К тому же сфера ИБ сильно зарегулирована; внедрение защитного ПО — в некоторых случаях требование законодательства». Поэтому, как ожидает эксперт, в 2015-м продажи ИБ-продуктов в России как минимум останутся на уровне прошлого года, а возможно, даже немного подрастут.

ИТ-ЗАМЕЩЕНИЕ

Политическое и экономическое давление на Россию возрастает с середины 2014 года, однако последствия этого для российской ИТ-отрасли нельзя называть негативными.

Во-первых, по мнению Сергея Земкова, ситуацию несколько выравнивает взятый курс на импортозамещение: российские ИТ-компании ищут и находят новые рынки сбыта и заказчиков внутри страны. Отечественный продукт уже и так широко представлен во многих сегментах — от бухгалтерских и учетных систем до геоинформационного ПО. А если в госзаказе будет сделан больший акцент на отечественные ИТ-решения, то это сильно поддержит бизнес разработчиков и системных интеграторов.

Во-вторых, ослабление рубля и санкции Запада сделали решения западных вендоров более дорогими и менее доступными, так что наши заказчики начинают присматриваться к отечественным аналогам.

По словам директора департамента по маркетингу и продуктовому направлению NGS Distribution Владимира Емышева, многие западные вендоры ввели «санкционные списки» в отношении крупных российских госкомпаний. Основанием

КИБЕРУГРОЗЫ В ЦИФРАХ

Источник: исследование «Информационная безопасность бизнеса 2014» (B2B International для «Лаборатории Касперского»)

98%

РОССИЙСКИХ КОМПАНИЙ В 2014 ГОДУ ТАК ИЛИ ИНАЧЕ СТАНОВИЛИСЬ ЖЕРТВАМИ ДЕЙСТВИЙ ВНЕШНИХ ЗЛОУМЫШЛЕННИКОВ В ИНТЕРНЕТЕ

87%

КОМПАНИЙ СТАЛКИВАЛИСЬ С УМЫШЛЕННЫМИ ИЛИ НЕУМЫШЛЕННЫМИ НАРУШЕНИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СО СТОРОНЫ СОБСТВЕННЫХ СОТРУДНИКОВ

25%

КИБЕРАТАК НА КОМПАНИИ ЗАКАНЧИВАЛИСЬ ПОТЕРЕЙ ДАННЫХ

24%

ТАКИХ ИНЦИДЕНТОВ ПРИВЕЛИ К ПОТЕРЕ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

20 МЛН Р

СРЕДНИЙ РАЗМЕР ФИНАНСОВОГО УЩЕРБА ДЛЯ КРУПНЫХ КОМПАНИЙ В РЕЗУЛЬТАТЕ ОДНОЙ КИБЕРАТАКИ

для включения в список порой служило изображение военного корабля или вертолета на сайте организации. Госзаказчики же приняли ответные меры. Минкомсвязи РФ, к примеру, утвердило план по импортозамещению и назначило госкорпорацию «Ростех» ответственной за его реализацию. Многие долгосрочные проекты, предполагавшие использование оборудования и ПО западных вендоров, были либо отменены совсем, либо заморожены на время подбора аналогов. В такой ситуации на первый план вышли отечественные производители и вендоры из дружественных нам стран — прежде всего Израиля и Китая.

— Поддержка отечественного производителя — полезная практика, но только если взвешенно подходить к ее реализации, — считает глава представительства ESET в России и СНГ Денис Матеев. — Она действительно нужна, когда зарубежный продукт является монополистом и не имеет локальной альтернативы. Другое дело, когда в отрасли и без того есть здоровая рыночная конкуренция — как, например, на рынке антивирусного ПО. В таком случае важно не лишать клиентов возможности выбора качественного продукта.

«Западные технологии и программные продукты широко используются в различных сферах деятельности, и многие из них просто нечем заменить», — добавляет эксперт проекта «Контур-Безопасность» компании «СКБ Контур» Вадим Галлямшин. При этом, по его мнению, сейчас есть несколько трендов, которые могут существенно изменить рынок ИБ. Это создание собственных продуктов на базе программного обеспечения с открытым исходным кодом (open source) и переориентация на продукты и технологии, созданные в странах, которые не поддержали санкции в отношении России. Например, сейчас можно наблюдать, как активно продвигаются на российском рынке корейская СУБД Tibero и другие аналоги продуктов американской Oracle. Определяющее значение имеет и деятельность регулятора. Минкомсвязи РФ подготовило проект постановления, в котором сформулированы критерии отнесения ПО к отечественному, правила формирования и ведения реестра такого ПО, а также преференции при госзакупках для ПО, внесенного в реестр.

«Да, мы видим, что государство движется в этом направлении, но должны признать, это пока только начало пути, — говорит исполнительный директор компании InfoWatch Всеволод Иванов. — Реализованных проектов по замене иностранных продуктов на отечественные пока практически нет».

Справедливости ради стоит сказать, что государство и до введения санкций выступало драйвером развития российского рынка ИБ. По мнению коммерческого директора компании «Аванпост» Александра Санина, одна из тенденций, которые можно отнести к доминирующим в области ИБ в стране, — это разворот регулирующих органов лицом к потребителю. За последнюю пару лет, к примеру, ФСТЭК России выпустила целый ряд нормативных документов в области ИБ. Были серьезно структурированы требования к защите персональных данных.

СЕРГЕЙ ЗЕМКОВ

УПРАВЛЯЮЩИЙ ДИРЕКТОР «ЛАБОРАТОРИИ КАСПЕРСКОГО» В РОССИИ, СТРАНАХ ЗАКАВКАЗЬЯ И СРЕДНЕЙ АЗИИ

С точки зрения технологий рынок информационной безопасности продолжает идти в сторону комплексных решений, которые обеспечивают защиту данных компании во всех аспектах ее деятельности, имеют централизованное управление, удобны и экономичны. Наиболее востребованные направления — решения для защиты виртуальных сред, а также связанные с защитой и управлением мобильными устройствами. Поэтому «Лаборатория Касперского» создала и развивает комплексную платформу Kaspersky Security для бизнеса. Другое направление, которое мы сейчас активно развиваем, — Kaspersky Fraud Prevention. Это специальное решение, которое предназначено для банков и позволяет им максимально защищать от мошеннических транзакций не только сами банки, но и их клиентов. Наше решение обеспечивает защиту как от зловредных приложений, так и от фишинга, а также позволяет распознавать нестандартное для пользователя поведение на пользовательском устройстве.

СЕРГЕЙ ВЯЗАНКИН

SENIOR PRODUCT MANAGER КОМПАНИИ «ИНТЕЛЛИН»

Информационная безопасность остается областью, которую приходится хотя бы в минимальных объемах финансировать даже в самые трудные времена. Потому что, с одной стороны, некоторые системы компании вынуждены иметь для соответствия требованиям законодательства, а с другой — полный отказ от систем ИБ может стать причиной значительных убытков. По крайней мере, никто из наших клиентов пока не рискует отказаться от услуги системы Antifraud (защита от мошеннических действий или так называемого фрода). И это понятно: даже для среднестатистической компании, имеющей лишь 200 соединительных линий, ущерб за каждый час своевременно не выявленного и не пресеченного фрода может стоить до 5,5 млн рублей.

ПЕРИМЕТР ОБОРОНЫ

Наиболее яркие тренды последнего времени в сфере ИТ — это развитие облачных сервисов и технологий совместной работы, виртуализация и BYOD[1]. Как и во всем мире, российские компании, специализирующиеся на информационной безопасности, ищут ответы на вызовы, которые возникают в связи с этим. «Построение периметра безопасности в подобных распределенных информационных системах требует новых подходов к обеспечению ИБ, — отмечает специалист по информационной безопасности компании DataLine Вячеслав Вовкогон. — В этих новых реалиях необходимо соответствовать отраслевым российским и международным стандартам». А стандартов в этой области немало: PCI DSS, ISO/IEC 27001:2013, требования Банка России и др.

«И у нас, и за рубежом все чаще можно услышать об «анализе в облаке» и «облачных сервисах анализа угроз», — говорит эксперт компании «Информзащита» Юлия Дороничева. — Однако отечественный бизнес, в отличие от американского и европейского, не спешит доверять облачным сервисам».

По словам Всеволода Иванова из InfoWatch, облачные технологии широко применяются в области антивирусов и защиты от внешних угроз, но при этом российские заказчики (особенно это характерно для госсектора) пока остерегаются передавать «чувствительную» информацию о клиентах и сотрудниках в облако. «Конфиденциальность информации и контроль доступа к ней становятся важным вопросом при размещении критических сервисов в облаке, — соглашается с коллегой Сергей Земков («Лаборатория Касперского»). — Речь идет о корпоративной почте, CRM, бухгалтерских системах». Крупных корпоративных заказчиков можно разделить на два больших класса. К первому относятся компании, работающие с персональными данными и гостайной. Передача данных вовне у них сильно регламентирована, а нередко попросту запрещена. Иногда такие компании не доверяют даже каналам голосовой телекоммуникации, выдвигая требования к шифрованию трафика мобильных операторов. Второй класс — это организации с внутренними требованиями информационной безопасности и регламентами. Среди них есть немало таких, которые активно пользуются облачными услугами.

Безопасность облачных сред действительно беспокоит российские компании все больше и больше, и это напрямую связано с усилением проникновения технологий виртуализации и построения облаков в ИТ-инфраструктуру компаний. Так, по данным исследования «Лаборатории Касперского», в отечественных компаниях виртуализация даже более популярна, чем в среднем в мире: 56% из них уже используют серверную виртуализацию, еще 8% планируют ее внедрение в течение ближайшего года. Виртуальные рабочие станции уже внедрили в четверти компаний, а еще 14% планируют сделать это в ближайшее время. С вопросами же защиты дела обстоят чуть хуже: пока лишь 18% российских компаний приняли все меры по обеспечению информационной безопасности

1 *Аббревиатура от англ. bring your own device — «принеси свое собственное устройство». Ею обозначают корпоративную политику, которая позволяет сотрудникам использовать для работы личные устройства (ноутбуки, смартфоны и т. д.), в том числе для доступа в корпоративную сеть.*

облачных сред, в то время как в 65% организаций защита внедрена частично, а 14% вообще пока об этом не задумывались.

«Облачный тренд проявляет себя двумя способами, — продолжает тему директор по развитию бизнеса центра информационной безопасности компании «Инфосистемы Джет» Евгений Акимов. — Первый способ — это когда ИТ-системы уходят в облака и им требуется информационная безопасность, учитывающая специфику облачного оказания услуг. Второй — когда уже сами безопасные сервисы работают из облака. С точки зрения количества реализуемых проектов первый метод не вполне оправдал ожидания участников рынка, зато второй — превзошел». Этот сегмент действительно сейчас очень активно развивается. Фактически заказчики обращаются к облачным ИБ-сервисам, понимая, что у них нет возможности решить задачу своими силами. Причины разные — от нехватки квалифицированных специалистов до необходимости оптимизировать расходы. Хороший пример — задача по мониторингу угроз и обработке инцидентов. Этим необходимо заниматься в режиме «24 часа в сутки 7 дней в неделю», однако компаний, которые могут позволить себе держать дежурную смену в таком формате, по словам Евгения Акимова, лишь единицы. Другой пример — защита сайта и веб-приложений, которая требует похожего режима работы. Обновление сайтов до новой версии иногда происходит за считаные часы. За это время, например, ритейлер средней руки не в состоянии собственными силами переконфигурировать систему безопасности. Поэтому правильнее и эффективнее отдать эту функцию на аутсорсинг.

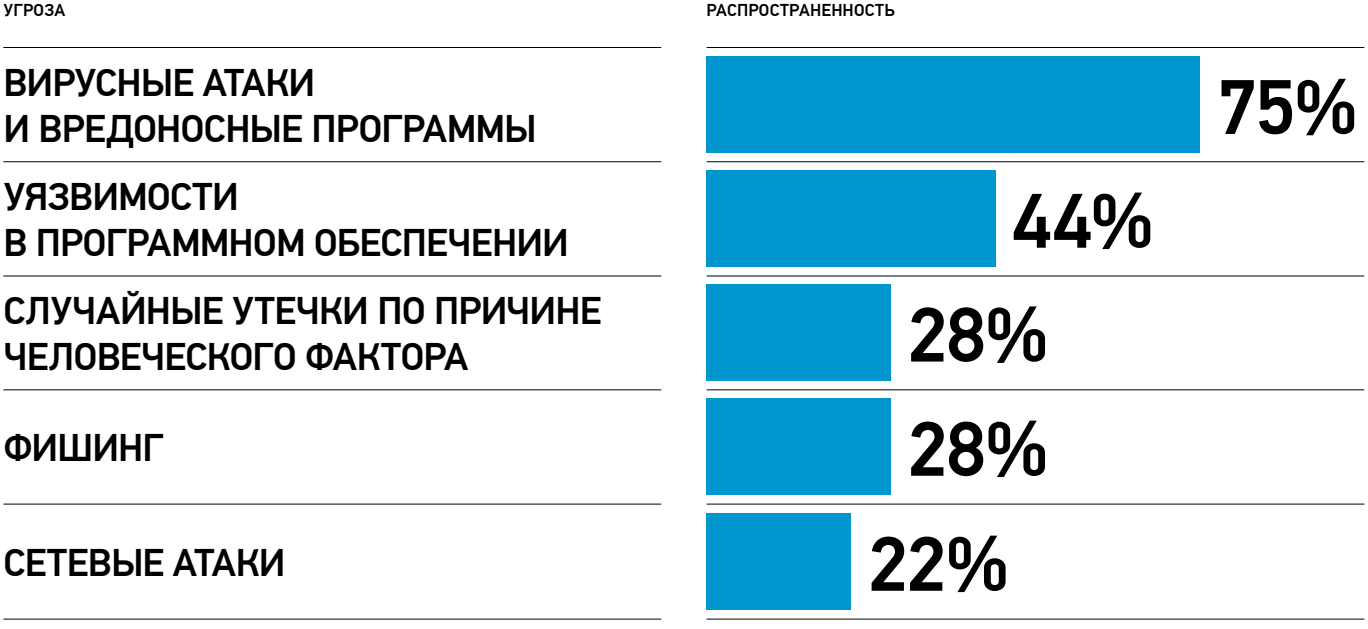
Такое новое веяние, как BYOD, также создает немало проблем. Хотя бы потому, что периметр корпоративной безопасности приходится увеличивать, включая в него личные устройства сотрудников, используемые для работы. Доступ к корпоративным данным открывается для самых разных устройств (смартфоны, планшеты, компьютеры) самых разных производителей и с самыми разными операционными системами. «Такой «зоопарк устройств» — очевидная угроза безопасности компании, — говорит Денис Матеев (ESET). — Разумеется, сотрудникам можно запретить пользоваться привычными устройствами, однако это ухудшит их продуктивность. Лучше обеспечить защиту от киберугроз и несанкционированного доступа».

ПРИКРОЙ, АТАКУЮТ!

За 2014 год число компаний, подвергшихся сложным таргетированным атакам, возросло в 2,4 раза; более 4,4 тыс. организаций по меньшей мере в 55 странах мира стали целью киберпреступников. Такую неутешительную статистику приводят эксперты «Лаборатории Касперского».

Если говорить о России, то, по мнению Евгения Акимова, большинство отечественных компаний даже не в состоянии противостоять целенаправленным кибератакам. «Хакеры объединяются в преступные группировки с узкопрофильной специализацией, имеют все необходимые ресурсы и прово-

ТОП-5 КИБЕРУГРОЗ ДЛЯ МАЛОГО И СРЕДНЕГО БИЗНЕСА



Источник: «Лаборатория Касперского»

дят целенаправленные атаки на бизнес с целью незаконного хищения средств, — говорит Владимир Емышев (NGS Distribution). — Сами атаки становятся комбинированными и многовекторными. Для их осуществления применяются уязвимости нулевого дня и технологии социальной инженерии, от которых очень трудно защититься». «Криминал все больше уходит в цифровое пространство, — соглашается директор по развитию бизнеса Check Point Software Technologies Дмитрий Титков. — Кроме того, все чаще приходится иметь дело с таким явлением, как «хактивизм» — когда люди совершают киберпреступления по идейным соображениям (например, исходя из своих политических взглядов)».

Угрозы безопасности компании могут быть и внутренними, связанными с умышленными или неумышленными действиями собственных сотрудников. При этом, по оценке Всеволода Иванова (InfoWatch), решения по защите от внутренних угроз внедрили не более 10% компаний. А решения по защите от целенаправленных атак тоже до сих пор воспринимаются как экзотика, несмотря на лавинообразный рост таких угроз. В этом случае на острие атаки оказываются в первую очередь банки и госучреждения. «Проблема в том, что компании просто не осознают, сколько средств они смогут сохранить при внедрении подобных решений, — уверен эксперт. — Весь российский рынок решений для защиты от целенаправленных атак пока меньше ежедневных потерь банков от воровства, мошенничества, коррупции, атак на системы дистанционного банковского обслуживания».

Как бы то ни было, именно банки предъявляют самый большой спрос на решения и услуги в области ИБ. Следом идут телекомы и крупные компании из нефтегазового сектора, энергетики и промышленности. Это обусловлено участившимися атаками на них с целью выведения систем из строя и промышленного шпионажа. Пристальное внимание ИБ, отмечает Всеволод Иванов, стали уделять и государственные структуры: при них создаются целые киберотряды для борьбы с внешними агрессиями и защиты суверенитета страны на просторах Всемирной паутины.

В свою очередь, Евгений Акимов полагает, что все больший интерес к продуктам ИБ будут проявлять крупные сетевые ритейлеры, чей бизнес все сильнее зависит от интернет-технологий. Тем более что в их случае инвестиции в безопасность дают более заметную отдачу даже по сравнению с компаниями из финансового сектора. Как подсчитал эксперт, каждые пять рублей, инвестированные в безопасность банка, за год позволят не потерять шесть, а в ритейле — десять.

«В целом же усредненный уровень защищенности российских предприятий довольно низок, — подчеркивает Александр Санин («Аванпост»). — Значительная часть предприятий все еще живет по принципу «Делаем только то, что требуется в обязательном порядке». А такой подход вряд ли может обеспечить высокую степень информационной безопасности». «Большинство компаний ограничивается созданием двух–трех уровней автоматизации: подключенной к сетям общего до-

ЕВГЕНИЙ АКИМОВ

ДИРЕКТОР ПО РАЗВИТИЮ БИЗНЕСА ЦЕНТРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ «ИНФОСИСТЕМЫ ДЖЕТ»

Наибольший бизнес-эффект в сфере информационной безопасности могут дать решения по противодействию мошенничеству, особенно для крупного ритейла. Мы, например, давно создаем процедуры в области противодействия кассовому мошенничеству, а в последнее время стали распространять их на логистику и складское хозяйство. Многие схемы обмана типичны и легко отслеживаются. Например, недобросовестный кассир обсчитывает покупателей, складывая «излишки» в кассу, с тем чтобы после окончания смены их каким-то образом «изъять» и положить в карман. Как это сделать, если касса открывается только при проведении операции продажи? Разумеется, продав самому себе что-нибудь — например, 10 граммов картофеля стоимостью копеек пятьдесят. Эффективные антифрод-системы отслеживают и анализируют в том числе и подобные «странные» операции и помогают зафиксировать момент выемки денег из кассы. Дальнейший сценарий таков: сотрудник службы экономической безопасности ритейлера получает оповещение и может уделить более пристальное внимание конкретному фрагменту видеозаписи с камеры наблюдения.

Мошеннические схемы в логистике имеют свои особенности, но и там, контролируя ряд параметров бизнес-процесса, можно их успешно выявлять. Например, движение погрузчика на складе имеет вполне определенную траекторию, и если она вдруг меняется, то это сигнализирует о том, что часть груза могла «уйти на сторону».

7%

В ОБЩЕМ ОБЪЕМЕ РОССИЙСКОГО ИТ-РЫНКА ЗАНИМАЕТ СЕГМЕНТ СРЕДСТВ И УСЛУГ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ступа, служебной и обрабатывающей те или иные сведения, определенные государством», — дополняет генеральный директор компании «НТЦ ИТ РОСА» Аркадий Тагиев.

МАЛЫШЕЙ НЕ ОБИЖАТЬ

По итогам прошлого года «Лаборатория Касперского» провела исследование киберугроз и масштаба последствий киберпреступлений для российских компаний малого и среднего бизнеса (МСБ). Согласно полученным данным, в случае успешной атаки предприятие теряло в среднем 780 тыс. рублей за счет вынужденного простоя, упущенной прибыли и расходов на дополнительные услуги специалистов. По сравнению с 2013 годом сумма потерь выросла на 64%. Большой средний ущерб от инцидента объясняется, в частности, тем, что успешные атаки дали злоумышленникам доступ к внутренней рабочей информации в 42% компаний: это включает в себя детали бизнес-процессов, электронную почту и прочие данные. А у 34% были похищены персональные данные клиентов. Исследование показало, что 98,5% компаний (то есть почти все!) как минимум раз в течение года имели дело с внешними угрозами, а 82% — с внутренними.

Если бы не усилия регуляторов (такие как требования по защите персональных данных), малые и средние компании попрежнему уделяли бы недостаточно внимания вопросам ИБ, считают на рынке. Руководитель офиса «Технологии Защиты Информации 7000» компании «Первый БИТ» Сергей Иванов утверждает, что основной фактор роста интереса к кибербезопасности — это «практически насильственно введенное» требование использовать при взаимодействии с министерствами, ведомствами и системами госзакупок электронную цифровую подпись, а также смарт-карты и USB-ключи.

Зато облачные технологии малый и средний бизнес использует все активнее, причем по собственной инициативе. «Вместо создания собственных серверных группировок и внедрения неподъемных для своего бюджета DLP-решений малый и средний бизнес начинает работать с данными в облаках, — поясняет Сергей Иванов. — Физически их обработка проходит вне офиса, обмен информацией контролируется владельцем. Эти решения популярны благодаря тому, что при должном уровне информационной безопасности недороги на стартовом этапе, масштабируемы и удобны в эксплуатации. Но при таких решениях вопрос защиты доступа встает наиболее остро. Видимо, именно поэтому мы отмечаем рост интереса представителей МСБ к средствам усиленной авторизации — смарт-картам, токенам, генераторам одноразовых паролей».

По мнению Евгения Акимова («Инфосистемы Джет»), за последние два–три года заказчик значительно изменился — стал грамотнее: «Раньше мы приносили бизнесу интересные идеи, и далее на основе нашего экспертного опыта и условий конкретной компании формировались требования к разворачиваемому решению. Сейчас бизнес уже понимает, что конкретно ему нужно, и очень четко ставит задачу интегратору. Раньше сектор МСБ ограничивался антивирусами и простейшими системами, а сегодня стал интересоваться решениями, обеспечивающими противодействие утечкам, централизованное управление правами доступа и инцидент-менеджмент». БЖ