телекоммуникации

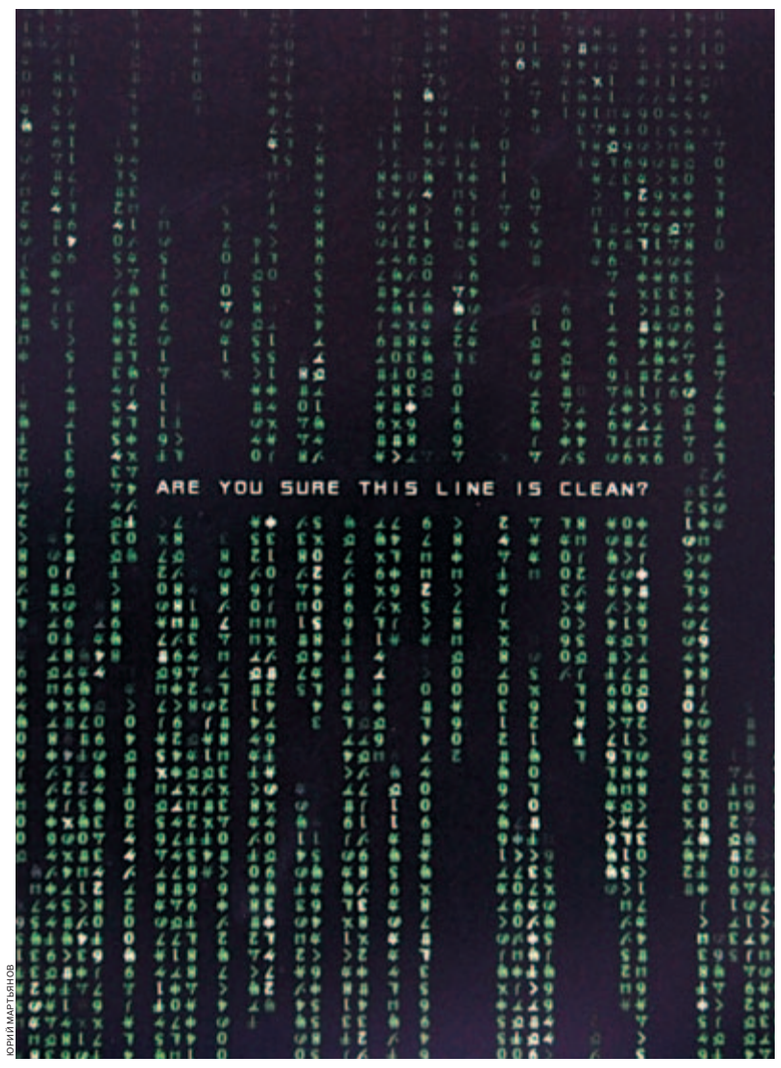
Постсноуденовская безопасность

Сегмент информационной безопасности — один из немногих оставшихся на ИТ-рынке, который продолжает показывать рост. Киберпреступность эволюционирует, вместе с ней приходится развивать и технологии защиты, менять подходы к информационной безопасности бизнеса, подстраиваться под новые угрозы и, главное, переходить от «бумажной» безопасности к реальным превентивным стратегиям защиты.

— правила игры —

По оценкам Gartner, бизнес во всем мире потратил на информационную безопасность (ИБ) в 2015 году $75 млрд, что на 4,7% больше, чем годом ранее. В то же время мировой ИТ-рынок снизился на 5,8%. В РФ ситуация выглядит похоже, если учесть разницу в объемах и курсах валют. На фоне падения всего рынка информационно-коммуникационных технологий (ИКТ) сектор информационной безопасности можно назвать одним из самых перспективных. В марте аналитики IDC пересмотрели прогноз на 2016 год по рынку ИКТ в целом, заявив, что его падение составит порядка 13%, тогда как ранее ожидалось незначительное сокращение его объемов. На прошедшей в сентябре конференции по информационной безопасности IDC IT Security Roadshow 2016 старший аналитик IDC по направлению ИБ Денис Масленников сообщил, что в первом полугодии 2016 года рынок аппаратных решений для обеспечения ИБ вырос в долларах на 26,8% по сравнению с первым полугодием 2015 года и составил $68 млн. По его мнению, положительная тенденция сохранится.

Андрей Янкин, руководитель отдела консалтинга Центра информационной безопасности компании «Инфосистемы Джет», говорит, что в целом тенденции на рынке ИБ в России те же, что и на мировом, хотя и существует задержка в один-два года, но она уменьшилась: раньше мы отставали на четыре-пять лет. По его словам, общие для всего мира проблемы — целенаправленные атаки, защита вебресурсов, в том числе от DDoS-атак. «В России можно выделить также тенденции замены систем ИБ в рамках импортозамещения, но их уже нельзя считать уникальными, так как в постсноуденовскую эпоху многие государства задумались об этом»,— добавляет господин Янкин. Кирилл Керценбаум также видит рост интереса к отечественным решениям в сфере ИБ на волне импортозамещения. Регулятор продолжает воздействовать на рынок ИТ и через него на сегмент ИБ также путем обновления российского законодательства. Так, «закон Яровой» может повлиять на рынок строительства новых дата-центров, объем поставок систем хранения данных и другого оборудования, а также повлечь рост спроса на решения в области сетевой безопасности, включая межсетевые экраны, анти-DDoS системы и пр.



ЮРИЙ МАРТЬЯНОВ

Одна из особенностей российского рынка информбезопасности – рост средней стоимости ущерба от кибератак

Как говорит Дмитрий Огородников, директор Центра компетенций по информационной безопасности компании «Техносерв», именно в сильном регулировании заключается принципиальное отличие российского рынка от общемирового. «Технологически это выражается в использовании некоторых уникальных решений, как-то средств АПМДЗ (аппаратный модуль доверенной загрузки. — „Ъ“) или отечественных криптоалгоритмов ГОСТ 28147-89 и последующего ГОСТ Р 34.12-2015. Законодательно это выражается в большом объеме различных руководящих документов в области защиты информации, которые по последним планам Федеральной службы по техническому и экспортному контролю (ФСТЭК) должны обновляться каждые три-четыре года,— объясняет он.— С другой стороны, наш рынок ИБ менее зрелый и многие процессы или технологии, которые на западном рынке уже широко используются, на нашем только делают первые шаги. Например, в этом году мы стали активного говорить о подходе Agile, о процессах ИБ и о решениях класса User and Entities Behavior Analysis (технологии анализа поведения пользователей и процессов в корпоративных системах на основе искусственного интеллекта. — „Ъ“)».

«Бумажная» безопасность подорожала

Еще одна из отличительных особенностей российского рынка ИБ, по словам ведущего эксперта направления ИБ компании КРОК Евгения Дружинина,— существенный рост средней стоимости ущерба от инцидентов. Так, в 2015 году по данным IDC она выросла почти в полтора раза, в то время как на мировой арене этот показатель уменьшился на 5%. Это заставляет бизнес более тщательно работать над стратегиями защиты, привлекать внешних специалистов. Соответственно, серьезный рост показывает сектор услуг в области ИБ. Господин Янкин комментирует: «Если с «железом» у нас все более или менее неплохо, то в области выстраивания процессов ИБ и встраивания их в бизнес наблюдается явное отставание. Консалтинг в области ИБ в коммерческом секторе показывает хороший рост, но во многом это эффект низкой базы. Интересная тенденция на рынке ИБ, к которой скептически относились многие эксперты еще три-четыре года назад,— это существенный рост рынка аутсорсинга, как качественный, так и количественный. В целом рынок ИБ в России бурно развивается даже в условиях экономического спада».

Евгений Дружинин также видит тенденцию по смещению акцентов в сторону услуг, включая аутсорсинг ИБ и облачные сервисы типа Security as a Service (SECaaS). «Заказчики все активнее ищут помощи внешних подрядчиков в вопросах выстраивания контура безопасности. Например, спрос на облачные сервисы растет, а вместе с этим формализуются и требования к их безопасности. Например, услугу Security as a Service крайне желательно выстраивать на базе сертифицированных ФСТЭК и ФСБ средств. Как раз таким сервисом мы сейчас защищаем ряд IaaS-сервисов, арендуемых в нашем публичном облаке автомобильной компанией. Защита реализуется в соответствии с индивидуальной моделью угроз заказчика и с учетом требований 152-ФЗ»,— говорит он.

Из-за того, что последствия кибератак становятся все более разрушительными, бизнес стал более внимательно относиться к защите. Господин Янкин говорит, что от формального выполнения требований регуляторов и отношения к ИБ как к некоторой экзотике бизнес перешел к восприятию рисков ИБ как к будничной и неотъемлемой части использования ИТ-технологий. «Конечно, в этой области все еще сохраняется правило о том, что пока гром не грянет, мужик не перекрестится, но гром стал греметь так часто и так у многих над головами, что большинство зрелых компаний перешли к плановому обеспечению ИБ, а не латанию дыр после инцидентов. Это приводит к росту роли ИБ в компаниях, выведению подразделений ИБ из-под ИТ или СБ в отдельные независимые структуры с мощными контрольными функциями, собственными бюджетами, дифференциацией персонала»,— говорит он.

Кирилл Керценбаум, менеджер по развитию бизнеса «Лаборатории Касперского», добавляет, что в связи с сокращением или оптимизацией бюджетов на ИБ российские компании стали уделять внимание более интенсивному использованию уже внедренных средств защиты, а не массовой закупке новых. В связи с этим и наблюдается рост спроса на сервисы Security & Threat Intelligence (интеллектуальные услуги по предотвращению угроз), которые позволяют повысить эффективность процессов ИБ за счет более качественной организации процессов мониторинга защищенности инфраструктуры. А также растет спрос на аудит безопасности, тесты на проникновение, данные по актуальным угрозам и услуги SECaaS, которые позволяют оптимизировать расходы на ИБ за счет аутсорсинга крупных инфраструктурных решений на сторону сервис-провайдера. Из этой категории услуги по защите от DDoS-атак — антивирусные решения по подписке, защита от взлома и т. д.

Михал Салат, ведущий вирусный аналитик Avast Software, добавляет: «Простого антивируса уже недостаточно для обеспечения корпоративной информационной безопасности, нужно использовать несколько уровней защиты, включая антивирус, межсетевой экран, системы обнаружения взломов, регулярное обновление аппаратного и программного обеспечения и надлежащее использование прав доступа сотрудниками. Важно помнить про человеческий фактор. Люди совершают ошибки, и хакеры знают, как их использовать. Поэтому важно, что организации осуществляют новую политику, например устанавливая ограничения на использование документов внутри компании для предотвращения фишинговых атак. Тестовые взломы — это отличный способ узнать слабые места, которые хакеры потенциально могут использовать. Тестирования на проникновение в идеале нужно делать несколько раз в год, так как хакеры постоянно ищут и находят новые способы взлома».

Бизнес реагирует на нарастающие угрозы — с существенным отставанием от развитых стран в России появился интерес к системам автоматического предотвращения мошенничества в ИТ-системах. Как говорят эксперты, сейчас в этой области настоящий бум.

Антон Карданов, руководитель сектора ИБ компании AT Consulting, говорит, что целью злоумышленников сегодня часто являются вебприложения, которые обладают достаточным количеством уязвимостей, позволяющих реализовать такие атаки, как межсайтовый скриптинг (XSS), SQL-инъекции, уязвимости конкретных плагинов. Господин Карданов рекомендует: «Создайте центр мониторинга и реагирования на инциденты информационной безопасности: подразделения, имеющие возможность в режиме реального времени отслеживать защищенность ресурсов и принимать адекватные и соответствующие текущей ситуации меры. Проведите инструментальный аудит практической защищенности ресурсов, он выявит наиболее уязвимые места и сформирует предположение о вероятных атаках. Таким образом, у вас будет заранее спланированный план действий, следуя которому вы сможете быстро восстановить работоспособность системы в случае взлома».

Андрей Бершадский, директор центра компетенции компании Positive Technologies, отмечает, что за последний год стало активнее происходить строительство центров мониторинга и управления информационной безопасностью (SOC). «Именно центры мониторинга начали мирить два противоборствующих лагеря: так называемых бумажных безопасников и ИБ-практиков. Ведь SOC — это люди, регламенты и технические средства. И без правильно выстроенных процессов реализовать практическую составляющую мониторинга и реагирования вряд ли представится возможным. Интерес к SOC подтолкнул интерес к SIEM-решениям (Security information and event management — управление информационной безопасностью и событиями ИБ. — „Ъ“). Многие сильно удивились, что, оказывается, однажды купленный и даже внедренный SIEM на практике не всегда способен решать те задачи, которые стоят перед специалистами SOC. В первую очередь ввиду неспособности оперативно подстраиваться под динамичную инфраструктуру и отсутствия серьезной встроенной экспертизы. Рынок SIEM в России фактически переживает вторую молодость, и вряд ли стоит ожидать его спада, ведь потребности заказчиков давно уже выходят за рамки классического решения SIEM»,— рассказывает он.

В сфере защиты государственных учреждений господин Бершадский видит прогресс: «Сразу несколько ведомств начали создание первых центров ГосСОПКА (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак. — „Ъ“), что должно крайне положительно сказаться на безопасности государственных учреждений и подтолкнет других участников рынка присоединиться к программе».

Мария Анастасьева

Установление робототорговли

— тенденция —

О необходимости цифровой трансформации бизнеса говорят по меньшей мере три-пять лет, но 2016 год становится началом массовой реализации такого подхода, в том числе в России. В нынешнем году тему поднимают под разными углами на самых разных конференциях, организуют новые. Цифровое предприятие — что это за явление и как его построить?

В нынешнем году организаторы известной российской конференции Docflow (что переводится примерно «Поток документов») внезапно переименовали ее в Digital Enterprise («Цифровое предприятие»). 20 лет проект существовал как площадка для обсуждения вопросов автоматизации управления и электронного документооборота, на 21-м году концепция изменилась, и в апреле на конференции поднимались новые темы: стратегии, технологии, практики управления цифровым предприятием. Анна Щепилова, руководитель проекта Docflow, объясняет: «Технологии и рынок вместе с ними развиваются, и, общаясь с заказчиками и активными игроками рынка, мы пришли к тому, что все актуальнее обсуждать опыт не только в рамках одной темы, а смотреть шире. Новые интересные возможности для бизнеса лежат на стыке решений класса ECM, Capture, BPM, BI, интеллектуальной обработки информации и других».

Тагир Яппаров, председатель совета директоров группы компаний «АйТи» и член правления АПКИТ (Ассоциации предприятий компьютерных и информационных технологий), комментирует: «Мы видим, что тренд в сторону цифровой экономики стал вовлекать в себя компании, которые раньше никогда не играли на поле ИТ. Понятие ИТ-индустрии расширяется. Теперь следует говорить о цифровой экономике и ее участниках. В том числе, на мой взгляд, необходимо расширять число членов АПКИТ, вовлекать в ассоциацию также не ИТ-компании».

Не простое, а цифровое

Аналитики Gartner, IDC и Forrester в своих прогнозах на 2016 год и дальше делают акцент на цифровой трансформации. Денис Реймер, вице-президент группы компаний ЛАНИТ по цифровой трансформации, председатель совета директоров компании CleverDATA, призывает определиться с терминологией. По его словам, большинство опросов по всему миру показывают: руководители по-разному понимают словосочетание «цифровой бизнес». «Для меня это новая модель ведения бизнеса за счет умения связать физический мир с цифровыми технологиями»,— говорит господин Реймер.

В стратегии ГК «АйТи» цифровое предприятие — одна из основных концепций, на которые делается ставка. В рамках этой концепции специалисты компании объясняют, есть ли жизнь после ERP. «Следующий виток развития — это цифровое предприятие, которое полностью построено на оцифрованных данных и оцифрованных процессах. К ERP нужно добавлять ECM, BPM, аналитику и вводить правило отсутствия нецифровых данных вообще. В таком предприятии ERP обеспечивает лишь около 30% функций»,— объясняет Тагир Яппаров.

Анна Щепилова добавляет: «Цифровая организация использует информационные технологии в качестве конкурентного преимущества в своих внутренних и внешних процессах. Такой бизнес внедряет технологии для создания новых услуг, повышения производительности, поддержки маркетинга и продаж. То есть, если кратко, это компания, которая так наладила за счет ИТ свои внутренние процессы и взаимодействие с клиентом, что ее продукт начинает создавать для потребителя новый, удобный опыт, граничащий с wow-эффектом. Можно обобщить, таким образом, три сферы, которые должны трансформироваться в организации: внутренняя оптимизация, аналитика и клиентский сервис». Для каких-то компаний, по ее словам, это будет означать использование интернета вещей или «умных» цепочек поставок. Чаще всего неотъемлемой компонентой цифровой трансформации становятся анализ и обработка данных в режиме, приближенном к реальному времени.

Вадим Пестун, управляющий директор Accenture в России, утверждает, что цифровая революция связана с несколькими темами: большие данные, прогнозная аналитика и облака. По его словам, прогнозная аналитика, позволяющая делать правильные выводы, строить обоснованные планы, невозможна без обработки больших объемов данных. Это требует обширных вычислительных мощностей, которые экономически оправданно потреблять из облака. Вадим Пестун отмечает, что сейчас происходят кардинальные изменения на рынке, касающиеся того, кто и как предоставляет данные услуги, рождаются новые альянсы. К примеру, Accenture совместно с Microsoft построили облако Accenture insight, способное получать информацию от клиентов в режиме реального времени с серверов обработки данных и помогать принимать решения, например вырабатывать программу оптимального использования водопроводной сети Лондона. Аналогичное решение работает для компании, управляющей несколькими портами, которые были превращены в автоматизированные. Для производителя лифтов создали систему мониторинга их состояния, чтобы планировать ремонтные работы. В горнодобывающей отрасли у нескольких компаний по такой модели ведется наблюдение за оборудованием.

Кто в лидерах

Аналитики IDC предсказывают, что доля предприятий, проводящих цифровую трансформацию, увеличится с 22% в 2015 году до 50% к 2020 году. В Gartner уверены, что уже в 2025 году все компании станут цифровыми. Согласно Forrester, сейчас всего 27% компаний в мире сформировали полноценную стратегию цифровизации бизнеса. Gartner утверждает, что 125 тыс. крупных организаций реализуют инициативы в этом направлении, а главы этих компаний ожидают, что их «цифровая выручка» вырастет более чем на 80% к 2020 году.

Вадим Пестун отмечает, что цифровая революция происходит не в каком-то конкретном сегменте экономики. В ней сплетаются разнородные индустрии. Происходит межотраслевая конвергенция: банков с телекомом, телекома с производственными компаниями, не остаются в стороне и социальные сети. «У Accenture в Испании есть забавный проект — „цифровая метла“,— рассказывает господин Пестун.— Идея проста: дворник метет улицу метлой с акселерометром, который меряет скорость чистки улицы и соединен по Bluetooth с мобильным устройством в кармане. Городские службы получают информацию о плотности дворников на улицах, их активности. Это одна сторона. Для дополнения картины используются социальные сети, в которых горожан приглашают оставлять отзывы о чистоте улиц. Наиболее активные граждане получают бонусы и купоны на скидки от ритейлеров».

ВАСИЛИЙ ШАПОШНИКОВ

Концепция цифрового предприятия предполагает, что весь документооборот становится электронным

Полностью цифровым бизнесом можно назвать первый в мире «отель-робот» в Японии, обслуживаемый исключительно роботами. Есть уже и банки, автоматически анализирующие кредитную историю человека на основе семантических технологий. По словам Анны Щепиловой, наиболее продвинут цифровой подход в финансовом секторе, рознице и телекоммуникациях: в этих сферах рост бизнеса зависит от качества работы с клиентами, а обеспечить его сегодня сложно без информационных технологий и налаженных операционных процессов. В этом же направлении следуют крупные промышленные холдинги, инвестирующие в развитие производительности за счет ИТ.

Есть интересные примеры и в самой ИТ-отрасли. К примеру, «Яндекс» использует свое решение Data Factory для анализа поведенческих паттернов сотрудников инжиниринговых компаний, имея доступ к статистике, к движению мышки пользователей. Они могут с высокой степенью точности предсказать, когда человек решит увольняться.

Денис Реймер приводит классический пример «цифрового бизнеса» — это Uber и его локальные конкуренты, сервисы доставки товаров и услуг в онлайн-режиме, персонализированные сервисы по обучению и многие другие. По его словам, пока в РФ нет ни одной компании, которая бы полностью трансформировалась из «аналоговой» в «цифровую», но и в мире таких «идеальных» преобразований не существует. «Компании, которые сегодня начинают бизнес с нуля, в первую очередь выстраивают модель вокруг цифровых технологий. В этом плане им намного легче, чем «носорогам», долгие годы вытаптывающим рынок под свои правила».

По мнению Тагира Яппарова, российским компаниям еще очень далеко до того уровня, когда их можно было бы назвать цифровыми предприятиями. «Если зайти в любой офис, там кто-то бегает с бумажками по коридору. Этого вообще не должно быть: все должно быть автоматизировано и структурировано, все документы в электронном виде. Должна быть интеграция не на уровне данных, как мы привыкли, а на уровне процессов. Именно процесс становится интегрирующим элементом между разными информационными системами. Сегодня большинство компаний автоматизированы „кусочно“ — приходится распечатывать документ, подписывать его, бежать к другой системе, там вносить его в базу,— объясняет он.— Если построить единое хранилище документов, автоматизировать процессы в BPM, то на порядок снижаются количество участников бизнес-процессов, временные затраты, количество ошибок». Именно процессная автоматизация — тренд текущего года в России.

Светлана Рагимова