информационные технологии

SEARCHINFORM
INFORMATION SECURITY

«Россия могла бы стать ведущей мировой державой на рынке инфобезопасности»

Рынок внутренней информационной безопасности (ИБ) в России — один из немногих в экономике, которые почти целиком держат отечественные игроки. По качеству работы российским специалистам практически нет равных, более того, Россия могла бы стать ведущей мировой державой в этом секторе, убежден основатель компании «Серч-Информ» **Лев Матвеев**. Сегодня у его команды с 25-летним опытом в IT уже более 3 тыс. клиентов в 17 странах мира, а под защитой флагманского продукта более 2 млн ПК. В интервью „Ъ“ Лев Матвеев рассказал, почему так важно защищать персональные данные, какие меры были бы для этого эффективны, зачем компаниям отдавать вопросы ИБ на аутсорсинг признанным экспертам и для чего России нужен единый регулятор в отрасли инфобеза.


СЕРЧИНФОРМ

— интервью —

— Вы последовательно критикуете власти за их отношение к защите персональных данных. Почему считаете этот вопрос важным?

— Чем больше данных переводится в «цифру», тем критичнее вопросы защиты. Подтверждением служит возможность в даркнете купить что угодно: от сканов паспортов и выписок с банковских карточек до данных одиноких пенсионеров—владельцев квартир. Каждый сталкивается с угрозой стать жертвой мошенника. Скажу за себя. Мне не хочется, чтобы кто-то распоряжался информацией о балансе моей банковской карты. А получить ее мошенникам — на раз-два. Я много путешествую, и в любой российской гостинице сканируют паспорт. Не хочется обнаружить однажды, что по копии паспорта кто-то зарегистрировал на меня фирму-однодневку.

Все переходит в цифру, и это неплохо! Посмотрите только на портал госуслуг: ни в одной стране нет такого удобного сервиса. Но почему при строительстве зданий мы требуем соблюдения правил пожарной безопасности, а IT-инфраструктуру строим без оглядки на ИБ?

— В национальной программе «Цифровая экономика» нет плана по защите персональных данных. Это осознанное решение или так получилось?

— Корень проблемы в том, что у нас нет единого органа-регулятора, который бы создал единые ИБ-правила для всех учреждений и нес ответственность за ИБ страны. А когда нет ответственного, нет и порядка. Я уверен, что такой орган нужен — не важно, как он будет называться: министерство информбезопасности, Росинфобезнадзор при Минцифре и т. д. При этом осознание важности всесторонней защиты персональных данных приходит и к законотворцам, и к простым гражданам. У нас есть предписания по защите от внешних злоумышленников. Но о защите от внутренних угроз просто забыли. Хотя утечек и манипуляций с информацией со стороны сотрудников больше 70% среди всех инцидентов. В основополагающих документах, в стратегиях проблема защиты от внутренних угроз просто упускается. Решение проблемы не стоит триллионов — достаточно направить на ИБ 5–7% от затрат от всей программы цифровизации. У России в сфере ИБ есть преимущество: сильные вендоры, уникальные профессионалы. У нас есть все шансы наладить эталонную защиту данных в стране — было бы желание.

— В чем вы видите уникальность российских ИБ-решений?

— Российские вендоры развивали продукты, отталкиваясь от обратной связи заказчика, в тесном с ним взаимодействии. При этом на заре развития защитных решений в безопасность пришли бывшие сотрудники спецслужб. Это были практики, опытные профессионалы, заточенные на выявление самых сложных инцидентов. Они нам и подсказывали, в какую сторону развивать продукты. Клиент говорит: «Система нас устраивает, но если доделать еще вот это, это и вот это, то мы закупим ее еще на N тысяч компьютеров» — это лучший стимул и развитие именно в том русле, которое нужно заказчику.

В итоге сфера ИБ стала единственным сектором IT-рынка, где даже до импортозамещения общая доля западных вендоров составляла 10–15%. Были Symantec, Forcepoint (ранее Websense), McAfee и т. д. Но, по сути, они не могли по возможностям и функционалу сравниться с отечественными вендорами.

— В начале марта Ассоциация юристов России предложила изменить закон «О персданных»: в случае утечки выплачивать компенсацию потерпевшим от 500 тыс. до 5 млн руб. Насколько потенциально эффективно это предложение?

— Это напоминает сказку, а я не очень верю в сказки. Если введут такие компенсации, компании быстро обанкротятся. Штрафовать надо серьезно, но так, чтобы бизнес мог продолжать работать. В этом плане европейская практика GDPR выглядит логичнее — штраф до 4% от оборота в случае утечки. Установить же единую сумму штрафа неверно. Для одной компании этого будет мало, для второй — слишком много.

— В РФ практика GDPR была бы более эффективной?

— Считаю, да. Если перед компанией встанет дилемма, потратить 5–10 млн руб. на системы защиты данных (DLP, систему файлового аудита и мониторинга баз данных) или получить штраф в условные 20 млн руб., бизнес выберет первый вариант — арифметика здесь проста. А когда вся ответственность — это несколько десятков тысяч рублей, большинству выгоднее заплатить мизерный штраф.

— А как насчет уголовной ответственности для лиц, виновных в утечке персональных данных, которую в феврале предложил ввести зампред ЦБ Дмитрий Скобелкин? Так ли это необходимо, на ваш взгляд?

— Нужно понимать, для кого ее собираются вводить. Если для инсайдера, сливающего данные миллионов людей,— так она уже есть, по статье 183 УК РФ, например. А вот для людей, ответственных за безопасность данных в компании,— руководителей высшего и среднего звена, ИБ-специалистов — уголовная ответственность иррациональна. Проблема должна решаться не громким введением ответственности, а нормальными директивами, чтобы у операторов ПДн не было даже мысли «не защищать данные».

У того же ЦБ множество рычагов, но в их директивах не прописано, что система защиты информации должна стоять на 100% компьютеров в банках, что должны контролироваться все базы данных, файловые системы. Есть только робкие рекомендации в духе «господа, было бы неплохо, чтобы вы защищали информацию». Это как я вам порекомендую: «Было бы неплохо не ехать на красный свет». Но вы можете и поехать со словами: «Я все понимаю, спасибо». Должны быть не рекомендации, а требования и контроль их исполнения.

— Каковы актуальные оценки ущерба, который происходит из-за утечек информации?

— Адекватно оценить можно только явное воровство. Но есть еще сотни других сценариев нарушений по вине инсайдеров: сливы клиентских баз конкурентам, разглашение информации о финансовом состоянии компании, саботаж со стороны деструктивных личностей в коллективе, создание откатных схем и др. Ущерб от всех этих действий посчитать сложнее.

— Как же тогда мотивировать компании закупать защитные решения?

— У меня встречный вопрос: как мотивировать человека поставить на сейф, в котором лежит 1 млн руб., замок за 20 тыс. руб.? Если серьезно, мы всегда предлагаем заказчику протестировать систему в течение месяца. И, увы, не было еще случаев, чтобы программа не выявляла серьезных инцидентов.

При нормально работающей службе ИБ система защиты от утечек (DLP) в среднем окупается в первый год работы. Тут есть важный нюанс: часто организации ставят защитные системы в недостаточном объеме. Например, в банках системы защиты от утечек ставят на 2 тыс. ПК из 10 тыс. Мотивация: «Мы контролируем 10–20% персонала на самых критичных местах». Но это неверная практика. Закрывать парадную дверь, оставляя при этом открытым черный ход и окна заодно,— так себе стратегия. И если вернуться к банкам, подтверждение моим словам — объем данных этих банков, которые лежат в даркнете.

— Вы в последние годы выпустили на рынок несколько новых продуктов. Все же спрос на защитные решения растет?

— Безусловно, компании чаще стали задумываться о безопасности. Мы сосредоточены на защите от внутренних угроз — эту проблему не решить без комплексного подхода. Раньше мы разрабатывали только DLP — главное ПО для защиты от утечек информации и корпоративного мошенничества. Но по мере усложнения процессов, увеличения штата компании, рисков у заказчиков возникает необходимость в других защитных системах. Собственно, их мы и выпустили на рынок.

Это SIEM — система для мониторинга IT-инфраструктуры, анализа событий и уведомления о возникающих угрозах. Система контроля файлов (FileAuditor) — программа, которая классифицирует файлы по содержимому, сигнализирует, если файл оказался у сотрудника, который не имеет права с ним работать, или хранится не там, где нужно. Система автоматического профилирования ProfileCenter, выявляющая группы риска в коллективах,— это тоже работа на упреждение. Еще один продукт, который мы выводим на рынок,— система мониторинга баз данных, которая фиксирует все изменения в БД — добавление, удаление, изменение информации.

Все продукты взаимосвязаны между собой, бесшовно интегрируются, увеличивают эффект друг друга. Например, при мониторинге баз данных выясняется, что подменено поле, оперативное расследование идет в DLP-системе, где мы смотрим, с кем общался виновник инцидента, выясняем мотивы его действия. То есть у ИБ-специалиста на руках оказывается вся информация о происшествии, о задействованных лицах.

Я рад, что в прошлом году мы запустили направление ИБ-аутсорсинга. Сейчас оно как никогда кстати. В России фирмы, в которых 50–200 компьютеров, находятся в замкнутом кругу и не покупают систему информационной безопасности.

— Дорого?

— Для кого-то дорого, но в основном вопрос стоит: «Зачем мне покупать самолет (пусть я даже могу это себе позволить), если я не умею им управлять и у меня нет доверенного пилота? Ну и зачем нанимать пилота, если у меня нет самолета?»

Плюс в маленькую компанию в 50–100 человек не придет суперквалифицированный специалист. А если придет — ему нужно платить немалые деньги. А наши аналитики ИБ все делают вместо клиента: устанавливают софт, мониторят ситуацию, расследуют и отчитываются о том, какие инциденты в компании происходят.

— То есть для СМБ выход — отдать на аутсорсинг вопросы информационной безопасности?

— Да. Аутсорсинг в долгосрочной перспективе может оказаться дороже, чем купить лицензии и нанять штатного сотрудника. Но на короткий срок «попробовать» дешевле. Одно дело — найти условные 2 млн руб., а другое — по 150 тыс. в месяц. Тем более что вопрос не только в деньгах — недостаточно купить софт, если с ним некому работать.

У нас есть прецеденты, когда ряд совсем небедных клиентов, поработав четыре месяца с нашим ИБ-аутсорсингом, отказывался от планов купить лицензии на ПО. Говорят: «Нас все устраивает. Вы же отвечаете за результат, у вас много квалифицированных аналитиков, уволится один — это не наша проблема. Мы готовы за это переплачивать». Услуга оказалась востребованной даже среди тех компаний, где мы не ожидали.

— Вы вносите какие-то коррективы в работу компании из-за сложившейся ситуации с коронавирусом?

— Во внутренней политике мы действуем просто: придерживаемся рекомендаций правительства. Что касается работы с заказчиками, то мы приняли ряд мер. Во-первых, предложили бесплатное расширение лицензий для всех действующих заказчиков, у которых продлена техподдержка. Это сделано для того, чтобы перевод сотрудников на удаленку не ударил по безопасности компаний-клиентов.

Во-вторых, предложили заказчикам помощь наших инженеров с перенастройкой системы под удаленную работу. Составили подробный чек-лист для потенциальных клиентов и максимально его распространили. В-третьих, всем желающим (не клиентам) предложили на выбор — внедрение DLP бесплатно до 1 июня (обычно триал длится месяц) или бесплатно ИБ-аутсорсинг на месяц. Наш специалист возьмет на себя внедрение DLP, работу по выявлению инцидентов, составление отчетов для компании. Все эти меры призваны поддержать отечественный бизнес в условиях экстренного перехода на удаленку.

Кроме того, мы продолжаем работу над оптимизацией продуктов. Понятно, что 2020-й станет для бизнеса не самым легким годом. И для компаний, которые стремятся вкладываться в ИБ, мы стараемся повысить экономическую эффективность вложений. В прошлом году мы увеличили производительность DLP-системы на 30%, это значит, что заказчикам придется меньше тратиться на «железо».

Интервью взял Роман Рожков

Digital в 2020 году: через конфликт к доверию

— экспертное мнение —

Скепсис общества в отношении новейших технологий нарастает. По мнению многих экспертов, хайтек не оправдывает возлагавшиеся на него надежды, а потребители и корпорации снижают ожидания от его дальнейшего развития. Однако факты говорят не столько о прекращении «романа» между цифровым миром и человеком, сколько об изменении формы отношений и их переходе в новую стадию. Специально для „Ъ“ управляющий директор и глава департамента «Технологии, цифровые решения и аутсорсинг» Accenture в России и Казахстане МАРИЯ ГРИГОРЬЕВА рассказала, какую трансформацию переживают взаимоотношения человека и технологий.


ACCENTURE

То, что нужно преодолеть

Несмотря на скепсис, люди сегодня используют технологии больше, чем когда-либо. По данным исследования Accenture Technology Vision 2020, 52% потребителей по всему миру говорят, что цифровые технологии играют важную роль или внедряются практически во все аспекты их повседневной жизни. В среднем современный человек проводит в интернете почти шесть с половиной часов в день. В этом свете текущую ситуацию вместо «техно-отката» имеет смысл называть «технологическим конфликтом». Люди не выступают против технологий в принципе. Более чем из 6 тыс. респондентов Accenture 83% признают, что цифровые технологии стали необходимой частью человеческого жизни (или клиентского опыта).

При этом 70% потребителей ожидают, что взаимодействие с digital продолжит углубляться и будет обретать все более важную роль в их жизни в течение следующих трех лет. Проблема — скорость развития IT-отрасли как таковой. IT-компании и глобальные бренды разрабатывают и внедряют новые технологии по старым шаблонам. Поэтому текущий «техно-конфликт» — это болезнь роста, которую можно преодолеть.

Уже сегодня можно говорить о пяти ключевых направлениях, благодаря которым появляется возможность ослабить существующую напряженность между социумом и технологиями.

«Я» — персонифицированный опыт

Традиционные отношения между бизнесом и людьми меняются. Успешные компании делают упор на человеческий фактор в цифровых инструментах, взаимодействие с аудиторией, создавая двусторонний цифровой опыт. Достаточно посмотреть на Netflix, который в сериале «Черное зеркало» позволяет зрителям прямо по ходу просмотра принимать решения о дальнейшем развитии сюжета.

Этот сдвиг отражает меняющиеся ожидания людей. В такой ситуации становится важным спроектировать «персонифицированный» путь клиента, усиливая роль человека и расширяя свободу его выбора.

Пять из шести опрошенных Accenture (85%) считают, что для успешной конкуренции в новом десятилетии компаниям потребуется перевести отношения с клиентами в формат партнерства. В российских условиях сегодня это наиболее актуальный тренд. Сбор личных данных становится все более агрессивным, людей раздражает, что информацию о них собирают с помощью микрофона или голосового ассистента, а затем бомбардируют предложениями в виде контекстной рекламы.

Социуму необходимо продумывать новые подходы к цифровой безопасности через законодательное регулирование. У людей не должна вызывать отторжения постоянная необходимость предоставлять личные данные, должно быть выгодно делиться ими добровольно.

«Я» и ИИ

Искусственный интеллект (ИИ) сегодня должен рассматриваться в качестве полноценного участника работы, выполняемой человеком, а не служить лишь средством автоматизации. По мере роста возможностей ИИ компаниям важно продумывать задачи и операции, в которых он может стать частью процесса, с учетом ориентации на доверие и прозрачность. В настоящее время только 37% компаний заявляют об использовании инклюзивного проектирования или человекоцентричных принципов сотрудничества между человеком и машиной.

Многие отраслевые лидеры успешно внедрили инструменты и методы искусственного интеллекта, которые ускоряют автоматизацию основных задач в существующих рабочих процессах. Однако истинный потенциал ИИ на предприятии заключается в использовании его в качестве инструмента для совместной работы с людьми: не только для эффективного выполнения задач, но и для преобразования бизнес-процессов.

Это означает, что «умные» чат-боты должны лучше понимать нюансы и возможности, лежащие в основе запроса клиента. Бизнес сможет заново изобретать и постоянно улучшать предложения и опыт, который хотят получить его клиенты. В результате ИИ становится чем-то большим, чем очередной технический инструмент. Он выступает агентом изменений в бизнесе.

В России в этом направлении имеет смысл делать то, что мы хорошо умеем уже сейчас. В стране существует огромный потенциал людей с хорошим техническим образованием: программистов, математиков. Необходимо использовать его для развития и воплощения в жизнь самых продвинутых идей.

Дилемма «умных» вещей

Привычное понимание того, кто является производителем продукта и отвечает перед потребителем за качество товара или услуги, становится не столь очевидным в цифровом мире, входящем сегодня в состояние «постоянной бета-версии». Потребитель не видит разницы между сбоями устройства и его приложений. В то же время плохая работа цифрового устройства может оттолкнуть клиентов и подорвать доверие к бренду.

Положительная сторона развития новых цифровых продуктов в парадигме «вечной бета-версии» очевидна: компании, которые могут реагировать на меняющиеся запросы и ожидания клиентов в режиме реального времени, становятся настоящими партнерами для потребителей.

Ценность их продукта существенно растет, но в шквале постоянных обновлений и изменений запросы клиентов могут оставаться без должного внимания. Компании должны обновить свое понимание того, что означает владение продуктом в постцифровую эпоху, и в результате изменить свою практику.

Тренд не так актуален для России в силу небольшого количества локальных производителей оборудования. Тем не менее уже сейчас необходимо продумывать законодательное регулирование цифровых платформ, чтобы избежать возможных рисков в отношениях с потребителем в будущем.

Роботы «на воле»

Распространение роботов больше не ограничивается пределами склада или завода. С технологиями 5G, способными значительно ускорить развитие этого тренда, компаниям стоит переосмыслить будущее через призму робототехники.

Компании осознали преимущества использования робототехники в контролируемых помещениях. Теперь бизнес смотрит на следующий рубеж робототехники — открытый мир.

Достижения в области датчиков, распознавания речи и компьютерного зрения в сочетании с более низкими затратами на оборудование делают робототехнику более доступной для компаний во всех отраслях промышленности, а развертывание сетей 5G откроет новые возможности за пределами контролируемой среды.

61% руководителей в 20 различных отраслях ожидают, что в ближайшие два года их организации будут использовать робототехнику в неконтролируемых средах. При этом руководители бизнеса и IT-подразделений, опрошенные Accenture, расходятся во мнениях, как их сотрудники воспримут робототехнику. 45% утверждают, что людям будет сложно понять, как работать с роботами, а 55% уверены, что затруднений эти задачи не вызовут.

В России роботизацию уже сейчас используют многие предприятия для работы в тяжелых климатических условиях (добывающая отрасль, металлургия, энергетика и т. д.).

Инновационная ДНК компании

Бизнес имеет доступ к беспрецедентному количеству прорывных технологий: распределенные реестры (блокчейн), ИИ, расширенная реальность и квантовые вычисления. Чтобы понять применимость, суметь управлять этим многообразием и развиваться со скоростью, востребованной рынком, компаниям важно создавать собственную уникальную инновационную ДНК.

Три четверти (76%) респондентов считают, что ставки в сфере инноваций сейчас самые высокие, поэтому требуются новые способы инновационного взаимодействия с партнерами по экосистеме и третьими сторонами.

Компании-лидеры нацелены на человекоцентричный подход — установление баланса (или устранение расхождений) между интересами потребителей и техно-методами, используемыми бизнесом.

Тематическое приложение к газете «Коммерсантъ» («Информационные технологии»). Учредитель: АО «Коммерсантъ». Адрес: 127006, г. Москва, Оружейный пер., д. 41. | **Владимир Желонкин** — генеральный директор АО «Коммерсантъ», главный редактор | **Сергей Вишневский** — руководитель фотослужбы | **Рекламная служба:** Тел. (495) 797-6996, (495) 926-5262 | **Владимир Лавицкий** — директор «Издательского синдиката» | **Роман Рожков** — выпускающий редактор | **Ольга Еременко** — редактор | **Сергей Цомык** — главный художник | **Екатерина Липатова, Галина Кожеурова** — фоторедакторы | **Екатерина Бородулина** — корректор | **Адрес редакции:** 121609, г. Москва, Рублевское ш., д. 28. Тел. (495) 797-6970, (495) 926-3301 | Ограничение: 16+