свести тренд к тезису: „Нет ИБ без цифровой грамотности“»,— подчеркивает господин Кузнецов.

«ИБ-аутсорсинг идет рука об руку с ИТ-аутсорсингом и развитием цифровизации, являясь некоторой формой „налога“ на ИТ и „цифру“. Часто бизнес автоматизирует и развивается быстрее, чем осознает последствия, поэтому, в отличие от ИТ-аутсорсинга, основным драйвером развития являются требования государства, к обеспечению безопасности разных категорий данных. Это ведет к тому, что у владельцев бизнеса и систем, возникает понятие ответственности перед клиентами и государством, а не только чистый бизнес-процесс. Поэтому ИБ-аутсорсинг будет чем-то средним между ИТ и бухгалтерским»,— выделяет тренд руководитель направления по работе с финансовым сектором компании «Информзащита» Денис Сенюков.

ВЗВЕШЕННОСТЬ РЕШЕНИЯ Вызовы последнего времени заставили и крупный, и средний бизнес пересмотреть свои подходы к информационной безопасности, отмечает Руслан Рахметов. По его словам, особенность российского ИБ-аутсорсинга в том, что исторически крупные компании стремились держать свои секреты при себе: нанимали штат безопасников, инвестировали в создание системы ИБ, развивали собственную IT-инфраструктуру. Небольшие и средние компании, как правило, либо вообще не занимались собственной кибербезопасностью, либо возлагали эти задачи на ИТ-специалистов по остаточному принципу.

Сейчас реальность разрушительных кибератак заставила всех игроков обратить внимание на ИБ-компании, которые предлагают создание киберзащиты по аутсорсинговой модели.

Принимая решение выбрать ИБ-аутсорсинг, компания должна тщательно взвесить все за и против, объективно оценить все риски, сценарии реализации угроз и экономическую целесообразность, акцентирует заместитель директора дирекции кибербезопасности IBS Сергей Грачев. Он замечает, что чем крупнее компания и выше уровень зрелости ИТ- и ИБ-процессов, тем должен быть более взвешенный и продуманный подход к аутсорсингу. Концептуальные подходы к таким услугам закрепляются в стратегии развития и внутренних регламентах.

«В случае принятия решения о целесообразности использования аутсорсинга на отдельных сервисах ИБ необходимо как минимум определить перечень процессов и сервисов ИБ, выделить из них критичные, которые в любом случае не подлежат передаче (например, стратегическое планирование, управление доступом к информации, контроль привилегированных пользователей, защита коммерческой тайны)»,— говорит эксперт.

Важно тщательно выбирать провайдера, который сможет предложить прозрачные условия и понятную отчетность, добавляет CEO компании «Облакотека» Максим Захаренко.

Чтобы предотвратить риск попасть в ситуацию, когда качество услуги не соответствует ожиданиям, нужно очень внимательно изучить контрагента, узнать о его партнерах и других заказчиках, возможно, попросить референс от них (это вполне стандартная практика для «чистого на руку» исполнителя). Такой совет дает Алексей Ахмеев, руководитель управления информационной безопасности и цифровизации Moneyman. Стоит внимательно обговорить условия оказания услуги в части соглашения об уровне обслуживания (SLA на сервис) и обязательно наладить контакт между локальным ИТ-подразделением и сотрудниками исполнителя.

РИСКИ ИСПОЛЬЗОВАНИЯ Аутсорсинг информационной безопасности несет определенные риски. «Сторонние ИТ-специалисты нередко становятся причиной утечки конфиденциальной информации, так как для администрирования инфраструктуры, как правило, создается отдельный аккаунт с административными правами. Даже если у внешнего системного администратора нет злого умысла, причиной утечки могут стать неправильно настроенные права доступа. Решить эту проблему помогают PAM-системы, которые могут обеспечить не только мониторинг и запись сессий, но и гибкое управление правами»,— отмечает технический директор ARinteg Максим Деев.

Особенно с осторожностью к ИБ-аутсорсингу нужно подходить банкам и финансовым организациям. «Финансовые организации несут основную ответственность за защиту данных и должны предъявлять высокие требования к подрядчикам, особенно в случаях использования облачных сервисов IaaS, PaaS и SaaS. Обеспечение безопасности на этих платформах требует от провайдеров соблюдения строгих стандартов, особенно если речь идет о сертификации, контроле физического доступа к оборудованию и сегментации данных»,— поясняет Александр Хонин, руководитель отдела консалтинга и аудита компании Angara Security.

По словам эксперта, российский рынок ИБ-аутсорсинга находится в процессе адаптации к этим вызовам, предлагая специализированные решения и усиливая требования к подрядчикам. Однако не все задачи информационной безопасности можно или нужно передавать на аутсорсинг. Например, компании часто предпочитают оставлять управление критическими бизнес-данными и стратегическое планирование ИБ внутри организации, а рутинные задачи, такие как мониторинг и техническая поддержка, передавать на сторону подрядчика.

ЧТО ДОВЕРИТЬ? Начать можно с передачи рутины, рекомендует Алексей Морозков. Например, с поддержки и сопровождения антивирусного решения или какого-то СЗИ, чтобы высвободить ресурсы и направить их на реализацию стратегических задач ИБ. Далее можно уже передавать более серьезные задачи, например, проектирование инфраструктуры ИБ, внедрение комплексных систем защиты. Аудиты ИБ, пентесты, и различные оценки защищенности должны выполняться внешними независимыми организациями, чего требует современные стандарты в области ИБ и регуляторы.

На российском рынке сегодня большое число разнообразных продуктов и услуг в ИБ-сфере, говорит Александр Злой, руководитель службы информационной и коммерческой безопасности ООО «Электрорешения». Предложение достаточно оперативно реагирует на изменения в законодательстве, запросы бизнеса, изменения киберсреды. Усложняющийся ландшафт и масштаб угроз, увеличение количества используемых сервисов и систем автоматизации, рост инфраструктуры и количества пользователей и клиентов стимулируют компании наращивать свой штат и количество средств защиты информации либо обращаться за помощью к внешним провайдерам.

«Все будет зависеть от того, какие задачи ставит перед собой заказчик, будь то снижение затрат или, наоборот, привлечение серьезной экспертизы. Более того, все зависит от того, насколько заказчик доверяет и готов подпустить внешнего поставщика аутсорсинга ИБ к своей инфраструктуре»,— добавляет господин Морозков.

«Я считаю, что внешним исполнителям лучше всего доверять задачи аудита, проведения пентестов, первоначальные настройки сложных и комплексных систем защиты информации, а также малозначимые работы типа обслуживания оборудования. Если есть доверенная компания, то ей можно отдать почти все виды работ»,— делится руководитель Лаборатории стратегического развития продуктов кибербезопасности «Газинформсервиса» Дмитрий Овчинников.

Однако он предостерегает от передачи повседневного контроля за защитой бухгалтерских систем. Подобного рода информация должна оберегаться и не должна покидать юридические рамки компании. «Хотя я надеюсь, что в будущем и этот рыночный тренд станет пережитком прошлого, когда на рынке появится много надежных и проверенных компаний, которые будут дорожить своей репутацией и содержать штат высококлассных специалистов»,— добавляет господин Овчинников.

Эксперт замечает, что особенность отечественного рынка аутсорса в том, что не у всех компаний есть доверие к сторонним ИБ-компаниям. Тех, кто работает на рынке на рынке ИБ свыше десяти лет, не так уж и много, и у них есть устоявшийся пул заказчиков. У молодых компаний нет такой клиентской базы и нет кредита доверия со стороны рынка. Даже внутри компании не всегда полностью доверяют администраторам и специалистам по ИБ. «Это специфика нашей психологии и неразвитости системы контрактов и договорных отношений, которая фактически находится в стадии развития и становления»,— акцентирует Дмитрий Овчинников. ■

В МЕТРО ПО БИОМЕТРИИ

ПЕТЕРБУРГ ПРОДОЛЖАЕТ РАЗВИВАТЬ ЦИФРОВИЗАЦИЮ ОБЩЕСТВЕННОГО ТРАНСПОРТА. В ГОРОДЕ УЖЕ ДЕЙСТВУЕТ СИСТЕМА ЭЛЕКТРОННОГО КОНТРОЛЯ ОПЛАТЫ ПРОЕЗДА, А ТАКЖЕ ЕДИНЫЙ БИЛЕТ (КАРТА «ПОДОРОЖНИК»), РАБОТАЮЩИЙ ПО ПРИНЦИПУ «ЭЛЕКТРОННОГО КОШЕЛЬКА». КРОМЕ ТОГО, ПЕТЕРБУРЖЦЫ ОДНИМИ ИЗ ПЕРВЫХ В СТРАНЕ ПОЛУЧИЛИ ВОЗМОЖНОСТЬ РАСПЛАЧИВАТЬСЯ В МЕТРО БАНКОВСКОЙ КАРТОЙ. ТЕПЕРЬ СОВМЕСТНО С ВТБ БУДЕТ РЕАЛИЗОВАНА НОВАЯ ИНИЦИАТИВА — ОПЛАТА ПРОЕЗДА ПО БИОМЕТРИИ. ВИКТОР ИРИСОВ

В декабре на двух станциях подземки стартует пилотный проект оплаты проезда по биометрии. Планируется, что при идентификации на турникете с помощью биометрии средства будут списываться с привязанной банковской карты любого российского банка. Чтобы воспользоваться новым способом оплаты, нужно зарегистрировать свои биометрические данные в Единой биометрической системе, проще всего это сделать через мобильное приложение «Госуслуги Биометрия» либо через аккредитованные банки или МФЦ, после — зарегистрироваться на специальном портале (интернет-сайте) банка и привязать к аккаунту банковскую карту. Первые терминалы для тестирования системы уже появились на станциях «Гостиный двор» и «Площадь Восстания».

Как пояснил заместитель начальника ГУП «Петербургский метрополитен» Вадим Арсеньев на конференции в пресс-центре «Интерфакса», в пилотном проекте примет участие фокус-группа до 50 человек, в числе которых — сотрудники метрополитена и банка ВТБ. Решение о расширении системы на другие станции метро будет принято в 2025 году по итогам тестирования. В дальнейшем также рассматривается возможность масштабировать технологию на наземный транспорт.

Соглашение о развитии современной платежной системы на общественном транспорте было подписано между президентом — председателем правления банка ВТБ Андреем Костиным и губернатором города Александром Бегловым на ПМЭФ-2024.

«Мы начинаем проект, который сделает проезд в городском транспорте еще более удобным, а его оплату — простой и быстрой. Предложенные ВТБ решения качественно улучшат пользовательский опыт пассажиров за счет усиления роли цифровых каналов. При этом будут использоваться платежные решения на платформе „Транспортный процессинг“. Это собственная разработка банка, позволяющая обеспечить высокий уровень технологического суверенитета»,— отмечал господин Костин на полях форума.

В Москве технология работает с 2021 года. ВТБ отвечает за проведение банковских платежей в московском транспорте, в том числе с применением биометрии. Сервис заработал сразу на всех станциях метрополитена, а в 2022 году — и на МЦК. Сегодня оплатить проезд по биометрии в Москве также можно на регулярном речном транспорте, железнодорожных направлениях аэроэкспресса и четырех станциях московских центральных диаметров. В планах — запуск сервиса на наземном транспорте и подключение всех станций МЦД.



АЛЕКСЕЙ СМАГИН

НА ДВУХ СТАНЦИЯХ ПОДЗЕМКИ СТАРТУЕТ ПИЛОТНЫЙ ПРОЕКТ ОПЛАТЫ ПРОЕЗДА ПО БИОМЕТРИИ

Начальник управления разработки и сопровождения специальных электронных продуктов, старший вице-президент департамента транзакционного бизнеса ВТБ Вадим Изотов сообщил, что с момента запуска сервиса в Москве пассажиры совершили свыше 129 млн поездок, оплаченных при помощи биометрии. В будние дни количество проходов в московском транспорте с использованием такого способа оплаты достигает 160 тыс. Одним из главных преимуществ системы для пассажиров он называет комфорт при оплате: нет необходимости в поисках карты или смартфона, достаточно посмотреть в камеру.

«Технология бесконтактной идентификации, надежная система хранения платежных данных и инновационные технологии ВТБ обеспечат удобство и безопасность платежей. Банк готов участвовать в дальнейшей реализации проекта и масштабировать сервис в петербургском метро в 2025 году»,— говорит Вадим Изотов.

Он также отмечает, что перспективы использования биометрии при оплате проезда будут зависеть от тарифной политики города и продвижения этого способа оплаты проезда среди горожан. ■