государством самому разработчику через налоговые льготы или бюджетные субсидии. Причем размер скидки может варьироваться в зависимости от отраслевой принадлежности покупателя программных решений. Так, если речь идет, например, о муниципальных и районных объектах, которые будет проектировать небольшое региональное бюро, работающее на госзаказе, то скидка может составлять и 90%, почему нет? Так или иначе, это экономия для бюджета. А если ПО приобретают компании из более высокомаржинальных сфер, скажем, представители крупных девелоперов, то скидка может быть меньше, например, 50%. То есть важно дать рынку возможность преодолеть финансовый порог перехода.

G: Над какими программными решениями сегодня работает «СиСофт Девелопмент»? Каковы приоритетные направления для развития?

М. Б.: Наша компания внесла значительный вклад в развитие технологий информационного моделирования в России, и сегодня «СиСофт Девелопмент» занимает на рынке лидирующее место в области бесшовных ТИМ-решений для всего жизненного периода информационной модели. На данный момент мы обладаем самой большой бесшовной линейкой по формированию, а главное, ведению информационной модели: начиная от изысканий и заканчивая архивным хранением. Мы продолжаем укреплять позиции в традиционных для себя нишах, расширяя сферы применения наших программных решений. Они становятся более универсальными и удобными для пользователя. Таким образом, в настоящее время мы являемся лидерами рынка в области проектирования и сейчас активно «заходим» в сферы строительства и эксплуатации.

Надо понимать, что международные BIM-лидеры занимаются общемировыми проблемами BIM. Рынок ТИМ в России идет своим путем, и прошло то время, когда он формировался под западные решения и продукты. Мы уже другие, и требования нашего рынка тоже меняются, поэтому они не будут локализовывать и подстраивать свои продукты под региональные рынки, в частности под российский (который они еще наверняка надеются вернуть под их стандарты и форматы). Западные вендоры сами понимают тупиковость своего подхода и также ищут решения. Поэтому расчет простой: пока разрабатываются новые продукты, держать нас на старых, чтобы исключить уход из-под контроля. Именно поэтому развитие цифровой вертикали и создание бесшовной интероперабельности во всех направлениях — это сегодня задача и для отечественных разработчиков, и для отечественной науки, которой пока нет и которую не заменят разнообразные центры компетенций, действующие каждый по своему разумению.

G: В каком положении оказались отечественные предприятия после ухода зарубежных вендоров?

М. Б.: Сложно сказать однозначно, потому что разные предприятия оказались в разном положении. Те, кто заранее начал процесс перехода — еще до введения санкций,— сегодня чувствуют себя лучше. На них уход зарубежных вендоров оказал меньшее влияние. Те, кто с этим опоздал, находятся в ситуации, когда приходится быстро принимать дорогостоящие и ресурсозатратные решения. А некоторые и вовсе до сих пор ждут возвращения западных вендоров. Это тоже позиция, но, на мой взгляд, не совсем правильная.

G: Как вы полагаете, возвращение в страну западных вендоров положительно отразится на рынке? Как это скажется на вас?

М. Б.: В первую очередь хочется отметить, что компания «СиСофт Девелопмент» была заметным игроком на рынке ТИМ и успешно конкурировала с решениями от Autodesk еще в то время, когда американский вендор работал в России и имел здесь свое представительство. Мы конкурировали и с ним, и с AVEVA, и с Bentley Systems. Поэтому их гипотетическое возвращение на нашем бизнесе никак не скажется. И не только потому, что мы сформировали качественную и понятную пользователям линейку программных решений, но и потому, что ситуация в нашей стране серьезно поменялась. Так, за последние годы был принят ряд документов, главный из которых — указ президента РФ № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации». Очевидно, что для множества российских предприятий и компаний использование западного ПО является очень рискованным и токсичным. И речь здесь идет не только о безопасности информации и ее возможной передаче вовне. Кто может гарантировать, что в определенный момент не повторится ситуация, при которой лицензии западных вендоров перестанут работать? А это может сказаться на сотнях и тысячах аффилированных с огромными корпорациями компаниях, деятельность которых влияет на экономику страны. То есть здесь уже налицо отсутствие доверия. Подчеркну, что самое главное сегодня — это понятная, четкая и последовательная политика государства по отношению к зарубежному ПО. Если нам важна информационная безопасность, то об использовании иностранных решений нужно забыть раз и навсегда.

G: Как изменились цены на отечественные решения за последние годы?

М. Б.: Если мы говорим о нашей линейке Model Studio CS, то она состоит из нескольких программных решений, или комплектов ТИМ: для проектирования строительных решений, трубопроводов, водоснабжения и канализации, вентиляции, электрики и так далее. Таким образом, потребитель может собрать свой собственный набор ТИМ под его нужды — и ничего лишнего не будет входить в его цифровую экосистему, например, для конкретных проектных работ. При этом цены на наши продукты из линейки за последние три года хотя и возросли, но они росли ниже уровня инфляции. За других коллег по отрасли говорить не хочу, но в «СиСофт Девелопмент» ситуация такова.

G: Сталкивается ли ваша компания с дефицитом кадров в сфере разработки?

М. Б.: Дефицит присутствует, но не могу сказать, что мы его сильно ощущаем. Конечно же, нам нужны квалифицированные кадры, поэтому мы на постоянной основе пополняем ряды наших разработчиков. Гораздо более важный аспект — дефицит кадров в тех сферах и отраслях, где работают пользователи наших программных решений. Причем здесь речь идет не только о проектировщиках, которые формируют информационную модель, но и о тех, кто ее впоследствии будет «вести». Приведу пример. Есть два глагола: «формировать» и «вести». «Формировать» — это значит создавать саму модель, собирать двухмерную и трехмерную графику, добавлять в модель атрибутивные данные. А «вести» — это когда в атрибутивные данные уже вносятся изменения. Например, проектировщиком предусмотрена стена, которая оштукатуривается и красится. При строительстве в модель важно внести дополнительные данные о том, какой бригадой выложена кирпичная стена, когда и какой кирпич пришел на стройплощадку и с какого завода, кто штукатурил и кто красил (и какой краской). Здесь происходит распределение обязанностей по ведению информационной модели. Точно, что каменщик, штукатур или маляр не будет вносить эти данные, а может сообщить их, например, нормировщику, а он внесет их в модель. Это будет дешевле и серьезно оптимизирует необходимые ТИМ-квалификации по ведению модели на этапе строительства. И дефицит ТИМ-специалистов на рынке будет намного меньше.

G: Как вы оцениваете подготовку студентов в вузах по направлению ТИМ?

М. Б.: Я оцениваю ее как недостаточную. Отечественные разработчики ПО ТИМ проводят огромную работу для внедрения своего ПО в программы обучения в российских вузах. Например, предоставляют бесплатные лицензии, помогают с разработкой учебных программ и курсов. Но проблема в том, что теоретическая часть в вузах устарела, а в ее основе лежат западные решения и стандарты. И наша нормативная база, как я уже говорил ранее, противоречивая и не позволяет создать научную основу информационного моделирования. Практическую часть мы «закрываем», показываем наши решения, учим, как на них работать. Но студент — строитель, инженер, архитектор — должен знать и теоретическую основу. Таким образом, сегодня образование в сфере ТИМ в России — это птица с одним крылом, «практическим», но без второго, «теоретического». Так она далеко не улетит. ■

НОВЫЙ ВИТОК ЩИТА И МЕЧА

ОСНОВНЫМИ УГРОЗАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В 2025 ГОДУ ОСТАЮТСЯ РОСТ ЧИСЛА КИБЕРАТАК, В ТОМ ЧИСЛЕ СВЯЗАННЫХ С ХАКТИВИЗМОМ, ВИРУСЫ-ВЫМОГАТЕЛИ, ФИШИНГОВЫЕ АТАКИ И МЕТОДЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ, АТАКИ НА ЦЕПОЧКИ ПОСТАВОК ЧЕРЕЗ СКОМПРОМЕТИРОВАННЫХ ПОДРЯДЧИКОВ, ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ, УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И АТАКИ НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. ДВОЙСТВЕННОЕ ВЛИЯНИЕ НА КИБЕРБЕЗОПАСНОСТЬ ОКАЗЫВАЕТ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ. АЛИСА МАЛЬЦЕВА

УДАР ПО КИИ Мониторинг RED Security показал, что в прошлом году было совершено 130 тыс. киберинцедентов, что в 2,5 раза больше, чем в 2023 году. Наибольшее количество кибератак приходится на отрасли критической информационной инфраструктуры (КИИ), включая промышленность, финансовый сектор и телекоммуникации.

«Удаленный доступ к системам управления объектами КИИ, террористические кибератаки на производственные цепочки — все это обратная сторона динамичной эволюции цифрового мира. В настоящее время в нашей стране наблюдается переломный этап, когда масштабы киберугроз осознаны на государственном уровне и закрывать на них глаза не представляется возможным. Начинаются тектонические процессы»,— комментирует управляющий директор по ИБ АО «Росатом автоматизированные системы управления» Евгений Дорофеев.

Эксперт прогнозирует дальнейший рост волны кибератак на объекты КИИ, особенно в крупной промышленности и энергетике. При этом «ахиллесовой пятой» в этих отраслях остается проблема импортозамещения. «Импортное ПО несет в себе риски. В условиях санкций утрачивается возможность его обновления и техподдержки. В отсутствие оригинальных ремкомплектов и запчастей для аппаратной составляющей, а также, при использовании „серого“ импорта гарантийное и сервисное обслуживание становятся недоступны. По мере увеличения доли непроверенного ПО и ПАК разных производителей и поколений усложняется IT-ландшафт, растет неоднородность комплексов и систем ИБ. Возрастает уязвимость и существенно снижается эффективность таких систем. Пристальное внимание на комплексное обновление ПО и ПАК — это первый шаг на пути к суверенитету в киберсреде»,— говорит господин Дорофеев.

В ТРЕНДЕ АТАК Представитель «Информзащиты» Александр Матвеев обращает внимание на увеличение числа деструктивных атак, нацеленных на разрушение информационной инфраструктуры без получения финансовой выгоды. И если в первой половине 2024 года такие атаки осуществляли хактивисты (политически мотивированные, но не всегда профессиональные хакеры), то теперь — профессиональные группировки, хактивистские сообщества. На хактивизм обращает внимание и Антон Антропов, технический директор IT Task.

Также господин Матвеев указывает, что в прошлом году сложился тренд на атаки через третьи стороны, которыми чаще всего выступали подрядчики компаний и партнеры, имеющие доступ к информационной системе компании. «Хакеры начали атаковывать организации с более низким уровнем информационной безопасности, чтобы проникнуть в инфраструктуры жертвы через существующие каналы. Таких атак будет еще больше в 2025 году, мы ожидаем рост как минимум на 50–60%. В-третьих, в этом году вырастет число атак с вымогательством. 59% ИБ-руководителей считают именно их главной угрозой для бизнеса в текущем году. Главной причиной роста количества таких атак является распространение RaaS-платформ — сервисов для злоумышленников, где они могут купить лицензию или получить подписку на вредоносное ПО для ransomware-атак. Мы ожидаем, что количество атак через такие платформы увеличится на 15% в 2025 году»,— рассуждает господин Матвеев.

Согласно исследованиям аналитиков компании «Бастион», свыше 60% успешных кибератак заканчивается утечками данных. «Один из главных факторов, позволяющих злоумышленникам вести свою деятельность,— уязвимость приложений. 85% пентестов заканчивается практически полным захватом контроля над сетью компаний»,— подчеркивает Дмитрий Калинин, руководитель департамента по работе с уязвимостями и инцидентами компании.

«Бизнесу необходимо укреплять защиту сетевого периметра, внедрять сертифицированное ПО (особенно компаниям, работающим с критической инфраструктурой), компонентный анализ (SBOM) для обеспечения прозрачности цепочек поставок, интегрировать инструменты безопасности на уровне JDK, серверов приложений и ОС, автоматизировать процессы безопасности и интегрировать их в цикл разработки ПО (DevSecOps), а также применять средства защиты от социальной инженерии, анализирующие подлинность изображений, видео и аудио»,— советует Алексей Рубаков, основатель компании Netrack. ➔ 6