# Сергей ОВЧИННИКОВ:

## «Мы видим увеличение спроса на российские решения»

Сложные решения для обеспечения информационной безопасности крупных предприятий, такие как системы оркестровки ИБ, автоматизации и реагирования на инциденты (Security Orchestration, Automation and Response – SOAR) или решения для управления безопасностью, рисками и соответствием законодательству (Security Governance, Risk Management and Compliance – SGRC), сложно разработать и внедрить быстро. К счастью, в России есть разработчики подобных комплектных систем, например компания UDV group. Чтобы понять текущую ситуацию на этом рынке, мы задали несколько вопросов руководителю направления продуктового маркетинга Сергею Овчинникову.

**– Какие решения, разработанные вашей компанией, оказались наиболее востребованы у промышленных предприятий в прошедшем году?**

– В прошедшем году группа компаний UDV объединила под единым брендом известных экспертов-разработчиков в области кибербезопасности и информационных технологий – «СайберЛимфа», «КИТ» и «ФТ-СОФТ». Наиболее востребованным у заказчиков ожидаемо оказался DATAPK (в настоящее время UDV DATAPK Industrial Kit) – комплекс решений для мониторинга состояния защищенности и оперативного обнаружения инцидентов информационной безопасности в промышленных сетях. Клиенты отмечают функциональность решения, так как UDV DATAPK Industrial Kit не только обладает возможностями промышленной сертифицированной системы обнаружения вторжений, но и является инструментом инвентаризации защищаемых сетей, контролирует конфигурации узлов, управляет уязвимостями и т. д. Кроме того, наблюдается большой интерес заказчиков к UDV ePlat4m SOAR – это интегрированная платформа оркестрации средств защиты информации и автоматизации функций ИБ. UDV ePlat4m SOAR обогащает данные об инцидентах, делает предварительные оценки и обеспечивает автоматизированное реагирование на основные типы инцидентов компьютерной безопасности. По оценкам наших заказчиков, применение UDV ePlat4m SOAR позволяет уменьшить количество обрабатываемых вручную инцидентов примерно в 20 раз, а среднее время реагирования уменьшается с трех дней до 25 минут.

**– Как на ваш бизнес повлияли ограничения, наложенные международными разработчиками ПО?**

– Компании, входящие в группу UDV, работают на отечественном рынке средств обеспечения кибербезопасности, где применяются российские решения, в том числе прошедшие оценку соответствия требованиям регулятора в системе сертификации ФСТЭК России. Ограничения, наложенные международными (иностранными) разработчиками в прошлом году, касаются поддержки поставляемых в Россию решений, включая обновления и бюллетени по безопасности, устраняющие уязвимости в программных продуктах и прошивках устройств. В итоге мы видим увеличение спроса на российские решения в области обеспечения кибербезопасности предприятий.

**– Как изменилась индустрия разработки программного обеспечения для промышленных предприятий в 2022 г.? Что вам пришлось поменять в своих бизнес-процессах?**

– Очевидный тренд в разработке программного обеспечения, который начался еще до 2022 г., – это совершенствование процессов безопасной разработки и внедрение SDL (жизненного цикла безопасной

разработки). Регуляторы также уделяют этому аспекту много внимания, в частности, совершенствуя процессы сертификационных испытаний. Для компаний UDV Group минувший год не стал в этом отношении каким-то особенным, так как процессам безопасной разработки мы всегда уделяли самое пристальное внимание, проводя статический и динамический анализ, включая фаззинг-тестирование.

**– Насколько повлияли на рынок разработчиков ИТ-решений меры поддержки, предпринятые Правительством РФ в прошедшем году?**

– Рынок разработчиков ИТ-решений довольно разнородный. Одни сосредоточены только на так называемых коробочных программных продуктах, другие – разрабатывают аппаратно-программные решения или занимаются заказной разработкой. Сложности с поддержкой неминуемо возникают при погружении в детали, тем не менее можно смело утверждать, что в целом меры поддержки, предпринятые Правительством РФ в прошлом году, оказали положительное влияние. Мы видим, что эти меры получают свое развитие на федеральном и региональном уровнях.

**– В каком направлении, по вашим расчетам, будет развиваться рынок разработки ПО для промышленных предприятий в 2023 г.?**

– На наш взгляд, на развитие рынка будут влиять следующие факторы. Во-первых, возросшее в 2022 г. количество атак на российскую критическую информационную инфраструктуру. Спрос на программные и аппаратно-программные решения, которые помогают обнаруживать и предотвращать вторжения, своевременно и качественно реагировать на инциденты, будет продолжать расти, в том числе в промышленном сегменте.

Во-вторых, в 2023 г. еще заметнее усилится тренд на импортозамещение. Если раньше кто-то из заказчиков откладывал такие проекты, а кто-то стремился все-таки воспользоваться покидающими рынок иностранными решениями, то в текущем году у заказчиков остается меньше возможностей для маневра. Необходимо будет не только выбрать новые для себя российские решения, но и интегрировать их с существующими системами, провести переобучение персонала, перестроить некоторые бизнес-процессы, решить вопросы с технической поддержкой по уже внедренным системам. Отдельно стоит упомянуть открытые решения, по многим из которых ранее оказывалась платная техническая поддержка. Заказчики вынуждены искать возможности по техподдержке таких систем у российских интеграторов либо переходить на совместимые российские решения. Одним из таких решений является сертифицированная система мониторинга ИТ-инфраструктуры UDV ITM, которая имеет полную совместимость с открытым решением Zabbix, дополняя существующие у заказчиков системы возможностью построения иерархической структуры сервисов мониторинга удаленных площадок и филиалов.

В-третьих, спрос на квалифицированные ИТ-кадры, в том числе в области разработки программного обеспечения, продолжает оставаться на высоком уровне. Трудности с наймом ИТ-специалистов испытывают как поставщики, так и потребители решений. Зарплаты специалистов высокие, поэтому заказчики разумно подходят к решению проблемы, применяя для разработки корпоративного программного обеспечения low-code-платформы автоматизации деятельности. В условиях меняющихся бизнес-процессов этот подход позволяет существенно снизить затраты на разработку и существенно ускорить создание корпоративных сервисов. Low-code-платформы не подходят для решения абсолютно всех задач современного промышленного предприятия, но в части автоматизации бизнес-процессов такие решения позволяют силами меньшего количества персонала при более низкой его квалификации разрабатывать качественное программное обеспечение. На российском рынке присутствует много производителей low-code-платформ, включая UDV ePlat4m, отличительными чертами которой являются высокая адаптивность к существующим разнотипным источникам данных и удобство интерфейса пользователя. Мы сами применяем эту платформу для разработки части функциональности наших решений, таких как UDV ePalt4m SOAR и UDV ePlat4m SGRC, что позволяет легко адаптировать «коробочные» версии под текущие нужды заказчиков.

В-четвертых, нельзя не упомянуть технологический тренд, связанный с технологиями машинного обучения. Речь идет не только о нейронных сетях и глубоком обучении, которые за последние несколько лет стали гораздо доступнее, но и о других эффективных подходах, которые мы применяем в своей практике в рамках НИОКР в нашем Научно-исследовательском центре по кибербезопасности в сотрудничестве с вузами, а затем эти технологии интегрируются в новые или существующие продукты. Например, при разработке нашего флагманского решения для обеспечения кибербезопасности промышленных сетей UDV DATAPK Industrial Kit был использован метод многоагентного моделирования, который позволяет путем машинного обучения осуществлять автоматический реверс-инжиниринг закрытых промышленных протоколов. Эта запатентованная технология обеспечивает возможность мониторинга отклонений от эталонных моделей и обнаружения несанкционированных изменений в АСУ ТП. ■