Сергей ОВЧИННИКОВ:

«Долгосрочный эффект связан с развитием экосистемы кибербезопасности»

Заказчики с высоким уровнем зрелости со сложной распределенной инфраструктурой и разнородными мультивендорными комплексами предъявляют повышенные требования к средствам защиты в целом. О том, какие решения доступны таким предприятиям на российском рынке и о перспективных направлениях развития средств ИБ, рассказал руководитель направления продуктового маркетинга компании UDV Group Сергей Овчинников.

– Год назад несколько разработчиков в области кибербезопасности и информационных технологий – «СайберЛимфа», «КИТ» и «ФТ-СОФТ» – объединились под общим брендом. Какие выгоды от реализации этого проекта извлекли заказчики?

– До образования UDV Group в конце 2022 г. компании группы продвигали свои продукты под собственными брендами. Сейчас это экосистема, над созданием которой мы работали весь 2023 г. на всех уровнях, от технических специалистов до маркетинга и продаж. Можно говорить о краткосрочном эффекте в горизонте одного года и о долгосрочных последствиях принятых решений.

За прошедший год мы создали и развили партнерскую сеть продаж – сейчас это уже более 30 ведущих российских интеграторов. Существенно усилены многие команды: продуктовая разработка, продажи и маркетинг. Мы развиваем технологическое партнерство. Как следствие, произошел многократный рост количества проектов.

Продажи по итогам 2023 г. подросли незначительно, но мы и не ожидали в первый год впечатляющих успехов, так как проекты в классах наших решений обычно длятся по полтора года. Долгосрочный эффект, на который мы рассчитываем, связан с развитием экосистемы кибербезопасности. Объединение разных продуктов в единый комплекс решений не может произойти мгновенно.

Мы работаем над единой дизайн-системой продуктов, постепенно переходим к единому технологическому стеку в разных продуктах для повторного использования компонентов и модулей, улучшаем инструменты для быстрого создания прототипов и тестируем гипотезы.

– Какие продукты UDV Group вывела на рынок в минувшем году, в чем их преимущества по сравнению с аналогами?

– Мы вывели на рынок много новых продуктов, но сначала хотелось бы рассказать о выпуске новой версии UDV DATAPK Industrial Kit – это комплекс решений для мониторинга состояния защищенности и оперативного обнаружения инцидентов информационной безопасности в промышленных сетях. Выпущенная в конце 2023 г. версия UDV DATAPK Industrial Kit 2.0 получила существенные изменения: переработанную архитектуру взаимодействия компонентов, новый механизм поиска уязвимостей, расширение возможностей анализа сетевого трафика, улучшения пользовательского интерфейса и быстродействия системы, расширение списков поддерживаемых операционных систем, промышленных протоколов, источников событий ИБ.

В рамках конференции «ИБ АСУ ТП КВО 2024» мы представляем новый выпуск 2.1, который расширяет существующие возможности комплекса. UDV DATAPK Industrial Kit отличается от аналогов возможностью комплексно решать задачи обеспечения ИБ в АСУ ТП, так как помимо функциональности по пассивному анализу трафика и выявлению ИБ-инцидентов комплекс позволяет проверять узлы промышленной сети на уязвимости и контролировать их конфигурации. Еще одно архитектурное преимущество нашего решения – возможность корректной работы на удаленных технологических площадках со слабыми каналами связи.

Второе значительное обновление – выпуск версии зонтичной системы мониторинга UDV ITM, которая предназначена для мониторинга функционирования распределенных автоматизированных и информационных систем различного назначения, в том числе АСУ ТП. Это единое решение для мониторинга удаленных технологических площадок и филиалов.

UDV ITM позволяет, в частности, бесшовно переходить с open-source-системы мониторинга Zabbix на сертифицированное ФСТЭК России отечественное решение с качественной технической поддержкой.

В 2023 г. в партнерстве с ЗАО «НИЦ» мы создали прототип первого в России межсетевого экрана на открытой процессорной архитектуре RISC-V – UDV Industrial Firewall. Ключевое преимущество решения заключается в аппаратной «начинке», которая делает продукт санкционно устойчивым, так как для его производства не требуется применения высокотехнологичных компонентов из недружественных стран. В 2024 г. мы продолжаем всестороннее тестирование и улучшение аппаратной платформы и проходим процедуру сертификации во ФСТЭК России.

Продуктовая экосистема UDV Group развивается высокими темпами. В прошедшем году мы также вывели на рынок облегченное решение для автоматизации реагирования на инциденты UDV ePlat4m IRP Lite, с помощью которого возможно закрывать инциденты одновременно в UDV SIEM. Создано несколько модулей на собственной low-code-платформе UDV ePlat4m и дополнена ими функциональность UDV ePlat4m SGRC.

В 2024 г. планируем выпустить решение для контроля версий проектов ПЛК в технологических сетях. Этот, во многом уникальный для российского рынка продукт, позволит реализовать централизованное управление репозиториями проектов ПЛК, осуществлять резервное копирование и восстановление проектов ПЛК, отслеживать и контролировать изменения в исходном коде.

– В каких промышленных сегментах наблюдается наибольший спрос на ваши решения, чем вы это объясняете?

– Если говорить про отраслевые сегменты, то исторически это металлургия, ТЭК, нефтегазовые компании, хотя довольно сложно выделить сегмент, в котором спрос был бы доминирующим. Здесь уместно сегментировать предприятия по уровням зрелости в области ИБ и некоторым особенностям ИТ-инфраструктуры.

Заказчикам с низким уровнем зрелости сложно осваивать решения таких классов, как SOAR и SGRC. Зачастую разрыв в понимании вопросов ИБ между службой ИБ и топ-менеджментом приводит к недофинансированию проектов по ИБ. В результате у таких заказчиков закрыты только базовые потребности в ИБ, обусловленные требованиями регуляторов. Нам есть что предложить и таким заказчикам: и экспертизу вендора, заложенную в продукты, и свое видение выстраивания процессов.

Наибольший спрос на наши продукты наблюдается у заказчиков со средним и высоким уровнем зрелости, где служба ИБ предъявляет повышенные требования к средствам защиты. Обычно это предприятия со сложной распределенной инфраструктурой и разнородными мультивендорными комплексами. Сильная сторона многих наших продуктов – относительно невысокие требования к аппаратному обеспечению и совместимость с существующими системами у заказчиков.

– Очевидное увеличение спроса на российские решения в области обеспечения кибербезопасности предприятий в силу геополитических причин заставило вашу ГК оптимизировать бизнес-процессы, расширить штат сотрудников, партнерскую сеть, предпринять иные шаги?

– UDV Group создавалась во второй половине 2022 г. в условиях и с учетом всех внешних факторов. Еще на старте этого проекта было очевидно, что без инвестиций в разработку, систему продвижения и продаж, без перестройки процессов, связанных с объединением усилий компаний группы, невозможно достичь поставленных целей.

За предыдущий год наш штат увеличился примерно на 20%. Много новых сотрудников принято в продуктовые команды. Мы получаем обратную связь от рынка, поэтому усиление команд в нашем случае неизбежно. Понимаем, что справиться в одиночку будет в разы сложнее, поэтому развиваем отношения с партнерами-интеграторами, технологическими партнерами, учебными центрами и вузами.

– Какие тенденции в индустрии разработки программного обеспечения для информационной безопасности промышленных предприятий вы относите к доминирующим на российском рынке?

– Можно выделить следующие тенденции в разработке ИБ-решений для промышленных предприятий. Во-первых, наблюдается постепенный переход от неинвазивных решений к продуктам, которые активно взаимодействуют с узлами технологических сетей. Сюда же можно отнести тренд на рассмотрение наиболее зрелыми заказчиками средств автоматического реагирования на ИБ-инциденты в АСУ ТП.

Во-вторых, явно прослеживается тренд на применение машинного обучения для выявления инцидентов в АСУ ТП. Преимущества ML-подхода для решения некоторых практических задач отрицать невозможно, а доступность и безопасность этих технологий незначительно отличаются от традиционных методов, поэтому в будущем увидим множество решений с машинным обучением в технологическом сегменте.

В-третьих, это применение облачных сервисов в АСУ ТП, что требует от заказчиков внедрения специализированных решений для защиты информации. Тенденция перехода на облака в АСУ ТП является общемировой. Два наиболее частых сценария использования облачных сервисов – удаленный мониторинг конфигураций и анализ телеметрии инженерных операций, а также хранение архивных данных.

В-четвертых, запрос заказчиков на решения на стыке ИБ и физической безопасности, что обусловлено сложностями в авторизации пользователей на полевом уровне АСУ ТП. В-пятых, применение low-code-платформ для быстрого создания приложений или прототипирования. В условиях меняющихся ИТ-инфраструктур под влиянием импортозамещения требуются новые решения, а подход low-code позволяет существенно сократить сроки разработки и вывода на рынок некоторых классов продуктов. ■