# Виктор СЕРДЮК:

## «На 2019 год компании запланировали работы по модернизации СЗИ»

Современные системы обеспечения информационной безопасности сложно самостоятельно внедрить, настроить и заставить эффективно работать. Поэтому компаниям на пути цифровой трансформации приходится прибегать к услугам интеграторов, которые в результате имеют объективное представление обо всем рынке информационной безопасности. Состояние российского рынка ИБ мы обсудили с Виктором Александровичем Сердюком, генеральным директором АО «ДиалогНаука».

**– Какие средства защиты и инструменты наиболее востребованы у российских клиентов? И что в большей степени влияет на выбор СЗИ: требования законодательства или реальная необходимость?**

– На сегодняшний день можно условно выделить две группы средств защиты информации – традиционные, существующие на рынке несколько лет, и перспективные, которые появились относительно недавно. К первой группе относятся антивирусы, песочницы, межсетевые экраны, средства обнаружения вторжений, SIEM-системы и др. Их приобретают заказчики с целью выполнить требования регуляторов и повысить реальный уровень защищенности своих компаний.

Ко второй группе можно отнести следующие типы средств защиты:

- решения класса UEBA (User & Entity Behavior Analysis), предназначенные для выявления инцидентов на основе поиска аномалий в поведении пользователей или узлов сети;
- средства SOAR (Security Orchestration, Automation and Response), направленные на автоматизацию процессов реагирования на выявленные инциденты информационной безопасности;
- решения класса EDR (Endpoint Detection and Response), предназначенные для выявления целенаправленных атак на уровне рабочих станций и серверов, а также для реагирования на них;
- решения ILD (Information Leaks Detection), позволяющие выявлять источник утечки конфиденциальной информации, опубликованной в сети Интернет, за счет встраивания в документ специальной невидимой метки (стеганография).

Интерес к решениям, относящимся ко второй группе, связан с необходимостью более эффективного противодействия новым угрозам безопасности, с которыми не способны в полной мере справиться традиционные средства защиты информации.

**– Изменилось ли за прошедший год соотношение между продажей продуктов и сервисов на рынке информационной безопасности в России?**

– В прошлом году сохранялась устойчивая тенденция увеличения доли сервисов в обороте «ДиалогНаука», что в первую очередь связано с непрерывным повышением уровня сложности систем информационной безопасности. Для эксплуатации таких систем зачастую требуются высококвалифицированные сотрудники, и в ряде случаев заказчику проще передать сопровождение систем внешнему подрядчику, чем содержать в штате высокооплачиваемых специалистов.

Еще одной причиной увеличения доли сервисов является возрастание количества нормативных требований регуляторов, которым должны соответствовать российские компании. Например, в 2018 г. был принят № 187-ФЗ, вступили в силу новая редакция Положения Банка России 382-П, а также новый ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций». Кроме того, в мае 2018 г. начали действовать требования Европейского регламента о защите персональных данных GDPR (General Data Protection Regulation). Некоторые российские компании, обрабатывающие персональные данные граждан ЕС, также должны выполнять требования по их защите. Для того чтобы самим не разбираться во всех тонкостях законодательства и гарантировать полное соответствие требованиям

регуляторов, компании обращаются к сторонним специализированным организациям. Это подтверждают и результаты работы нашей компании за 2018 г., показывающие увеличение количества проектов по перечисленным направлениям консалтинга.

**– Как влияют на российский рынок ИБ требования регуляторов и международная обстановка? Изменилось ли соотношение между зарубежными и отечественными продуктами?**

– Безусловно, внешнеполитическая ситуация сказывается на процессе импортозамещения в России. Все больше заказчиков отдают предпочтение отечественным разработкам на этапе выбора новых подсистем, а многие уже инициировали процессы по замене существующих зарубежных систем защиты российскими аналогами. С нашей точки зрения, эта тенденция в ближайшее время будет только усиливаться. Подтверждением является директива, выпущенная в декабре 2018 г. и предписывающая госкомпаниям разработать план перехода на российское ПО, доля которого до 2021 г. должна превысить 50%.

**– Насколько популярной темой для российских клиентов является защита критической информационной инфраструктуры? Часто ли такие проекты доходят до построения качественной системы защиты?**

– С нашей точки зрения, Федеральный закон № 187-ФЗ на сегодняшний день является одним из драйверов развития российского рынка информационной безопасности. Под действия данного закона подпадает достаточно большое количество компаний из разных отраслей, и многие из них предпочитают обращаться к сторонним специализированным компаниям для реализации мероприятий по приведению в соответствие с требованиями по защите КИИ. За прошлый год основная часть организаций только приступила к категорированию своих объектов КИИ, а работы по созданию/модернизации средств защиты запланированы на 2019 г.

**– В чем особенности сфер деятельности, перечисленных в законе «О безопасности КИИ»? На каком уровне, по вашим оценкам, находится их защищенность?**

– Сферы деятельности, перечисленные в названном законе, позволяют однозначно определить, подпадает ли предприятие под действие данного нормативно-правового акта. Если организация имеет информационные системы, функционирующие в одной из сфер, перечисленных в законе, то она является субъектом КИИ и должна провести категорирование своих объектов. Если по результатам категорирования какие-то из объектов будут признаны значимыми, то в этом случае необходимо реализовать комплекс мер по защите информации на основе соответствующих приказов ФСТЭК России.

С нашей точки зрения, было бы неправильно оценивать степень защищенности в какой-то сфере деятельности в целом. Наш опыт показывает, что уровень безопасности компании зависит не от сферы ее деятельности, а от того, сколько внимания в ней уделяется вопросам защиты информации.

**– Какие новые продукты или новых поставщиков «Диалог-Наука» может добавить в свой ассортимент в этом году? Каких продуктов не хватает на российском рынке?**

– Наша компания постоянно следит за новыми перспективными решениями, которые выпускают как российские, так и западные вендоры. Так, например, в начале года мы подписали партнерское соглашение с российской компанией Everytag, являющейся разработчиком системы контроля и защиты от несанкционированного распространения документов Everytag ILD. Технологии, лежащие в основе системы, позволяют гарантированно обнаружить виновника утечки информации по фрагменту документа, скану копии или фотографии с экрана компьютера. Система реализована как самостоятельное решение и поддерживает интеграции с популярными системами документооборота. Решение компании запатентовано и включено в Реестр российского программного обеспечения.

Еще одним интересным решением, которое наша компания включила в свой продуктовый портфель в 2019 г., является продукт класса UEBA – Exabeam. В отличие от SIEM-системы, где в качестве единицы измерения используется событие, в решении Exabeam Advanced Analytics применяется понятие «сессия», и в уже в рамках сессии пользователя или узла система фиксирует происходящие события. Если событие несет в себе угрозу и является отклонением (например, запуск процесса, который до этого ни разу не запускался в сети предприятия), система повышает уровень риска пользователю или узлу. При достижении порогового значения система выделяет таких пользователей, чтобы офицер безопасности мог сфокусироваться в первую очередь на них. Чтобы минимизировать ложные срабатывания, необходимо сначала дать возможность системе обучиться – от двух недель до нескольких месяцев. В результате работы Exabeam Advanced Analytics формируется план-график (timeline) деятельности пользователя или узла, на котором выделяются наиболее подозрительные моменты его деятельности. Построенный график является удобным инструментом для изучения активности пользователей и узлов, а также расследования инцидентов с возможностью обнаружения взаимосвязей с другими пользователями и узлами на предприятии. При помощи подобных графиков служба безопасности может составить максимально подробное представление о процессах, происходящих в информационных системах компании. ■