Глобализация и импортозамещение: какие тренды будут актуальны на рынке ИБ в следующем году

Сергей Панов, *заместитель генерального директора, АО "ЭЛВИС-ПЛЮС"*

Подводя итоги года, хочется вспоминать достижения, а не проблемы. К счастью, нам есть о чем рассказать — это наши отечественные разработки. Несмотря на дефицит кадров, несовершенство нормативной базы и рост количества хакерских атак, проекты в сфере импортозамещения развиваются. И хотя производители пока не могут полностью отказаться от импортных комплектующих, решение, как минимизировать эту зависимость, у них уже есть. Об этом мы поговорили с Сергеем Борисовичем Пановым, заместителем генерального директора компании "ЭЛВИС-ПЛЮС".

– Как вы можете охарактеризовать состояние рынка ИБ в мире на пороге 2019 года?

– Информационные технологии развиваются и проникают во все сферы нашей жизни. Увеличивается уровень их вовлеченности в различные виды производств, поднимаются требования к эффективности. С повышением удобства и доступности тех или иных услуг растет и привлекательность информации для злоумышленников. Соответственно, увеличивается количество хакерских атак. Атакующие технологии развиваются быстрее, чем защитные, мы всегда идем следом за мошенниками и вынуждены реагировать на появление новых подходов.

Угрозы становятся все более изощренными, и выявлять их становится все сложнее, поэтому наиболее высокий темп роста показывают средства обнаружения атак, средства анализа защищенности и сегмент предоставления услуг.

Информационные ресурсы стали носить глобальный характер, активно развиваются облачные сервисы. По сути, обращаясь к облаку, используя почтовые сервисы, социальные сети, мы не знаем, где находится информация, на каких серверах и на чьей территории она обрабатывается. В настоящее время это одна из проблем, которую пытаются решить как на технологическом, так и на государственном уровне путем установления законодательных требований по переносу и обработке ПДн на территории РФ. Не только информация перестала быть привязанной к конкретной территории и государству, атакующая сторона тоже приобрела трансграничный характер. Мы не можем вычислить стратегию преступника, а если это таргетированная атака – не знаем заранее ее цели. Абсолютная неопределенность. Поэтому если мы говорим про общемировые проблемы, то крайне важно наладить международное сотрудничество в разработке общих стандартов, в заключении международных соглашений, которые позволят привести к единообразию методы и способы технологии реагирования. Нужно наладить информационный обмен по уязвимостям, инцидентам ИБ и способам их предотвращения, повысить роль международной нормативно-правовой базы.

Далеко не все организации могут позволить себе большой штат квалифицированных сотрудников по информационной безопасности, экспертов и соответствующее оборудование. Это дорого. Поэтому значительный рост мы видим на рынке услуг специализированных организаций, сервисных провайдеров, наиболее прозрачных и удобных с точки зрения пользователя.

– А как обстоит дело с информационной безопасностью в России?

– Для России как для части мировой экономики актуальны все мировые тенденции. В текущей непростой политической и экономической ситуации у нас по сравнению с другими странами низкий уровень национальной независимости с точки зрения ИТ и, в частности, технологий ИБ. Государство должно поддерживать и стимулировать разработку систем обеспечения ИБ, обнаружения атак, анализа защищенности; должно обеспечить независимость каналов связи, точек хранения и обработки данных, чтобы обеспечить национальный контроль за киберпространством в широком смысле этого слова; развивать отечественную элементную базу.

В деле обеспечения ИБ важен также и уровень межведомственного взаимодействия. Активную деятельность по разработке нормативных документов ведут отраслевые организации, в частности ЦБ РФ, ведь основными целями атак как раз и являются предприятия кредитно-финансовой сферы.

Еще одна проблема – кадровые ресурсы. ИТ-специалистов в России категорически не хватает. На рынке ИБ профессионалов еще меньше, чем в целом в отрасли информационных технологий.

Если говорить про информационно-психологический блок вопросов ИБ, то здесь нужно ужесточить контроль не только с точки зрения классического обеспечения безопасности (конфиденциальность, целостность, доступность), но и с точки зрения анализа информационного контента. Вал информации, который обрушивается на пользователей, может приводить к непредсказуемым последствиям. Эта проблема требует решения на уровне законодательном, технологическом и методическом.

– Вы не первый, кто отмечает проблему кадров на рынке ИБ. Как вы ее решаете?

– Ситуация с кадрами сложная. Меняется рынок, и людей интересует развитие в этих сферах, смена обстановки. Чтобы заинтересовать сотрудников, мы вынуждены искать новые формы, развивать новые услуги, например, услуги сервис-провайдера ИБ, и наша компания на этом рынке планирует проявить себя уже в следующем году.

Помимо традиционных способов поиска сотрудников, мы используем наши возможности по привлечению студентов.

Есть курсы в формате семинаров, на которых мы демонстрируем технологии ИБ, обучаем нашим продуктам, рассказываем, какие услуги есть на рынке, читаем лекции. Мы предоставляем студентам возможность получить практические навыки для написания диплома или сдачи нормативов. Если человек нас устраивает – приглашаем его на работу. 8–10 выпускников приходят к нам ежегодно.

По мнению экспертов, одним из недостатков разработок на отечественном рынке являются телеком-компоненты. А чего, на ваш взгляд, не хватает российскому рынку ИБ?

– Абсолютно верно. В этом плане мы серьезно отстали. Одно из решений вопроса – разработка устройств на собственной элементной базе (процессоры "Салют 24", "Байкал", "Эльбрус"). Они пока существенно уступают по характеристикам зарубежным аналогам, есть проблемы со стоимостью, что связано с небольшими объемами текущего спроса и производства. Есть и другой подход. Наверное, в ближайшее время

Intel нам не догнать с точки зрения его целевого функционала, но можно попробовать обеспечить контроль процессов внутри компьютера, обеспечивать независимое хранение и независимую обработку информации путем добавления в систему доверенной составляющей (доверенного процессора) на собственной элементной базе. То есть реализовать некий доверенный компьютер внутри Intel-based-компьютера, который позволит контролировать чувствительную информацию и процессы, возьмет на себя функции по доверенной обработке и хранению критичных данных. В теории звучит красиво, на самом деле это достаточно сложное решение. И мы стараемся не отстать: совместно с нашими коллегами из компаний НПЦ "ЭЛВИС", ТОНК и "Базальт" активно прорабатываем отечественные устройства на базе линейки продуктов ЗАСТАВА, в том числе работаем над созданием аппаратного тонкого клиента на отечественной элементной базе, что может позволить получить пусть небольшой, но элемент той независимости, о которой я говорил, – независимости системы обеспечения ИБ в России.

– Летом этого года вы выпустили АПК VPN/FW "ЗАСТАВА-150". Что подтолкнуло ЭЛВИС-ПЛЮС к созданию именно аппаратного решения?

– Раньше мы производили программное обеспечение и сертифицировали его. На мой взгляд, очень гибкий механизм без привязки к каким-либо платформам, что было одним из наших достоинств. Мы могли предложить заказчику выбор платформы, включая использование всех существующих. Но сейчас требования регуляторов поменялись, а у заказчиков изменились требования к уровню защищенности. Поэтому в некоторых случаях только привязка к аппаратной платформе позволяет нам выполнить новые требования. Мы уже анонсировали выход целой линейки шлюзов разного уровня защищенности и производительности, в которых планируем использовать платформы отечественных производителей.

– В чем преимущество АПК "ЗАСТАВА-150"?

– Главное преимущество – надежность платформы из-за отсутствия движущихся частей. Информация хранится на SSD-диске. Блок питания внешний, охлаждение пассивное. В АПК также отсутствуют наложенные аппаратные средства типа электронных замков, которые могут выходить из строя, сбоить, что негативно отражается на надежности. Наша уникальная разработка совместно с компанией ТОНК – датчик вскрытия, который является частью самой аппаратной платформы. Необходимо отметить, что замену ключей и сертификатов можно производить удаленно. Еще одно достоинство нашего решения – возможность удаленного обновления всего программного обеспечения. Это важно для оперативного устранения ошибок и уязвимостей в ПО.

Хотелось бы отметить, что в линейке ЗАСТАВА есть устройство АПК "ЗАСТАВА-ТК" – аппаратный тонкий клиент, который использовался в рамках построения системы защиты ЕГР ЗАГС, успешно введенной в эксплуатацию с октября 2018 г. ЕГР ЗАГС – система сложная: более 15 тыс. клиентских рабочих мест находятся на 5,5 тыс. объектах ЗАГС. Нам удается эффективно поддерживать систему в оптимальном рабочем состоянии благодаря заложенным технологическим и архитектурным решениям ЗАСТАВА, включающим технологии обновления ключей и сертификатов, ПО, а также поддержки эксплуатации и сопровождения.

– На какие группы заказчиков рассчитаны "ЗАСТАВА-150", "ЗАСТАВА-ТК"?

– Это малые и средние офисы, государственные организации, которым требуется высокий уровень защищенности в соответствии с требованиями регулятора (до КС3, К1). Это также организации и компании, работающие с ведомственными централизованными ГИС (Росреестр, ЗАГС, ФНС России и другие) и подключенные к их информационным ресурсам. Здесь могут применяться устройства как "ЗАСТАВА-ТК", так и "ЗАСТАВА-150", в зависимости от потребностей.

– Каковы дальнейшие планы по развитию линейки ЗАСТАВА?

– Сейчас в состав линейки входят АПК "ЗАСТАВА-150", "ЗАСТАВА-1500", "ЗАСТАВА-6000", "ЗАСТАВА-ТК" и их модификации, а также ПО "ЗАСТАВА-Офис", "ЗАСТАВА-Клиент", "ЗАСТАВА-Управление". Мы будем расширять эту линейку. Появятся другие платформы, на которые планируем получать сертификаты ФСБ России, ФСТЭК России и Минобороны. Есть планы по выпуску устройств как тонкого аппаратного клиента, так и шлюзовых решений на полностью отечественной платформе. Этими задачами в следующем году мы будем активно заниматься вместе с нашими партнерами.

– Но на этом новинки 2018 года от вашей компании не закончились, и уже в сентябре вы представили новый продукт – БДМ-АРМ-ФК. Расскажите о нем подробнее, пожалуйста.

– ПК БДМ (Базовый Доверенный Модуль) позиционируется как решение по защите данных на мобильном устройстве от хищения или утери, оно удобно для ноутбука или планшета. Использованные при проектировании продукта решения делают задачу взлома и получения доступа к данным практически нереализуемой, потому что каждый сектор физического диска шифруется своим отдельным ключом, применена оригинальная схема аутентификации и выработки ключей, продукт в режиме онлайн шифрует всю информацию на диске. Вам недостаточно подобрать только один ключ, вам придется это сделать отдельно для каждого сектора. Продукт может быть установлен на любую платформу. В этом году вышла третья версия ПК БДМ. В ней мы учли системные недоработки и добавили новую функциональность, которая потребовалась заказчикам в процессе эксплуатации. В первой половине года должна завершиться сертификация БДМ во ФСТЭК России по требованиям к средствам доверенной загрузки для использования в ГИС и СПДн уровня защиты до К1. В этом году мы также выпустили продукт БДМ-АРМ-ФК, который позволяет заказчику самостоятельно формировать ключи, контрольные суммы и обновления, необходимые для эксплуатации ПК БДМ. В 2019 году совместно с российским производителем ноутбуков и планшетов планируем выпустить мобильные устройства уровня КС3.

Продукт достаточно востребован, наиболее крупные проекты – в интересах Центрального банка РФ и ДИТ г. Москвы.

– В 2018 году у ЭЛВИС-ПЛЮС вышли два продуктовых релиза. Каковы планы на 2019 год? Куда планируете двигаться дальше?

– Мы продолжаем расширять линейку продуктов. Кроме того, намерены далее развивать продуктовые подразделения с перспективой выделения их в отдельную компанию. Продолжим работу с нашими ключевыми заказчиками. Наша компания, как и ранее, предлагает широкий спектр услуг по ИБ, в том числе консалтинговые. В планах – дальнейшее развитие направления защиты КИИ. Планируем также активно выходить на рынок как компания, предлагающая профессиональные сервисы ИБ, включая свои собственные услуги, экспертов и развитую технологическую базу.

ЭЛВИС-ПЛЮС

NM
АДРЕСА И ТЕЛЕФОНЫ АО "ЭЛВИС-ПЛЮС"
см. стр. 56