Круглый стол

Импортозамещение как защита

В круглом столе принимают участие

Дмитрий Бирюков,
директор направления информационной безопасности, компания «Атринити» (группа «Астерос»)

Алексей Гришин,
директор Центра информационной безопасности, компания «Инфосистемы Джет»

Максим Дружинин,
главный инженер проектов «ЛАНИТ-Урал» (группа компаний ЛАНИТ)

Алексей Качалин,
заместитель директора по развитию бизнеса, компания Positive Technologies в России

Сергей Корольков,
технический директор, АО «ДиалогНаука»

Игорь Корчагин,
руководитель группы обеспечения безопасности информации, компания ИВК

Александр Новожилов,
генеральный директор ООО «АйТи БАСТИОН»

Дмитрий Огородников,
директор Центра компетенций по информационной безопасности, компания «Техносерв»

Алина Хегай,
руководитель отдела информационной безопасности, компания «ЛАНИТ-Интеграция» (группа компаний ЛАНИТ)

Российская отрасль информационной безопасности является одной из наиболее успешных в мире, поскольку в ней есть известные российские компании, такие как «Лаборатория Касперского», «Доктор Веб», Positive Tecnologies и некоторые другие. В этой индустрии доля решений мирового уровня больше, чем в среднем по отрасли. Тем не менее именно разработчики средств защиты чаще других говорят о необходимости перехода на российское программное обеспечение. Может, они что-то знают?

Насколько критична зависимость отечественного рынка от зарубежных разработчиков? Какие дополнительные риски по сравнению с ИТ-продуктами несет в себе такая зависимость?

Дмитрий БИРЮКОВ

Признанными лидерами в области разработок на рынке ИБ сегодня являются США и Израиль. Не секрет, что наша страна в силу политических, экономических и исторических причин на данном этапе находится в роли догоняющих. При этом у нас есть ряд уникальных отечественных разработок, созданных с учетом требований российского законодательства. Например, продукты таких компаний, как «Лаборатория Касперского», Positive Technologies, InfoWatch, Group-IB, «Код безопасности» и др.

Думаю, если чисто гипотетически предположить возможность остановить поставки иностранных решений на российский рынок, то отечественными продуктами мы закроем все основные потребности в области защиты информации в стране. Но насколько отечественные решения будут удобными для пользователей и соответствовать запросам бизнеса – пока большой вопрос.

Если для направления ИБ в России существует четкий контроль со стороны государственных регуляторов, то для ИТ все гораздо менее нормировано. В настоящее время ИТ-отрасль – крайне конкурентный рынок, где у нас гораздо больше зависимости от западного оборудования, чем в области ИБ, что накладывает свой

отпечаток на объемы использования отечественных ИТ-технологий и продуктов.

Алексей ГРИШИН

На сегодняшний день зависимость существенная, и ее сохранение является положительным фактором для развития отечественных средств ИБ. Ведь если единственным драйвером развития будут требования регуляторов, то в условиях низкой конкуренции среди отечественных производителей функциональные возможности продуктов будут значительно уступать зарубежным аналогам.

Алексей КАЧАЛИН

Зависимость от производителей конечных продуктов и решений информационной безопасности снижается в первую очередь благодаря развитию и повышению конкурентоспособности отечественных разработок. Также положительную роль сыграли изменения курса валют и ограничения, вводимые нашими зарубежными компаниями. При этом по-прежнему нет альтернативы иностранным средствам разработки и системному ПО. Текущий «горячий вопрос» – активное строительство облачных сервисов. Создание подконтрольных облачных IaaS и SaaS определит, насколько изменится ситуация с импортозависимостью на горизонте в три-пять лет.

Игорь КОРЧАГИН

К сожалению, в области ИТ уровень зависимости отечественного рынка от зарубежных разработчиков крайне высок: продолжается повсеместное использование зарубежных решений разработки ПО, компиляторов, общесистемного ПО, прежде всего корпоративного класса, ну и, конечно, импорт аппаратного обеспечения со своим микропрограммным ПО. Иногда такое положение дел связано даже не с продолжающимся лобби зарубежных решений, а с производственной необходимостью. Но во многих случаях качественное и надежное ПО (входящее в реестр отечественного ПО или поддерживаемое международным сообществом Open Sourse) существует, но пока не получило распространения на предприятиях, особенно коммерческих. Не стоит забывать и тот факт, что многие открытые проекты представлены в основном зарубежными разработчиками и поддерживаются крупнейшими зарубежными ИТ-компаниями, что в долгосрочном плане может создавать риски для отечественных решений. Эти риски будут особенно высокими, если мы не будем создавать свои центры компетенций.

В области ИБ разработчики отечественного ПО занимают более прочные позиции, чем в среднем по ИТ. Есть области ИБ, где давно применяется преимущественно (или даже исключительно) отечественное ПО.

Дмитрий ОГОРОДНИКОВ

Зависимость отечественного ИТ- и ИБ-рынка в настоящее время остается высокой. У нас достаточно широко используются отечественные разработки по автоматизации бизнес-процессов, но и аппаратное обеспечение, и системное программное обеспечение, включая СУБД, в большинстве случаев остаются западными. Для ИТ-рынка такая зависимость несет риски отказа со стороны западных производителей от лицензионной и технической поддержки. Например, как это было в 2014 г., когда Oracle, Microsoft, Symantec и HP присоединились к санкциям США в отношении ряда российских компаний. Кстати, свободно распространяемое ПО и основанные на них проекты в данном случае тоже относятся к зарубежным, поскольку ядро систем разрабатывается и поддерживается западными разработчиками.

В ситуации с ИБ риски иные – недекларированные возможности, закладки или ошибки, о которых мы ничего не знаем и которые могут быть сделаны случайно либо преднамеренно. Например, обход систем аутентификации администраторов и пересылка копии трафика в облако производителя замечены едва ли не у всех производителей сетевого оборудования.

Однако от этой зависимости не так просто избавиться, и пока мы не производим достойную замену западным ИТ-разработкам, правительство было вынуждено снять ограничения по закупке западных продуктов с МВД, ФСБ, ФСО, СВР и ФСТЭК в рамках постановления № 684 от 18.07.2016.

Что сегодня сдерживает отечественных разработчиков ИБ-продуктов? Каков в этой индустрии кадровый, финансовый, организационный потенциал?

Дмитрий БИРЮКОВ

На наш взгляд, это нехватка финансовых и кадровых ресурсов. К сожалению, в нашей стране слабо развито направление профильных институтов, которые готовят высококлассных специалистов в области защиты информации, их можно пересчитать по пальцам. Кроме того, не стоит забывать, что мы упустили определенный временной период, когда западные вендоры активно технологически развивались и вкладывали миллиардные бюджеты в маркетинг и продвижение своих продуктов. Поэтому в нашей стране сейчас очень мало экспертов, имеющих опыт серьезных технологических разработок в области средств защиты.

Не способствуют развитию российских разработчиков ИБ-продуктов и ограниченные возможности для сбыта. Есть признанные лидеры, и с новыми разработками зайти на рынок достаточно сложно. В такой ситуации взятый правительством страны курс на импортозамещение может стать мощным толчком для развития отечественных продуктов и решений в области ИБ. Но без серьезных финансовых вложений и поддержки со стороны государства это маловероятно.

Алексей ГРИШИН

Сдерживающим фактором развития для разработчиков как раз и является кадровый и финансовый потенциал. В частности, на кадровом рынке мы наблюдаем серьезнейший дефицит высококвалифицированных специалистов. Как следствие, необходимые инвестиции выглядят неоправданно завышенными. В этих условиях разработчики ищут «инвесторов» – компании, готовые покупать альфа- и бета-версии продуктов. Но большинство заказчиков вынуждены оптимизировать бюджеты и не готовы инвестировать «в завтрашний день». В результате возникают серьезные финансовые ограничения развития рынка.

Максим ДРУЖИНИН

Кадровый потенциал в стране есть. Хотя зачастую компании, специализирующиеся на информационной безопасности (ИБ), самостоятельно выращивают кадры. Именно потому подобные специалисты высоко ценятся на рынке труда.

Основными потребителями отечественных ИБ-продуктов являются госструктуры. Исключение составляют разве что антивирусные и некоторые узкоспециализированные ИБ-решения.

Отрасль могла бы развиваться быстрее при условии повышения динамики изменений нормативной базы. Даже при том, что за последние несколько лет Федеральная служба по техническому и экспортному контролю (ФСТЭК России) издала приказы № 17 и № 31 и были приняты стандарты по виртуализации, нормативы в сфере ИБ требуют существенной доработки и обновления.

Алексей КАЧАЛИН

Сегодня ведущие российские ИБ-компании ставят перед собой амбициозную задачу: сделать свой продукт лучшим в мире и, с учетом глубокого понимания российской специфики, лучшим в России. Для этого требуется объем инвестиций, который значительно превосходит возможности, ограниченные внутренним рынком. Большинство компаний самостоятельно решают задачу вывода продуктов на зарубежные рынки, но здесь поддержка государства и госфондов не будет лишней.

Сергей КОРОЛЬКОВ

Потенциал развития есть, но не у всех российских средств ИБ. Некоторые средства защиты, необходимость применения которых обусловлена положениями нормативной документации, на мой взгляд, имеют меньше пространства для развития. А вот средства, которые появились «естественным» путем, как ответ на современные угрозы, развиваются очень динамично и уже на начальном этапе развития могут быть сравнены с продуктами ведущих производителей средств защиты.

Кадровый голод является одной из ключевых проблем индустрии ИБ, но в данном случае он не главный. Существенное препятствие – нежелание некоторых заказчиков тестировать и внедрять новые российские продукты. Отчасти это связано с репутацией отдельных российских продуктов, но в основном обусловлено уровнем зрелости заказчиков и их оценкой современных угроз ИБ.

Игорь КОРЧАГИН

Единственное, что может действительно удерживать отечественных разработчиков от активного развития рынка отечественных решений, и не только в области ИБ, это риски, связанные с возможностью последующей реализации продукции, ее востребованностью у отечественного потребителя. Разработка любого нового продукта требует серьезных финансовых инвестиций, при этом, если говорить об открытом рынке, достичь конкурентного преимущества перед мировыми лидерами крайне сложно, так как те за счет объемов могут существенно изменять стоимость своих решений либо предлагать комплексные решения, включающие множество взаимоувязанных продуктов

разного типа. Только однозначная нацеленность на импортозамещение со стороны потребителя может поддержать отечественного разработчика, хотя тут риски несет уже сам потребитель.

Дмитрий ОГОРОДНИКОВ

С кадровым потенциалом у нас все более чем хорошо! Во всяком случае, с 2006 по 2016 г. российские студенты восемь (!) раз выигрывали Чемпионат мира по программированию. Можно только гордиться такими результатами, однако если возникает необходимость найти в штат высококвалифицированного специалиста, в поисках можно провести не одну неделю, а то и не один месяц. Талантливые программисты и ИТ-специалисты, конечно, есть, но в целом их становится все меньше и меньше, что связано с заметным снижением качества образования за последнее десятилетие. Если говорить об организации процесса разработки, здесь все гораздо хуже: помимо недостатка программистов не хватает руководителей проектов, архитекторов систем, дизайнеров интерфейсов и пр. Мы пишем быстро, самозабвенно, с присущим нам максимализмом, но результат далеко не всегда совпадает с ожиданиями, и выход очередной номерной версии продукта может затянуться на годы.

Алина ХЕГАЙ

К сожалению, сегодня не так много российских компаний обладают по-настоящему сильной командой разработчиков и достаточной базой знаний. Это обусловлено целым рядом факторов. Во-первых, размер инвестиций в R&D в России явно не дотягивает до средних мировых показателей. Во-вторых, работодатели предпочитают экономить на высококвалифицированном персонале. В-третьих, не хватает государственной поддержки и сформированной в полном объеме потребности рынка. Некоторые разработчики грешат тем, что смещают фокус с первоочередных требований бизнеса на регулятивные, а это тормозит процесс создания качественного продукта, поскольку нормативная база значительно отстает от развития бизнес-систем. Кстати, многие отечественные продукты изначально создавались для госструктур, что наложило соответствующие ограничения на их функционал. Россия не входит даже в пятерку крупнейших стран-потребителей ИТ, соответственно и в сфере ИБ. А ведь спрос определяет предложение.

Какие классы ИБ-продуктов сегодня закрываются качественными российскими разработками, а в каких российских аналогов пока не хватает?

Дмитрий БИРЮКОВ

Сегодня российские разработки в области защиты информации способны закрыть базовые направления ИБ в разрезе общего рынка. В первую очередь речь идет о решениях по контролю доступа, межсетевому экранированию, криптографической защите, анализу защищенности и антивирусной защите.

В последнее время активное развитие получили системы обнаружения вторжений, но в большей степени это именно системы обнаружения, а не предотвращения. Чтобы эти технологические решения работали, отечественным разработчикам необходимо провести серьезную работу и иметь мощную научную базу.

Что касается классов решений, которые на данный момент уступают иностранным разработкам, то это решения класса DLP. Также пока не приходится говорить и о сформировавшемся отечественном рынке SIEM-решений. Слабо развито направление решений по контролю действий администраторов: отечественный рынок здесь представлен лишь несколькими OEM-решениями.

Алексей ГРИШИН

В первую очередь, конечно, нужно отметить традиционно российские направления ИБ. Это защита каналов связи, антивирусы, DLP, средства контроля уязвимостей. За последнее время вышли на конкурентный уровень средства контроля администраторов, решения классов WAF, IDM, средства анализа кода, средства безопасности АСУ ТП. Если же говорить о периметральных средствах защиты, тем более о так называемых NG, то пока они не составляют конкуренцию импортным аналогам.

Максим ДРУЖИНИН

Необходимо учесть, что ввоз криптографических средств с длиной ключа более 56 бит на территорию стран Таможенного союза Евразийского экономического союза требует прохождения сложной, длительной и непрозрачной процедуры получения лицензии ФСБ. На этом фоне отечественные производители криптосредств («С-Терра», «Континент», Vip-Net) значительно продвинулись в завоевании российского ИБ-рынка.

Алексей КАЧАЛИН

За последние годы спектр задач, решаемых на достаточно высоком уровне отечественными продуктами и сервисами, расширился. В таких сегментах, как, например, управление уязвимостями, мы занимаем до 80% российского рынка и можем составить реальную конкуренцию зарубежным аналогам. Крепкие позиции у наших разработчиков по антивирусам, системам защиты от утечек, безопасности приложений (Application Security), средствам защиты каналов (VPN). Активно совершенствуются продукты обнаружения

и управления инцидентами ИБ (SIEM), управления доступом (AM), решения по защите систем технологического управления. Отечественные решения давно и успешно используются клиентами как из госструктур, так и из бизнес-среды. При этом определяющим для клиентов является не страна происхождения, а качество и функционал российского софта.

Большой проблемой остается «системная» часть. Тяжело развивать и поддерживать на высоком уровне наложенные средства защиты информации, когда отсутствует контроль на системном уровне: операционные системы и СУБД, системы управления виртуализацией, а также инструменты и среды разработки прикладного и системного ПО и реализованные в них подходы и меры обеспечения безопасности пока слабо замещаемы. Но и в этом направлении есть позитивные тенденции – развитие отечественных разработок, «локализация» мировых вендоров. Примером такого движения можно считать начало сотрудничества SAP и «Газпрома» по созданию совместного предприятия – разработчика ПО. И хотя такие громкие заявления могут восприниматься как очередная «сборочная локализация», это еще одна возможность выстроить более контролируемый (и следовательно, безопасный) процесс разработки, придать импульс развитию систем анализа кода и повышению требований к встроенной безопасности платформ.

Сергей КОРОЛЬКОВ

Необходимо отметить, что количество российских продуктов в последние годы растет высокими темпами. И что особенно отрадно, появились продукты, которое занимают места на ведущих позициях в своих нишах. Сегодня отечественные продукты не уступают зарубежным аналогам в следующих группах: средства анализа защищенности, включая средства анализа защищенности исходного кода, межсетевые экраны уровня веб-приложений, средства противодействия утечкам конфиденциальной информации и, конечно, средства антивирусной защиты. Средства обеспечения безопасности в средах АСУ ТП являются вполне самобытными решениями, для которых даже ниши еще не сформировались.

Игорь КОРЧАГИН

На отечественном рынке ИБ-продуктов несомненное лидерство принадлежит средствам антивирусной защиты, средствам межсетевого экранирования, средствам защиты от НСД и средствам криптографической защиты информации. Именно эти классы продуктов ИБ всегда являлись неотъемлемой частью любой автоматизированной системы. Но такое положение дел не актуально для современных автоматизированных систем, где постоянно увеличивается количество специфических каналов проникновения в систему. В ответ на изменяющиеся условия, методы и средства обработки информации возникают новые методы и средства защиты такой информации, а также средства менеджмента ИБ. Наиболее популярными трендами последних лет являются SIEM, защита виртуализации и облаков, MDM (mobile device management), IAM (identity and access management), WAF (web application firewall), защита от DDOS, DLP. Многие из этих трендов уже активно реализуются отечественными разработчиками, но пока мы в числе догоняющих мировую ИБ-отрасль.

Особое место занимают отечественное ПО класса middleware и основанные на нем технологические платформы, которые позволяют строить крупномасштабные территориально распределенные информационные системы с высокими требованиями к безопасности информации и надежности, сложности ее логической обработки в масштабах сети. Построение ИС на базе этих продуктов резко сокращает сроки и стоимость построения и эксплуатации систем. Такие платформы являются зрелыми решениями, сертифицированными в соответствии с требованиями отечественной нормативной базы в сфере ИБ. Существует многолетний положительный опыт применения этого подхода.

Дмитрий ОГОРОДНИКОВ

Российский ИБ-рынок достаточно жестко регулируется законодательством. Наши разработки практически безальтернативны в случаях, когда нужно обеспечить защиту государственной тайны и государственных информационных систем. Это касается средств криптографической защиты и защиты от несанкционированного доступа, контроля целостности, строгой аутентификации и контроля устройств. Мы также сильны в части обнаружения киберугроз, специфика которых относится к России, и противодействия им. Особенно хорошо, что эти решения могут не только поставляться в виде отдельных программно-аппаратных средств, но и работать по сервисной модели, оказывая соответствующие услуги из облака производителей.

Вместе с тем, мы проигрываем в части обеспечения функций безопасности на уровне инфраструктуры и системного программного обеспечения. В первом случае у нас нет возможности разрабатывать аппаратные платформы с собственной схемотехникой, во втором – нет собственной операционной системы, которая, кстати, должна работать на нашей платформе. Да, у нас появился процессор «Эльбрус» и есть производство отдельных микросхем, но все это работает на западных архитектурах.

Алина ХЕГАЙ

Пробелы существуют, например, в части высокопроизводительного оборудования сетевой безопасности, применяемого для защиты сетей операторского класса. К тому же не всегда своими продуктами российские производители готовы обеспечить базу знаний для эффективного предотвращения инцидентов ИБ (например, базы сигнатур, репутации и т. д.). Как минимум, это можно объяснить количеством инсталляций.

Сегодня немало примеров, когда зарубежные разработчики ИТ- продуктов совместно с отечественными разработчиками в сфере ИБ предлагают рынку «защищенные» или «доверенные» продукты и решения. Насколько оправдано такое позиционирование? Какие риски снимает применение подобных решений, а какие нет?

Дмитрий БИРЮКОВ

По нашему мнению, такие понятия, как «доверенные» ИТ-продукты, – в большей степени маркетинговый ход в части позиционирования на рынке. Любая «доверенная система» (или продукт) должна пройти через оценку соответствия органов по сертификации, которые проведут проверку и выдадут соответствующие подтверждающие документы.

Также существуют риски наличия недекларированных возможностей в продуктах и системах западной разработки. И только специальная их проверка позволит снизить риски до приемлемого уровня. Но для этого производитель должен передать исходный программный код на анализ. Очень не многие зарубежные производители на это решаются, ибо сделать такой шаг – значит, добровольно раскрыть свою технологию, ноу-хау.

Алексей ГРИШИН

В большинстве случаев подобное позиционирование решает одну-единственную задачу – предоставление российским заказчикам, для которых ограничена возможность приобретения импортных продуктов, возможности соответствия. При этом подобные решения даже не решают проблемы фиксирования рублевых бюджетов. Тем не менее мы все чаще сталкиваемся с примерами, когда российские производители средств ИБ берут на себя разработку дополнительного функционала и техническую поддержку, что является прекрасным примером локализации импортного ПО.

Алексей КАЧАЛИН

Угрозы информационной безопасности легко преодолевают границы государств, а зачастую активно используют административные преграды при взаимодействии «защитников» и правоохранительных органов. С другой стороны, большинство решений ИБ сегодня – сложный продукт, основанный на интеграции (и поддержании ее в работоспособном состоянии) для получения данных и передачи команд, использования баз знаний, собираемых по всему миру. Таким образом, можно говорить, что подобное сотрудничество необходимо для решения многих (если не большинства) задач ИБ: борьбы с массовым вредоносным ПО, распределенными атаками, киберпреступностью во всех ее проявлениях. «Серой» областью в таком сотрудничестве остается противодействие группам, работающим в интересах конкурирующих государств. Здесь важно понимать необходимость дополнительных компенсирующих мер: чтобы защита от бытовых атак не приводила к повышению возможностей нарушителей высоких классов.

Игорь КОРЧАГИН

Конечно, такой подход имеет множество скрытых угроз и рисков, где ключевым моментом является именно доверие к предоставляемой зарубежным разработчиком продукции как программного, так и аппаратного обеспечения. Ведь оценить именно ее доверенность зачастую невозможно. Любые наложенные средства защиты скорее расширяют возможности изделия, нежели делают его доверенным, так как наличие уязвимостей или закладок в базовом изделии позволит обойти любые наложенные СЗИ.

Александр НОВОЖИЛОВ

Эта светлая идея волнует не первое поколение представителей ИТ-индустрии, вокруг этой темы сломано немало копий. Выглядит все замечательно: ИТ-система уже содержит в себе все необходимые средства защиты и не содержит ошибок и уязвимостей. Давайте разберемся, так ли все красиво.

Первое и самое важное: у ИТ и ИБ разные задачи. Для ИТ во главе угла – производительность и надежность. Поэтому необходимы максимальная гибкость и открытость системы. Для безопасности главное – контролируемость и максимальная закрытость системы. Здесь-то и скрывается основное противоречие. Ровно поэтому с таким трудом ИТ и ИБ сосуществуют в едином подразделении, если так принято в компании. Изначально задачи противоположны. Точка соприкосновения – надежность. Но и здесь подходы сильно отличаются. Надо ли объяснять, что создать систему, одновременно удовлетворяющую взаимоисключающим требованиям, невозможно?

Вторая причина, по которой я называю такие идеи утопическими, – сложность и тяжесть продуктивных ИТ-систем. Представьте, что выявлена новая уязвимость. Разработчик, например, межсетевого экрана, выпустит обновление в считанные дни, разработчик антивируса – в считанные часы, разработчик ОС – за несколько недель. А у разработчика тяжелой продуктивной системы будет непростой выбор: потратить ресурсы на устранение бага, связанного с производительностью системы, или на заплатку для устранения уязвимости, которой неизвестно воспользуются ли вообще. Кроме того, имеется серьезный соблазн переложить проблему на смежников.

Ну и третье. Вернемся к производительности. Известная проблема, что ИТ (а тем более АСУ ТП) пытается отказаться от наложенных средств безопасности, чтобы сэкономить ресурсы инфраструктуры для продуктива. Также зачастую отключаются или сводятся к минимуму средства журналирования и встроенные средства защиты систем. Это превращает процесс расследования инцидентов в каторгу для службы ИБ. Потому

и приобретаются дополнительные средства мониторинга и контроля.

Напоследок хочу сказать, что не вижу причин, которые побудили бы рынок к столь тектоническим изменениям. Энтузиасты, продвигающие подобного рода идеи, будут всегда. Однако «привить» это на объективную реальность, на мой взгляд, невозможно либо очень близко к этому. По крайней мере в среднесрочной перспективе.

Дмитрий ОГОРОДНИКОВ

В настоящее время Государственный реестр сертифицированных СЗИ содержит 1141 запись. Трудно выделить, сколько сертифицировано зарубежных средств из-за отсутствия соответствующего признака в записи, но Cisco, Microsoft, Oracle, Juniper, IBM и HP в сумме занимают 218 позиций. Поэтому в сертификации функций безопасности западных продуктов нет ничего удивительного – устоявшиеся практика. Другое дело, что большинство из них сертифицированы по ТУ, т. е. сертификация проведена без исследования исходных кодов в форме подтверждения соответствия встроенных функций безопасности. Такая сертификация оставляет риск существования недекларированных возможностей и программных закладок. Но эти средства не могут быть использованы для защиты государственных систем, а для защиты персональных данных в коммерческих системах, как выяснилось (одно из разъяснений ФСТЭК по поводу сертификации СЗИ), обязательная сертификация не требуется. Поэтому, как минимум для коммерческого рынка, сертификация СЗИ не дает конкурентных преимуществ. С другой стороны, у нас теперь есть реестр отечественного ПО, и все внимание производителей переключилось на него. В нем уже 1186 записей.

Но есть и обратные примеры. Так, несколько продуктов Oracle сертифицировано по второму уровню РД НДВ, что дает право использовать их в автоматизированных системах, которые содержат сведения, составляющих государственную тайну.

Что государство может и должно сделать для поддержки российских разработчиков средств ИБ? В частности, как вы оцениваете поручение Президента Правительству о переводе органов власти и внебюджетных фондов на российские средства шифрования? Каковы его возможные последствия?

Дмитрий БИРЮКОВ

Нужно вывести проблему на государственный уровень, проработать стратегию развития на несколько лет вперед, стимулировать появление совершенно новых направлений. В частности, нам нужно возродить отечественную элементную базу, которая сейчас крайне незрелая, слабая. Для этого необходимы мощные финансовые вливания в развитие технологий и соответствующей инфраструктуры, а также в обучение и формирование команд высококвалифицированных специалистов. Возможно, также потребуются некоторые изменения в области государственного регулирования в вопросах ИБ.

Стоит подумать и о дифференцировании требований регуляторов в зависимости от размеров бизнеса. Для крупных корпораций они могут быть одни, а для компаний более скромных масштабов – другие. На Западе такой подход широко практикуется. У нас же требования унифицированные к любому предприятию – от многофилиальных банков до организаций СМБ. В результате не учитываются финансовые возможности бизнеса и потенциальные бюджеты на информационную безопасность.

Инициативу применения российских средств шифрования мы поддерживаем и оцениваем позитивно – это правильный ход с точки зрения повышения защищенности нашего государства. Применение российских средств шифрования будет способствовать усилению безопасности как отдельных учреждений и структур, так и страны в целом.

В свою очередь, мы, как интегратор с большим опытом в сфере информационной безопасности, готовы поддержать наших клиентов на любом этапе построения систем защиты корпоративных данных.

Алексей КАЧАЛИН

Большинство мер, в частности, регламентация требований к встроенным механизмам защиты и процесса управления уязвимостями, требований по безопасной разработке и к системам обнаружения атак, интеграция систем сбора информации об атаках, сейчас активно продвигаются представителями регуляторов и практически не вызывают негатива со стороны как ответственных за создание и эксплуатацию ИТ-систем, так и разработчиков системного и прикладного ПО. Они воспринимаются как необходимые условия нормального развития ИТ в России.

Дмитрий ОГОРОДНИКОВ

Поручение Правительству было вызвано в первую очередь необходимостью разделения ответственности за использование средств шифрования в государственных структурах и пользователями сети Интернет, по отношению к которым ФСБ выпустило разъяснение, допускающее использование несертифицированных средств, т. е. это скорее была организационная процедура, которая не связана с поддержкой отечественных разработчиков. Но вот что им необходимо – это поддержка в виде масштабных и длительных государственных заказов на разработку полностью отечественных продуктов. Многие знают, что компания IBM выжила в кризис 1930-х гг. благодаря крупным государственным заказам, но мало кому известно, что в годы Второй мировой войны «Голубой гигант» выпускал стрелковое оружие

(карабин М1 и винтовку Браунинга) для армии США.

Алина ХЕГАЙ

Государство должно в первую очередь обеспечить достаточные условия для разработки ПО. Начало уже положено: вспомним хотя бы инициативы, связанные со Сколково. Крайне важно также уменьшить пропасть в развитии нормативной базы и используемых бизнесом ИТ.

Результаты поручения Президента Правительству оценивать еще рано: мероприятия по нему должны быть сформированы только к декабрю 2017 г. Можно предположить, что государственным органам в обязательном порядке придется отказываться от зарубежных алгоритмов и переходить на отечественные криптопровайдеры, встраивая их в ПО или используя наложенные средства абсолютно для всех электронных каналов взаимодействия с гражданами, в том числе порталов, которые работают по HTTPS. Им придется задуматься о том, каким образом компенсировать свои затраты на безвозмездное предоставление средств шифрования клиенту. Для некоторых потребителей подобный шаг может стать препятствием в использовании электронных услуг. В любом случае все будет зависеть от конечной реализации конкретных сервисов. ■

Серверы IBM под маркой YADRO

В день проведения в Москве Инфраструктурного форума IBM вендор объявил о том, что компания YADRO, член консорциума OpenPOWER Foundation, стала первым российским OEM-партнером, получившим сертификацию на компонентную сборку серверов на базе процессоров POWER. Технологическая компания YADRO («КНС групп») с собственным дизайн-центром стала девятым OEM-партнером в мире, который сертифицировал свое производство в соответствии с технологическими требованиями IBM, и третьим партнером в мире, которому разрешено выполнять компонентную сборку под своей маркой. По итогам первичного анализа производственного цикла YADRO компания IBM составила около 160 замечаний. «Мы упорно работали над тем, чтобы пункт за пунктом снять замечания и привести технологические процессы к тем нормам и критериям качества, которые вендор выдвинул в качестве требований», – пояснил коммерческий директор компании YADRO Александр Бакулин. Параллельно в несколько этапов осуществлялось обучение сотрудников на базе IBM.

Сегодня компания готова к сборке любых объемов продукции. Производственный цикл предусматривает одновременную сборку и заливку прошивок, а также тестирование 128 серверов в сутки. Собственно компонентная сборка включает полный цикл: от установки компонентов в чистом модуле, активации процессоров и памяти до комплексного тестирования, установки локализованного программного обеспечения и проверки электрической безопасности. Линия компонентой сборки появилась в дополнение к крупноузловой сборке, тестированию продукции и установке локализованного программного обеспечения на базе производственных мощностей в городе Шуя Ивановской области. Этап компонентной сборки реализован в рамках плана повышения локализации продукции YADRO. Опыт трансфера технологий и создания высокотехнологичного производства закладывает основу для развития производственных мощностей, необходимых для выпуска собственной продукции компании YADRO.

www.connect-wit.ru

Генеральный директор IBM в России и СНГ Андрей Филатов

Коммерческий директор компании YADRO Александр Бакулин