МНЕНИЕ /

Санкции не смогут повредить обеспечению кибер-безопасности

Внедрить единую экосистему решений

Сергей Шалимов,
руководитель направления по работе с технологическими партнерами компании «Аладдин Р.Д.»

ПРЕСС-СЛУЖБА «АЛАДДИН Р.Д.»

Сергей Шалимов: Надо заменить средства защиты на сертифицированные российские.

Переход с импортной операционной системы (ОС) на отечественную кажется тривиальной задачей. Но, чтобы не зависеть от санкций в сфере кибербезопасности, необходим комплексный подход и замещение всего технологического стека решений: клиентских ОС, прикладного ПО, серверных решений.

95 процентов российских объектов критической информационной инфраструктуры (КИИ) базируются на Windows Server Active Directory (AD), центре сертификатов Microsoft CA, веб-сервере IIS и базе данных Microsoft SQL, Oracle. Для обеспечения кибербезопасности нужно заменить все упомянутые решения и внедрить единую экосистему из отечественных компонентов.

Именно такую систему информационной безопасности (ИБ) и создает компания «Аладдин Р.Д.». Уже на этапе проектирования и разработки российских дистрибутивов Linux и СУБД мы интегрируем в них наши компоненты ИБ.

Первый из них—корпоративный центр выдачи и обслуживания сертификатов доступа Aladdin Enterprise Certificate Authority (Aladdin eCA), способный заменить Microsoft CA. Aladdin eCA позволит без дополнительных настроек разворачивать домены безопасности и обслуживать контроллеры доменов, серверы, сетевое и IoT/M2M оборудование, пользователей, обеспечить непрерывность и связанность сервисов при миграции с Windows на Linux.

Второй компонент—строгая двухфакторная аутентификация пользователей (2ФА) с использованием USB-токенов и смарт-карт.

Aladdin SecurLogon добавляет недостающие компоненты на клиентские ОС: автоматически конфигурирует ПК для единого входа в различные домены (Samba DC, FreeIPA, AD), поддерживает 2ФА в разных инфраструктурах, обеспечивает работу прикладного ПО с электронной подписью.

Третий компонент—сервер аутентификации. Многие компании уже столкнулись с блокированием подобных импортных сервисов. Решением может стать JaCarta Authentication Server (JAS), позволяющий продолжить использование имеющихся средств аутентификации—одноразовых паролей, USB-токенов, смарт-карт и U2F-токенов.

Для защиты баз данных от возможных утечек при миграции с MS SQL и Oracle на отечественные СУБД используется система Крипто БД.

И даже если переезд с Oracle невозможен, например, в случае с большими базами данных, Крипто БД позволяет там остаться, заменяя встроенные в Oracle средства защиты на сертифицированные российские. Система также «изолирует» обрабатываемые данные от самой СУБД, предотвращая их утечку.

Для защиты данных на дисках в Windows многие используют встроенную функцию шифрования BitLocker, при этом, рискуя полностью потерять к ним доступ. Наша альтернатива—Secret Disk—система прозрачного шифрования данных для Windows и Linux. ●

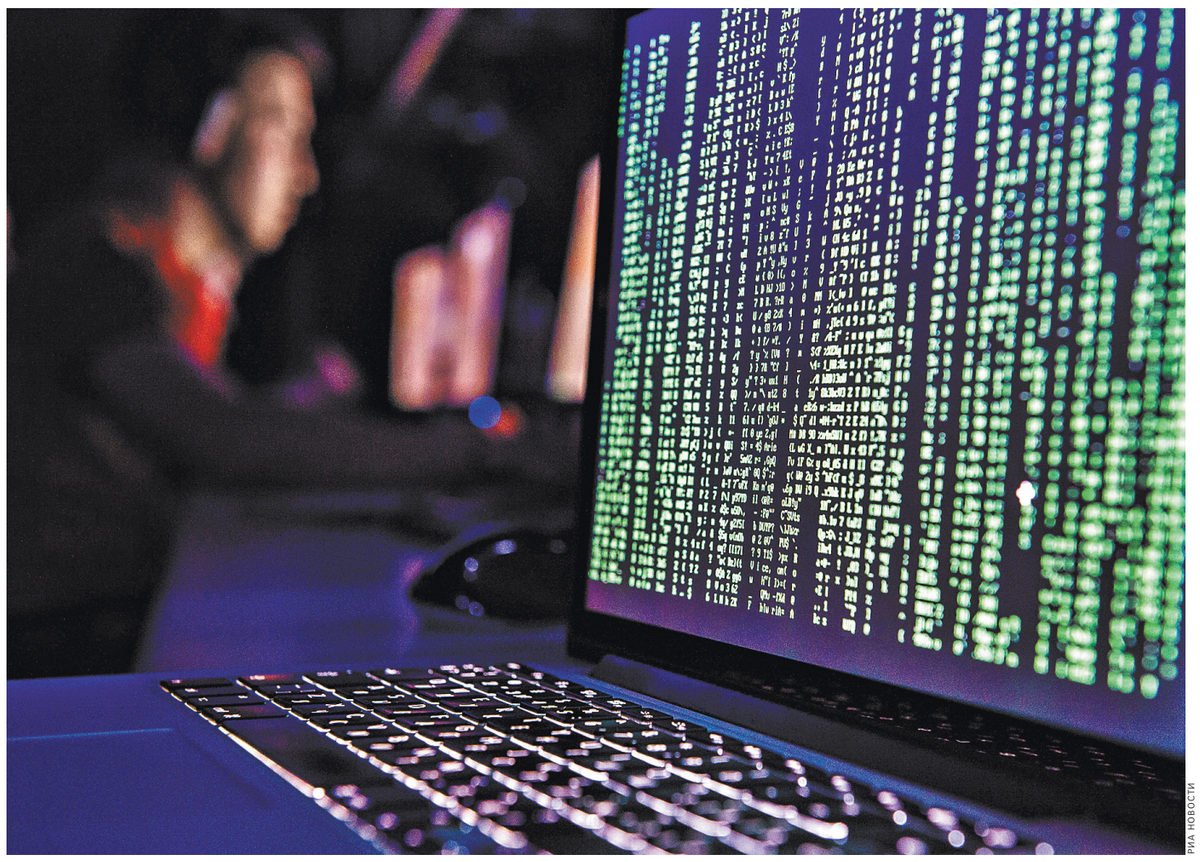
Замуровать «черный ход»

A1 — Целью атаки могут быть все элементы программно-аппаратного стека, не только собственно программный код вебсайтов, но и код инфраструктурных пакетов (операционная система, средства виртуализации или контейнеризации, среды выполнения управляемого кода и т.п.), а также микрокод контроллеров. Некоторые из подобных атак уже были реализованы, например, внедрение вредоносного кода в проекты с открытым исходным кодом—нашумевший случай деструктивных действий разработчика npm-пакета node-ipc, которые привели к проблемам по всему миру, не только в России»,—поясняет Роман Карпов.

Одна из причин роста киберугроз—уход с российского рынка иностранных поставщиков корпоративных средств информационной безопасности. «Зарубежные вендоры ушли с российского рынка, оставив свои продукты без техподдержки и обновлений, что влечет дополнительные риски информбезопасности для заказчиков,—рассказал «РГ» директор по инновационным проектам ГК InfoWatch Андрей Арефьев,—любая операционная система или программное обеспечение без своевременной поддержки обновлений подвержены уязвимостям, эксплуатируемым хакерами. Уже сегодня мы видим увеличение целенаправленных атак на российские компании, и этот повышенный интерес хакеров и злоумышленников вряд ли пропадет в ближайшее время, скорее, наоборот, возрастет».

В России, добавил эксперт InfoWatch, исторически сложилась сильная практика в области разработки ИБ-продуктов, направленных на защиту от различных типов угроз. Поэтому одной из важнейших задач является всестороннее усиление периметра российских организаций современными отечественными средствами защиты, несмотря на сложности, связанные с недостатком квалифицированного персонала в области ИТ и ИБ.

Разработка иностранного ПО зачастую включала внедрение уязвимостей в коммерческие системы шифрования, рассказали «РГ» в лаборатории искусственного интеллекта, нейротехнологий и бизнес-аналитики РЭУ им. Г.В. Плеханова. Там пояснили, что этим в свое время активно занималось Агентство национальной безопасности США. Поэтому почти в любом устройстве от смартфона до индустриального оборудования есть так называемый черный ход. Использование отечественного ПО способно снизить риски, связанные с такими лазейками.



РИА НОВОСТИ

Атаки злоумышленников на базы данных российских компаний будут только возрастать.

АКЦЕНТ

ЛЮБАЯ ОПЕРАЦИОННАЯ СИСТЕМА БЕЗ СВОЕВРЕМЕННОЙ ПОДДЕРЖКИ ОБНОВЛЕНИЙ УЯЗВИМА

«Для того чтобы обезопасить свой бизнес от взлома и потери работоспособности, следует выбирать провайдера с распределенной edge-инфраструктурой, а также постараться защитить свой ресурс от DDoS-атак на уровнях L3, L4 и L7,—советует генеральный директор EdgeЦентра Михаил Шурыгин.—Для того чтобы нейтрализовать крупномасштабные DDoS-атаки, нужно иметь действительно большие каналы связи, а также производительное серверное оборудование. EdgeЦентр располагает собственными центрами очистки трафика, а также каналами связи с широкой пропускной способностью, что позволяет выдержать атаки более 2 терабит в секунду. А это сопоставимо с мощностью самой крупной из зафиксированных DDoS-атак в мире. Инфраструктура Edge Центра распределена по многим городам России, Беларуси, Казахстана, Армении, Киргизии и Узбекистана. Подобное географическое распределение исключает возможность концентрации больших нагрузок на отдельный центр очистки».

Ситуация осложняется тем, что многие компании в России до недавних событий, недооценивая угрозу, не очень охотно вкладывались в свою защиту, считают в Аналитическом центре при правительстве РФ. Все атаки, безусловно, не отразить, но необходимо наверстывать упущенное—изыскивать ресурсы, укреплять или менять подходы к обеспечению информационной безопасности. И сейчас все зависит от изменения структуры мышления российского бизнеса—в среднесрочной перспективе ведущие позиции в России будут у бизнеса, миссия которого лежит много дальше сиюминутного профита.

«Переход российских предприятий на отечественное ПО и телекоммуникационное оборудование требует целого ряда шагов и определенного времени. Замена самого минимального набора программных продуктов (операционной системы, офисных приложений, антивируса, программы для видео-конференц-связи и бухгалтерской системы) потребует вложений, но главное—организационных усилий. Многим системным администраторам потребуется время для адаптации. Тем не менее в перспективе же данная мера даст новый мощный импульс развитию отечественного рынка программного обеспечения»,—сообщил «РГ» заведующий лабораторией искусственного интеллекта, нейротехнологий и бизнес-аналитики РЭУ им. Г.В. Плеханова Тимур Садыков.

Предстоит решить и проблему подготовки кадров ИТ. По оценке вице-премьера Дмитрия Чернышенко, в отечественной ИТ-отрасли не хватает около миллиона специалистов. Подготовить такое количество в один момент, конечно, невозможно. «Однако, если посмотреть на флагмана и законодателя практик безопасной разработки ПО—Институт системного программирования им. В.П. Иванникова РАН, то есть все основания полагать, что возможность вырастить достаточное количество экспертов все-таки есть,—считает Роман Карпов.—ИСП РАН активно сотрудничает с университетскими и исследовательскими центрами, что позволяет обучать и воспитывать новые квалифицированные кадры. В МГУ, МФТИ и ВШЭ работают кафедры системного программирования под руководством ИСП РАН, которые позволяют каждый год набирать более 100 студентов для обучения в бакалавриате и магистратуре. При условии наращивания темпа через 3–5 лет кадровый голод должен будет значительно снизиться, и государство сможет обеспечить информационную безопасность, основанную на собственных кадрах и технологиях». ●

Тем временем

Для защиты российского информационного пространства и инфраструктуры принимается широкий спектр мер. Так, указ президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной структуры Российской Федерации» запретил закупки иностранного программного обеспечения в целях его использования на значимых объектах критической информационной инфраструктуры нашей страны уже с 31 марта этого года. «Эта мера положит конец засилью продукции компании Microsoft в России и обеспечит широкое внедрение программного обеспечения с открытым кодом, российской технической поддержкой и сопровождением и репозиториями на территории нашей страны»,—подчеркнул «РГ» Тимур Садыков.

ГАРАНТИЯ /

Российские программы защитят предприятия от кибератак

Пора защищать, а не наблюдать

Игорь Душа,
технический директор InfoWatch ARMA

ПРЕСС-СЛУЖБА ГК INFOWATCH

Игорь Душа: Защита от кибератак сейчас более приоритетна, чем наблюдение.

Резкий рост интенсивности кибератак на российские промышленные предприятия создает впечатление, будто мы столкнулись с новым набором угроз и известные принципы защиты информации больше не работают. Однако все не так пессимистично. Типы атак, которые мы наблюдем сейчас, хорошо известны специалистам.

Что же тогда изменилось? Увеличилась частота атак, плюс с рынка стали уходить иностранные разработчики средств защиты, отключая обновления, а иногда и само ПО. Например, компания Cisco покинула нашу страну, оставив заказчиков с устройствами без обновлений. Для информационной безопасности такие устройства теперь бесполезны. Есть и более опасные случаи: иностранный разработчик без каких-либо уведомлений отключил клиентам ряд важных функций в ПО, оставив предприятия уязвимыми для атак.

Очевидный шаг для российских компаний в таких условиях—импортозамещение. С ним в сфере информационной безопасности дела обстоят неплохо—есть конкурентоспособное ПО для защиты промышленных систем. Выбор таких программных решений сейчас определяется двумя факторами: насколько легко их внедрить, получив работающую защиту с минимумом затраченных ресурсов, и может ли решение предотвращать атаки или только следить за происходящим. Скажу сразу—защита сейчас приоритетнее, чем наблюдение.

Разберем это на примере InfoWatch ARMA—системы защиты информации, разработанной в России специально для промышленных предприятий. Она состоит из трех компонентов, каждый из которых заменяет несколько классов решений иностранных аналогов. Первый компонент—промышленный межсетевой экран нового поколения—предотвращает атаки на сетевом уровне и может заменить аналогичные решения от Fortinet, CheckPoint, Tofino и др. Второй—промышленная защита рабочих станций и серверов, это альтернатива иностранным Endpoint-решениям, например, от McAfee или Symantec. Третий—центр управления системами защиты—позволяет увидеть цепочки событий в единой консоли, а не вылавливать из разрозненных средств защиты отдельные инциденты. Он может заменить иностранные системы централизованного управления от Cisco, McAfee и др. С помощью InfoWatch ARMA прямо «из коробки», минуя долгие и затратные интеграции, можно реализовать принцип эшелонированной защиты технологической сети—создать барьеры на каждом этапе проникновения злоумышленника. Вдобавок выполняется сразу 90 процентов технических мер Приказа №239 ФСТЭК России, который обязателен к исполнению для предприятий с объектами КИИ.

Второй принцип, подходящий для немедленной защиты,—это замкнутая среда. С помощью InfoWatch ARMA можно ограничить список операций только разрешенным перечнем, что лишает злоумышленника возможности проводить недопустимые действия. В итоге получаем сокращение поверхности и возможность предотвращения атаки—и все с помощью единой системы российской разработки. ●

АЛЬТЕРНАТИВА / Необходим масштабный переход на отечественные процессоры и ПО

Архитектура свободы

Инесса Суворова

Разговор о необходимости обеспечить совместимость отечественных программных продуктов между собой и с российским оборудованием начался еще восемь лет назад. Теперь, когда присутствие отечественных ИТ-компаний на рынке ПО стало быстро расти, процесс ускорился, заставив российских программистов и производителей провести срочную инвентаризацию того, что уже сделано.

За прошедшие годы в ИТ-сфере многое поменялось: новые отечественные разработки появились как в сегменте программного обеспечения (ПО), так и в «железе». Однако, по мнению экспертов, пока отечественная номенклатура покрывает лишь небольшую часть потребностей. И на полный переход к использованию российского цифрового продукта потребуется еще не один год.

—Надо понимать, что полностью отечественного «железа», точнее отечественных процессоров, в стране сейчас нет,—говорит заместитель генерального директора компании Postgres Professional Иван Панченко.—И чем более отечественным является процессор, тем труднее работа с ним. Для полностью отечественной архитектуры мы не можем пользоваться свободными или иностранными программными разработками, все приходится делать с нуля.

По его мнению, на сегодняшний день самой успешной отечественной разработкой является процессор «Эльбрус». Его производитель компания МЦСТ создает собственные компиляторы и низкоуровневое ПО, при этом достаточно быстро продвигается в этом направлении. Уже многие российские операционные системы работают на этих процессорах. Согласно каталогу АРПП (catalog.arppsoft.ru) на процессоре от МЦСТ в том числе работает и прикладное ПО—TrueConf, RAIDIX, Дело и Communigate. СУБД Postgres Pro также поддерживает «Эльбрус».

—Экосистема «Эльбруса» в последнее время сильно подросла,—говорит Иван Панченко.—Конечно, компиляторы МЦСТ, несмотря на все старания разработчиков, не полностью совместимы с тем, к чему привыкли другие разработчики, поэтому портирование на «Эльбрус»—сложная задача. Тем не менее основные российские ОС—Alt Linux и Astra Linux—работают на «Эльбрусе». Также объявлялось, что на нем работает ПО МФЦ госуслуг разработки ЭОС.

АКЦЕНТ

ТЕПЕРЬ БУДУТ НАИБОЛЕЕ ВОСТРЕБОВАНЫ ИМЕННО ЭКОСИСТЕМЫ, ЦЕЛОСТНЫЕ ЛИНЕЙКИ ПРОДУКТОВ И АППАРАТНО-ПРОГРАММНЫЕ КОМПЛЕКСЫ

Другой крупный производитель отечественного «железа», о котором говорит Иван Панченко—компания «Байкал». Ее процессор тоже является отечественным, несмотря на то что создан на платформе ARM иностранного происхождения. Поскольку платформа ARM очень популярна в мире и на ней работают свободно распространяемые компиляторы и инструментальные средства, то у «Байкала» по совместимости с отечественными ПО дела обстоят гораздо лучше, чем у «Эльбруса». Гипотетически, считает Панченко, может быть создан и отечественный процессор на базе «открытой архитектуры» RiscV.

Российский софт совсем не отстает от именитых зарубежных аналогов, а по многим показателям даже превосходит их. По словам директора по развитию бизнеса компании Vinteo Бориса Попова, при необходимом качестве и конкурентоспособности он, как правило, дешевле импортного. И перепрофилирование, например, на российские продукты ВКС класса telepresence идет максимально безболезненно, даже без необходимости замены имеющегося оборудования.

—На сегодняшний день в сегменте видеосвязи (ВКС) импортозамещение ПО выполнено практически на 100 процентов,—говорит Борис Попов.—Отечественные решения есть в каждом технологическом классе: и в веб-конференциях, и среди профессиональных решений telepresence. Например, протокольная и функциональная совместимость решений ВКС Vinteo с оборудованием видеоконференц-связи иностранных производителей (Cisco, Poly (Polycom), LifeSize, Avaya др.) обеспечивается в более чем в 95 процентов случаев, в том числе с устаревшими устройствами.

Проблема в том, что серверные процессоры российской разработки, способные составить конкуренцию зарубежным по обработке большого количества видеоданных, просто не успели полноценно выйти на рынок из-за введения санкций. Но, как отметил эксперт, типовые программные решения и кодеки видео-конференц-связи уже работают на отечественных процессорах, даже предназначенных для обработки лишь одного-двух потоков видео. Это итоги многолетней работы предыдущих лет.

—Наша компания вкладывает значительные средства и усилия разработчиков в тестирование всех доступных на рынке—в первую очередь отечественных—«железных» решений, а также в разработку собственных технологий,—говорит Борис Попов.—Сегодня мы еще не готовы заявить о каком-либо прорыве в этом направлении, однако уже можем с уверенностью сказать, что даже в узкопрофильной и крайне сложной нише технологий видео-конференц-связи «интелозамещение» вскоре состоится.

Типовым отечественным решением для безопасной видеосвязи и корпоративного общения на рабочих местах сотрудников госкомпаний и госслужащих по всей стране может стать предложение альянса UC 3.0, в который входят CommuniGate Systems, Vinteo, eXpress и Neutronix. Компании предлагают SuperApp на основе мессенджера с возможностями видеосвязи, телефонии, офисной АТС, управлением задачами, сложными календарями и пр. По сути, это система для любых корпоративных коммуникаций с высоким уровнем защиты информации. Именно такие решения унифицированных коммуникаций интересны сегодняшним заказчикам не только из государственного сектора, но и из бизнес-сферы.

АКЦЕНТ

НА СЕГОДНЯШНИЙ ДЕНЬ САМОЙ УСПЕШНОЙ ОТЕЧЕСТВЕННОЙ РАЗРАБОТКОЙ ЯВЛЯЕТСЯ ПРОЦЕССОР ЭЛЬБРУС

По словам заместителя генерального директора компании РЕД СОФТ Рустама Рустамова, тестирование на совместимость российских программных и аппаратных продуктов в их компании с 2014 года стало одним из приоритетных направлений работы.

—Сейчас в Реестре отечественного ПО зарегистрировано четыре тысячи производителей и внесено почти 13 тысяч продуктов, которые представляют весь спектр решений, от операционных систем, СУБД и офисных приложений до специализированных программ,—говорит Рустам Рустамов.—Только в прошлом году наша компания обрела более 100 новых технологических партнеров среди российских разработчиков. Аналогично мы работаем и с каталогом Минпромторга России, тестируя уже готовые решения на российском «железе», в том числе на базе российских процессоров, в частности, Baikal-M.

Результатом этой работы стало создание и внедрение автоматизированных рабочих мест (АРМ). Среди заказчиков РЕД СОФТ—Пермский край, Калужская область, Ставропольский край, Волгоградская область и другие регионы. Наши решения применяются и на объектах КИИ, в частности, в ТЭК.

Именно экосистемы, цифровые платформы, целостные линейки продуктов и аппаратно-программные комплексы, предлагающие полный цикл решений, будут наиболее востребованы в сегодняшних реалиях. Первый в России полностью отечественный программно-аппаратный комплекс для развертывания инфраструктур виртуальных рабочих мест на базе собственных продуктов разработали ГК «Астра» и ГК Delta Solutions. Заказчиком разработки стал Концерн «Росэнергоатом».

—Такие проекты позволяют отвязать пользователя от конкретного «железа» и обеспечить его удаленный доступ к компьютеру из любой точки мира,—говорит директор по решениям импортозамещения ИТ-компании КРОК Наталия Софронова.—Для их тиражирования и дальнейшего успешного внедрения нужна серьезная инвестиционная поддержка в рамках приоритетных сквозных проектов, к которым сегодня относится программно-аппаратные комплексы, вычислительная техника, цифровая энергетика и другие сегменты электроники.

По мнению Наталии, формат сквозных проектов на сегодняшний день является наиболее эффективным инструментом для достижения целей импортозамещения в сфере вычислительной техники. В рамках сквозных проектов разработчики «железа» находятся в тесном контакте с разработчиками программного обеспечения, что впоследствии позволяет избежать проблем, связанных с несовместимостью оборудования и софта.

В настоящее время готовятся к реализации сквозные проекты в сфере вычислительной техники. Это и перевод информационной инфраструктуры российских корпораций, стационарных и мобильных рабочих мест на базу отечественных процессоров, и создание отечественного АРМ нового поколения, а также отечественных программно-аппаратных комплексов для корпоративных облачных и информационных платформ. Перевод позволит увеличить количество успешных примеров комплексных решений, совмещающих отечественные процессоры и операционные системы, которых в России уже немало. Учитывая, что сферу ИТ-технологий, возможно, внесут в число национальных проектов, есть вероятность ускорения этого процесса. ●