ГРИГОРИЙ СИЗОНЕНКО,
генеральный директор компании ИВК

Главные направления российского рынка ИБ: опасайтесь экстраполяции прошлых трендов

Сегодня большинство экспертов и участников рынка, пытаясь прогнозировать динамику развития отечественного ИБ, на первое место ставят фактор импортозамещения и… останавливаются на этом. Но такой прогноз не только практически очевиден и почти бесполезен, ведь он не показывает конкретные направления развития, их взаимосвязи, не выявляет ловушки. Он еще и создает ложную успокоенность: и разработчикам, и заказчикам может показаться, что развитие рынка будет происходить само собой –по прежней траектории. Но это не так. Я утверждаю это на основании реального опыта компании ИВК, которая вот уже 20 лет занимается разработкой и внедрением отечественных системообразующих технологий и продуктов в сфере ИТ и ИБ, позволяющих создавать безопасные информационные системы всероссийского масштаба для госструктур, силовых ведомств. То есть именно тем, что теперь получило название импортозамещения.

Несомненно, усиление государственного регулирования является ведущим фактором развития не только рынка ИБ, но и всего отечественного ИТ-рынка. Технология была «обкатана» на защите персональных данных. Стало ясно, что это стратегическая линия, которую государство внедряет достаточно мягко и не без ошибок, но последовательно. Теперь та же ситуация складывается в сфере импортозамещения, но в гораздо большем масштабе. Как импортозамещение будет взаимодействовать с другими тенденциями, например, непростым состоянием экономики и сокращением ИТ бюджетов? Как все это повлияет на рынок ИБ? Как отразится на заказчиках и разработчиках? И насколько серьезно развитие рынка ИБ будет отличаться от простой экстраполяции прошлых трендов? Сегодня именно эти вопросы имеют первостепенное значение. И данная статья, надеюсь, даст если не готовые ответы на них, то информацию для размышления.

Почему экстраполяция не работает?

За прошедший год меня не раз спрашивали о том, для каких направлений ИБ выбор российских продуктов достаточно широк, а в каких областях пока еще сложно заменить зарубежные решения? На мой взгляд, этот вопрос не будет оказывать решающего влияния на рынок.

Общее состояние «объединенного продуктового портфеля» сегодня хорошо известно. Там, где обрабатывается государственная тайна или просто чувствительная для государства информация, импортозамещение ничего не меняет: здесь и так использовались только отечественные разработки, поэтому «импортозамещать» просто нечего. Разумеется, силовые ведомства и спецслужбы также изначально ориентированы на отечественные разработки в сфере ИБ.

На рынке же ИБ для коммерческих организаций ситуация иная. Здесь отечественное ПО пробивало и пробивает себе дорогу в тяжелой конкурентной борьбе с противником, имеющим не только качественные ИТ-решения, но и неограниченные финансовые ресурсы, мощь брендов, агрессивный международный маркетинг, выстроенные каналы продвижения через системных интеграторов. Кроме того, десятилетиями российские организации отдавали предпочтение зарубежным решениям, таков был долгосрочный вектор развития ИТ-рынка. Немногие отечествен-


SHUTTERSTOCK.COM/SI_NYAM_NYAM

ные разработчики сумели выстоять в этой борьбе, выведя свои продукты на уровень функциональности, зрелости и технической поддержки, отвечающий требованиям крупного предприятия (сегмента enterprise). Причем, пока все это – разработки, возникшие задолго до провозглашения политики импортозамещения. И именно поэтому сегодня мы имеем зрелые конкурентоспособные продукты практически во всех ключевых сегментах ИБ-рынка. Вот несколько примеров: антивирусное ПО (Лаборатория Касперского и Доктор Веб), DLP (Infowatch), системообразующее инфраструктурное ПО класса middleware с интегрированными средствами ИБ (ИВК), контроль и управление доступом (Аванпост, производители токенов и др.). Для некоторых категорий ИБ-продуктов отечественных решений, насколько я знаю, пока нет. Трудно заменить, скажем, системы корреляции событий. Их созданию пока мешает слишком узкий внутренний рынок. Если он расширится, то решения появятся.

Значит ли все это, что теперь, когда отечественное ПО получило преференции, рынок ИБ, продолжая развиваться по прежней траектории, будет расти как на дрожжах? А информационные системы станут, наконец, значительно безопаснее? К сожалению, нет.

Линейной экстраполяции мешает несколько существенных моментов. В первую очередь, надо учесть, что первостепенным фактором роста ИТ- и ИБ-рынков является создание и развитие крупных информационных систем всероссийского масштаба с высокими требованиями к защищенности информации. В качестве примера отмечу две такие системы, к которым наша компания имеет прямое отношение – ГАС Правосудие и система электронного документооборота в Министерстве обороны РФ. При этом защищать нужно не отдельные элементы или функции, а информационную систему в целом. Это изменение носит принципиальный характер, ниже мы к этому вернемся. К сожалению, пока по пути защиты системы в целом идут только наиболее дальновидные организации, а таких всегда немного. Их число неуклонно растет, но медленно. Более того, это изменение пока не стало определяющим в стратегии интеграторов и разработчиков ПО.

Во-вторых, в ходе импортозамещения нужно исправлять ошибки проектирования информационных систем, допущенные при «островной информатизации». Ведь некоторые архитектуры просто невозможно защитить, сколько ни вкладывай в это денег и интеллектуальных усилий. Например, это касается непродуманных способов интеграции элементов ИС. Или построения крупных систем на основе любого варианта синхронного взаимодействия ее элементов – вместо применения механизма очередей.

Третья сложность и источник новых рисков связана с тем, что в информационных системах начинает широко применяться отечественное проприетарное и свободное ПО, а также свободное ПО (СПО), развиваемое международным сообществом разработчиков. При этом такие продукты зачастую сразу становятся системообразующим элементом ИБ или ИС. Наиболее яркий пример последнего тренда – использование свободного ПО Samba DC в качестве альтернативы Microsoft Active Directory (именно в этом качестве Samba DC полностью поддерживается первой отечественной ОС уровня предприятия, созданной компанией «Базальт СПО» и сообществом «Сизиф»).

Кроме того, важно учитывать, что замена ПО в ИС предприятия – это чрезвычайно сложный и длительный процесс, в ходе которого замещающая и замещаемая подсистемы сосуществуют и должны

поддерживать согласованную работу ИС в целом. Причем это относится не только к прикладному ПО, но и к системообразующим элементам и подсистемам ИС и ИБ (операционные системы, служба каталогов, СУБД и т. д.)! Как защитить такой объект? Здесь требуется особый подход, на котором я остановлюсь ниже.

А сейчас давайте присмотримся к этим новым факторам, чтобы почувствовать глубину их влияния на задачи ИБ.

Что защищаем?

В чем разница между защитой системы в целом и защитой ее элементов. Почему второе не перерастает в первое?

В первом случае цель состоит в том, чтобы информация была гарантированно защищена на всех этапах обработки: при хранении, передаче, предоставлении доступа к ней пользователю, при трансграничной передаче партнерам. Чтобы на всем пути ее логической обработки (которая может охватывать множество территориально удаленных единиц) была гарантирована ее целостность и подлинность, гарантированно соблюдались и контролировались регламенты обработки, например, своевременность каждого действия (ведь во многих случаях злоумышленнику, чтобы нанести ущерб, достаточно лишь задержать какие-то данные, исключив их из процесса принятия решения). Кроме того, система должна гарантированно защитить каждый свой узел от непреднамеренной или умышленной подмены ПО, а поврежденные узлы – автоматически изолировать, оповестив соответствующих должностных лиц.

А во втором случае, образно говоря, организации старательно укрепляют дверь, навешивают замки и цепочки (скажем, защищают периметр организации или внедряют DLP), не обращая внимание, что рядом находится распахнутое окно, через которое злоумышленник действует совершенно свободно. К сожалению, большинство государственных и коммерческих организаций пока идут именно по этому, а не по первому пути. Результат все мы видим: на ИБ тратятся астрономические суммы, а злоумышленники попрежнему добираются до секретных данных, клиентские базы продолжают утекать. Защищая отдельные элементы, систему защитить нельзя.

Как видим, водораздел между двумя подходами проходит по нескольким линиям. Это: степень интеграции ИБ с функциями ИС, полнота защиты и гарантированный характер сервисов уровня ИТ и ИБ.

Решенные проблемы ИБ возвращаются

Еще одна важнейшая задача организации – помешать одним людям выдавать себя за других, ведь сегодня такая подмена лежит в основе многих компьютерных преступлений. Если злоумышленнику удается выдать себя за легитимного пользователя, которому вполне легально открыт доступ к конфиденциальной или секретной информации, то такой замаскированный враг разом обходит все системы ИБ, какими бы они ни были сложными и дорогими. Для них его просто нет.

Особенно острой эта проблема становится в периоды кризисов. Люди теряют рабочие места, сталкиваются со снижением реального уровня доходов,

SHUTTERSTOCK.COM/REENYA

с неопределенностью перспектив. Это создает благоприятную почву для роста компьютерных преступлений, опирающихся на инсайдеров. В то же время, из-за возросшей конкуренции усиливается промышленный шпионаж и попытки нарушить деятельность конкурента, воздействуя на его информационную систему. Обе линии смыкаются, что создает значительные риски, на которые организации должны реагировать.

Хорошо известно, что одно из наиболее эффективных средств противодействия инсайдерам – это и системы IDM, и усовершенствованные средства аутентификации (биометрические, с помощью аппаратных ключей и др.), и многофакторная аутентификация. Казалось бы, беспокоиться не о чем. Тем более, что в этой сфере есть чрезвычайно эффективные отечественные разработки, не уступающие лучшим западным аналогам. Однако пока они гораздо менее распространены, чем должны бы. Но даже если они используются, это может не дать ожидаемого результата. Например, из-за отсутствия у IDM-системы коннекторов к каким-то элементам ИС. Эта проблема резко обострилась в связи с неизбежным появлением на всех этажах информационных систем нового ПО – от отечественных разработчиков и от международного сообщества Open Source.

Пример с IDM я привожу не потому, что это особо проблемный участок. Скорее, наоборот. Но именно поэтому IDM хорошо иллюстрируют два общих положения. Технические средства должны быть интегрированы в сбалансированную защиту информационной системы как целого, а не составлять бастион, который трудно взять, но легко обойти. И еще: новые виды ПО создают не только очевидные риски (например, трудную притирку к сложившемуся ИТ-ландшафту), но и такие, которые пока даже не учитываются никем, кроме, вероятно, злоумышленников.

Обращение к теме инсайдеров позволяет четко высветить еще несколько проблем. Для сферы ИБ до сих пор характерны низкая грамотность и даже какой-то нигилизм. О беспечном отношении к учетным данным кто только не говорил. А топ-менеджеры почти всегда используют свое влияние, чтобы отменить как можно больше механизмов защиты. Хотя риски этого очевидны. Очень многие организации даже не разъясняют сотрудникам, где проходит граница между открытой информацией и коммерческой тайной. И легко становятся объектом социальной инженерии, как правило даже не подозревая об этом. Противодействие усложняется тем, что зачастую злоумышленники действуют сразу против нескольких территориальных единиц, а организация, даже зафиксировав отдельные попытки, не может собрать все элементы атаки в одно целое. Защитить информационную систему только техническими средствами нельзя, необходимы усилия и на организационном уровне.

Топ-менеджеры почти всегда используют свое влияние, чтобы отменить как можно больше механизмов защиты

Время технологических платформ с интегрированными средствами ИБ

Так как же защитить информационную систему как целое с у четом всех вышеперечисленных и многих оставшихся за кадром проблем?

Если посмотреть на вопрос глазами организации-заказчика, то сегодня наиболее правильный шаг – это построение новых и перестраивание существующих информационных систем на базе целостных технологических платформ с интегрированными функциями ИБ. Отмечу желательность построенния таких платформ на базе ПО middleware, ориентированного на передачу сообщений (message-oriented middleware или MOM). Взаимодействие элементов системы через очереди улучшает такие важные ее свойства, как надежность и отказоустойчивость, формирование доверенной среды для прикладного ПО, интеграция элементов ИС, работа с унаследованным ПО (теперь в эту категорию попадает не только старое, которое плохо вписывается в новые ИС или которое не имеет поддержки разработчиков, но и все западное проприетарное ПО!), возможность опираться на любые системы связи (очень важно для нашей страны!), упрощение миграции на новые виды ПО, способность переживать (без прекращения работы системы) смену поколений оборудования, операционных систем и др. Но эти вопросы выходят за рамки данной статьи.

Хорошая технологическая платформа – это готовое отлаженное сочетание свободного и проприетарного ПО. При этом платформа скрывает (инкапсулирует) сложности выбора и интеграции продуктов, а также замены одних продуктов на другие. (Разумеется, поставщик платформы должен брать на себя ответственность за ее неограниченно долгое развитие, за качественную техническую поддержку, за полную маскировку от потребителя особенностей и сложностей взаимодействия с другими отечественными разработчиками и международными сообществами Open Source.) Заказчику, решившему широко применять свободное ПО, технологическая платформа возвращает привычные характеристики проприетарных решений: поддержку вендора, принцип одного окна, наличие единой точки ответственности за огромный пласт технологий.

Множество сложнейших в реализации функций хорошая технологиче-

ская платформа предоставляет в виде готовых гарантированных сервисов. За счет этого прикладное ПО резко упрощается, ведь сложности системной части выносятся за рамки конкретных проектов, а заказчик может полностью сконцентрироваться на прикладной части, т. е. именно на том, в чем он заинтересован и разбирается. Средства ИБ интегрированы в функции платформы, которая, в частности, может автоматически контролировать целостность всего ПО в системе: прикладного и системного. Более того, такая технологическая платформа позволяет решить сложнейшую задачу, о которой я говорил выше, – обеспечить информационную безопасность в период длительного сосуществования замещаемых и замещающих продуктов.

Организация, перейдя на систематическое использование технологических платформ, не только решает ранее неразрешимые задачи ИБ, но и получает огромную экономию времени, уверенность в успехе проекта, а также единую точку ответственности за инфраструктурную составляющую. И значительно упрощает сопровождение и развитие системы.

Разумеется, заказчику стоит удостовериться, что у выбранной им платформы есть все нужные ему возможности. Еще лучше, если их наличие подтверждено в ходе сертификации.

Как вписать инфраструктурное ПО Open Source в систему ИБ предприятия

Особо хочу остановиться на важнейшем вопросе, которому почему-то не уделяют достаточного внимания ни разработчики, ни интеграторы, ни заказчики информационных систем.

Сделав ставку на широкое использование OpenSource-технологий, государство приняло правильное стратегическое решение. Но внедрение открытого ПО отнюдь не сводится к простейшему алгоритму: скачал – установил – заработало. Из огромного разнообразия надо выбрать что-то действительно подходящее, интегрировать разрозненные компоненты в единую систему, добавить новые функции – причем так, чтобы конечная сборка не перестала работать. А еще надо конструктивно взаимодействовать с сообществами, развивающими каждый продукт. Чтобы создавать работающие ИС, всем сторонам – разработчику, интегратору и заказчику – нужна готовая технологическая платформа, снимающая с них все эти вопросы. Сам по себе Open Source платформой как таковой не является. Скорее, это набор хороших (а иногда не очень) технологий и компонентов.

Очевидно, что будущее информационных систем для госсектора – это не чистый Open Source. В реальных ИС гражданского назначения 20–25 % кода будет приходиться на совершенно обязательное проприетарное ПО прикладного и инфраструктурного уровней, созданное и поддерживаемое российскими компаниями. В эту категорию попадают подсистемы ИБ (особенно если ИС обрабатывает персональные данные и гостайну), средства интеграции унаследованных систем, а также – и это исключительно важно! – программный код, превращающий совокупность свободных информационных технологий и продуктов в целостные технологические платформы. Разумеется, в системах специального назначения доля проприетарного ПО будет намного выше – вплоть до 100 %.

Специфика регионов

Говоря о направлениях развития отечественного рынка ИБ, нельзя не коснуться специфики российских регионов. Здесь очень многое зависит от двух факторов: экономической ситуации в регионе и позиции первых лиц Администрации, отвечающих за информатизацию. Если последние заинтересованы в эффективном контроле за деятельностью коммерческих компаний, то в различных региональных госструктурах появятся проекты сбора и анализа данных. Если власти заинтересованы в развитии малого бизнеса, появятся информационные порталы, выгодно представляющие товары и услуги местных предприятий, а также способствующие развитию деловых сетей. Если власти хотят улучшить работу системы здравоохранения, появляется телемедицина, в масштабах всего региона может появиться катастрофоустойчивая защищенная масштабируемая инфраструктура хранения и обработки данных, которой могут пользоваться и ЛПУ, и информационные порталы медицинской направленности. Знаю это точно, т. к. в таких проектах наша компания участвовала как поставщик системообразующих инфраструктурных ИТ-решений.

Говоря о специфике регионов, я бы особо подчеркнул два момента: географическую протяженность и малую плотность населения. Если больному или просто пожилому человеку приходится ехать в поликлинику добрую сотню километров, то для большей части населения это будет означать отсутствие медицинской помощи. В такой ситуации лучшим решением являются подвижные медицинские бригады и лаборатории, в зависимости от региона и времени года передвигающиеся по сельским дорогам или по рекам или водоемам. А это полностью меняет подходы к архитектуре информационных систем, к размещению данных, к информационной безопасности. Это актуально и для Юга России (например, Астраханской области), и для Сибири и Крайнего Севера, да и для всей российской глубинки.

Плотность населения влияет, в частности, на то, какие средства связи реально доступны для подключения к Интернет (для дистанционной работы, дистанционного обучения, получения информации и услуг по самым разным вопросам). Как, например, без интернета удаленно записаться на прием в госучреждение или ЛПУ, как заглянуть на медицинский портал или получить консультацию?

Все это определяет большое разнообразие создаваемых систем. И если применение многих средств ИБ практически не зависит от того, в каких ИС они используются, то защита информационной системы в целом не может

быть настолько же слабо связана с ее спецификой. Но здесь четко проявляется еще одно преимущество платформенного подхода к ИБ. Ведь, как мы говорили выше, ИБ интегрирована в гарантированные сервисы платформы (по хранению, передаче и обработке информации). И эти сервисы распространяются и на стационарный, и на мобильный сегменты информационной системы. Внедрив такую платформу ради какого-то одного решения, организация получает универсальную среду, гармонизирующую архитектуру и систему защиты всех ИС организации.

На чем основаны мои оценки

Бич современного информационного пространства в сфере ИТ – засилье псевдоэкспертов, готовых давать рекомендации о чем угодно. Особенно это касается вопросов, связанных с импортозамещением. Поскольку в этой статье я говорю о фундаментальных для рынка вещах, способных повлиять на стратегию компаний и, соответственно, на результаты их основной деятельности, считаю необходимым представить тот опыт, на котором основаны мои суждения и рекомендации.

В СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ДОЛЯ ПРОПРИЕТАРНОГО ПО БУДЕТ НАМНОГО ВЫШЕ – ВПЛОТЬ ДО

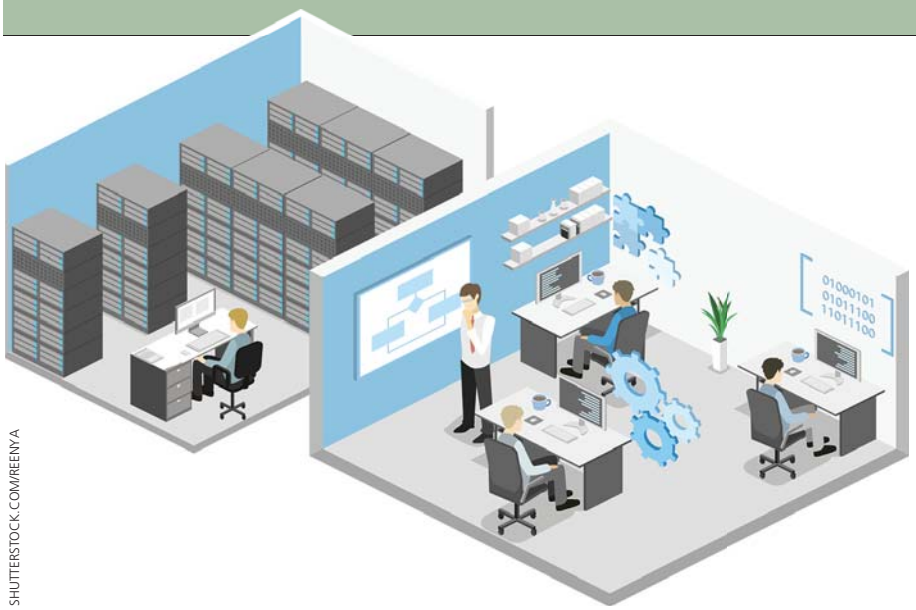
100%

SHUTTERSTOCK.COM/ENOTMAKS

ИВК разрабатывает полностью отечественные инфраструктурные информационные технологии и ИТ-продукты с 1997 года. И ни разу не свернула с этого пути, несмотря на всем известные кризисы в экономике и общую линию на применение западного ПО, десятилетиями господствовавшую на нашем ИТ-рынке. В 2002 г. выпущено системообразующее ПО middleware с интегрированными функциями ИБ «ИВК Юпитер» для комплексного решения задач информатизации территориально-распределенных структур. А в 2004 увидела свет наша первая разработка, полностью основанная на ПО Open Source, совмещающая функции межсетевого экрана с расширенной функциональностью и коммуникационного центра организации.

Сегодня компания располагает достаточно широким и полным набором собственных инфраструктурных технологий и основанных на них зрелых ИТ-продуктов, чтобы на их основе создавать и эксплуатировать территориально распределенные информационные системы любого масштаба с высокими требованиями к информационной безопасности и сложности обработки информации. Наши разработки сертифицированы и защищены патентами РФ. Также компания проектирует и выпускает промышленные компьютеры и вычислительную технику со спецсвойствами, основными потребителями которой сегодня являются силовые ведомства и госучреждения. В обеих линейках (ПО и аппаратное обеспечение) есть решения стационарные и мобильные.

Среди этих разработок имеются две технологические платформы, первые версии которых были выпущены в 2012 и в 2015 гг. Это первые отечественные продукты такого класса, до сих пор не имеющие аналогов на нашем рынке. Обе эти платформы предназначены для ускоренного создания и упрощенного обслуживания безопасных территориально распределенных информационных систем любой сложности. Обе основаны на наших многолетних разработках. И обе позволяют защитить



SHUTTERSTOCK.COM/REENYA

информационную систему в целом. Но на этом их сходство заканчивается.

Первая технологическая платформа ИВК – полностью проприетарная. Она предназначена, главным образом, для закрытых систем, где заказчику требуется российский продукт без заимствований кода, минимальное число точек сопряжения ИС с внешним миром, а также гарантированная поддержка множества унаследованных вычислительных систем и полная уверенность в отсутствии недекларированных возможностей, удостоверенная сертификацией в компетентных органах РФ.

Сфера преимущественного применения этой платформы – информационные системы с очень высокими требованиями по безопасности (конфиденциальные сведения и гостайна), где никакой открытости не должно быть по определению. Заказчики – силовые ведомства и некоторые госструктуры. Второй целевой рынок – различные системы технологического уровня, которые сегодня все чаще становятся объектами тщательно подготовленных атак, что создает огромные риски. Пока этот сегмент невелик, но он быстро расширится, если отечественная промышленность будет развиваться. Еще одна перспективная область – автоматическое взаимодействие систем (без участия человека), например, слаженная работа промышленных роботов в условиях техногенной аварии, взаимодействие звена дронов и т. п.

Вторая технологическая платформа ИВК на 85 % основана на открытом ПО (Open Source) и нацелена на открытый рынок. Но и она отвечает всем требованиям безопасности – за счет остальных 15 % закрытого кода, который, с одной стороны, обеспечивает соответствие российским требованиям к ИБ, а с другой, – превращает россыпь опенсорсных продуктов в единое целое.

Мы параллельно развиваем обе платформы, поскольку они отлично дополняют друг друга.

В настоящее время платформы и продукты ИВК служат фундаментом для десятков информационных систем, включая такие, как ГАС Правосудие, система электронного документооборота Министерства обороны РФ, система обработки обращений граждан и др.

Заключение

Импортозамещение – вполне адекватный ответ на реальные риски сегодняшнего дня. Мы увидели, как легко наши зарубежные «партнеры», прежде веско говорившие о нерушимости договорных обязательств и о своей ответственности за информационные технологии в рамках международного разделения труда, прекращают его техническую поддержку и переходят к шантажу. Это – реальная угроза основной деятельности наших госструктур, госкорпораций и крупнейших коммерческих компаний.

Но с проприетарным зарубежным ПО связаны и другие риски. Например, учрежденческая АТС, операционная система или какое-либо инфраструктурное ПО вдруг начинает передавать куда-то какую-то информацию. Куда? Какую? Кем и как она может быть использована? Недавний скандал с Windows 10 показал, что ОС стала средством сбора информации о пользователях. А если это госучреждение? Или крупная компания? Ведь ясно, что информация, скажем, об одном-двух колодцах не представляет большого интереса. Но объединив все такие данные, получаем достоверную информацию о системе водоснабжения. И так в любой области. Думаю, не только госструктурам и госкорпорациям пора задуматься о практическом импортозамещении, но и любым дальновидным руководителям, не желающим, чтобы какие-то внешние структуры имели прямой доступ ко всей информации в их организации. Начать стоит, на мой взгляд, с операционных систем, почтовых систем, СУБД, АТС. А потом заменить и офисное ПО.

Но на этом пути защищенность информационной системы не должна снижаться. Ни из-за перехода на новые виды ПО, ни из-за исправления ошибок прошлой информатизации, ни из-за того, что миграция растягивается надолго. Поэтому именно системная защита информационных систем в целом (простите за использование однокоренных слов) – это самое важное и перспективное направление развития отечественного рынка ИБ на ближайшие годы.

Безусловно, здесь многое зависит от функциональности и качества отдельных ИБ-продуктов. Но определяющим является именно переход от защиты элементов к защите систем как целого. Именно такой должна быть эффективная стратегия информационной безопасности в российской госструктуре или коммерческой компании.

А технологические платформы позволяют реализовать эту стратегию, одновременно получив огромные преимущества в сроках внедрения, эксплуатационных и экономических характеристиках решений. ●

КЛУБ

ДИРЕКТОР
ПО БЕЗОПАСНОСТИ

СПЕЦИАЛИСТАМИ НЕ РОЖДАЮТСЯ,

ИМИ СТАНОВЯТСЯ