Импортозамещение
или технологический суверенитет?

Андрей НЕКЛЮДОВ,
ведущий инженер,
ООО «Газинфомсервис»

Илья ЛИВШИЦ,
ведущий инженер,
ООО «Газинфомсервис»

Проблема импортозамещения, внимание к которой особенно усилилось в последнее время, получила широкое распространение на все сферы деятельности, в том числе на область защиты информации. Следует заметить, что решения в области защиты информации всегда подчинялись определенным строгим правилам игры, часть которых формировал рынок, но в основном – государственные регуляторы. Соответственно при оценке текущей ситуации необходимо определить, что было сделано в области защиты информации в РФ до настоящего времени, что делается сейчас и какие тенденции следует принять во внимание для успешной защиты от возможных негативных воздействий в будущем. Можно предложить следующую формулировку исследуемой проблемы: является ли возможным решение глобальной проблемы защиты информации на современном уровне при решении локальных задач импортозамещения (технических, технологических, методических) и какие условия при этом необходимо принять во внимание?

Рассмотрение проблемы удобно начать с анализа главной стратегической цели – обеспечения технологического суверенитета в области информационной безопасности (ИБ). Понятие «ИБ» уместно применить по причине того, что оно представляется намного более общим, чем только практическая задача по защите информации.

Особенности технологического суверенитета

В июне 2016 г. случился казус: в реестре российского программного обеспечения (ПО) были обнаружены (https://reestr.minsvyaz.ru/reestr/) экземпляры, помеченные как российские, но даже признаки принадлежности к известным иностранным продуктам выступали столь вопиюще, что правда была восстановлена (это решения «Логика ECM ASL.СЭД», «Карельская медицинская информационная система» и «M1: ECM Платформа»). Просмотр реестра российского ПО сопровождался мыслью, которая родилась уже несколько лет назад при анализе ландшафта индустрии информационных технологий (ИТ) в России. По нашему мнению, никакое импортозамещение не приведет к положительным тенденциям без обретения технологического суверенитета в области ИТ.

Отсутствие технологического суверенитета в области ИТ досталось России по наследству от СССР, который к моменту своего распада утратил возможность эффективно использовать существовавшие ранее заделы по названной тематике. Под технологическим суверенитетом подразумевается такое устойчивое и наблюдаемое состояние, когда реализация ИТ возможна исключительно на основе компонентов, которые производят организации

в пределах юрисдикции России и имеют на них исключительные права.

Правовая база

Первым условием достижения технологического суверенитета в области ИТ является правильное целеполагание, что обеспечивается использованием адекватных нормативных документов. В начале нынешнего века в блоке западных стран на разных уровнях было достигнуто понимание необходимости отнесения вопросов ИБ к сфере компетенции ИТ. Это обусловлено бурным развитием ИТ, в ходе которого средства обработки информации насыщались встроенными функциями безопасности, так что потребность в средствах безопасности вне контекста ИТ («наложенных» средствах ИБ) сошла на нет.

Рассмотрим, какие существенные изменения произошли в области методического обеспечения ИБ в наиболее значимых организациях в мире. В США был выпущен закон Federal Information Security Management Act (FISMA), во исполнение которого NIST разработал ряд нормативных документов, предусматривающих принципиально новый подход к организационному обеспечению ИБ. Документы знаменитой ранее «радужной серии» утратили статус действующих. Также на международном уровне были приняты стандарты ISO/IEC 15408 Information technology. Security techniques. Evaluation criteria for IT security и ISO/IEC 27001 Information technology. Security techniques. Information security management systems. Requirements. Отметим, что все указанные стандарты переведены в настоящее время и являются национальными стандартами систем ГОСТ Р ИСО/МЭК.

Таким образом, национальными и международными регулирующими органами во взаимодействии с обладающими технологическим суверенитетом представителями индустрии ИТ была обеспечена адекватная нормативная поддержка полного замкнутого процесса защиты информации, которая опирается на современные достижения индустрии ИТ и хорошо коррелирована с ними.

Российские регулирующие органы, к сожалению, не имели возможности такого же плотного взаимодействия с обладающими технологическим суверенитетом национальными представителями индустрии ИТ, нередко по причине отсутствия таковых. А проблемы в понимании сути ИТ и внедрения в них компонентов ИБ как неотъемлемых функций, судя по всему, существовали еще со времен попыток создания национальных документов (ФАПСИ, Гостехкомиссия и пр.) на основе документов из американской «радужной серии». В результате сегодня в России не обеспечена адекватная методическая поддержка процесса защиты информации, а взаимодействие с национальными представителями индустрии ИТ, не обладающими в полной мере технологическим суверенитетом, представляется не слишком результативным.

Ситуацию несколько смягчают постепенно переведенные и принятые аналоги международных стандартов в системе ГОСТ Р ИСО/МЭК. Но остается проблема применения действующих документов российских регулирующих органов (принятых большей частью еще в 1992 г.). Критики не выдерживает даже «новый подход» ФСТЭК России с приказами № 17, № 21 и № 31, представляющими собой вольный (и весьма избирательный) перевод APPENDIX D из документа NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. И вопрос даже не в том, что вместо APPENDIX D следовало, как минимум, приложить APPENDIX F (там содержится более структурированная и точнее изложенная информация по исследуемому вопросу), как максимум, принять SP 800-53 и перевести в разряд ГОСТ Р целиком. Соответственно возникает вопрос переосмысления всей национальной нормативной базы, поскольку современный уровень ИТ и вызовы ИБ поставили вопрос ребром: либо переходить к национальной нормативной базе, полностью основанной на современных международных стандартах (например, серии ISO/IEC 15408, ISO/IEC 27001, ISO 22301, ISO/IEC 20000, ISO/IEC 31000 и пр.), либо продолжать применять выборочно нормативную базу российских регулирующих органов, частично «улучшенную» международными методиками (ISO, NIST, CoBIT, ITIL, COSO и пр.).

> Под технологическим суверенитетом подразумевается такое устойчивое и наблюдаемое состояние, когда реализация ИТ возможна исключительно на основе компонентов, которые производят организации в пределах юрисдикции России и имеют на них исключительные права.

Технологические условия

Второе условие достижения технологического суверенитета в области ИТ: обладание полным спектром технологий – от проектирования микроэлектронных компонентов до выпуска готовых изделий на их основе, прошедших оценку доверия в уставленном порядке. Некоторые успехи в области космической и военной электроники, обеспечении органов государственной власти (ОГВ) планшетами на базе «новой гарвардской архитектуры» представляются достаточными для парирования современных вызовов в области ИБ только символически. Целесообразно привести пример пирамиды, стабильное положение которой основано на максимально широком спектре доступных доверенных компонентов ИБ и оборудования общего назначения, прошедших необходимые проверки в России.

Третьим условием достижения технологического суверенитета в области ИТ является обладание полным спектром технологий безопасного замкнутого цикла разработки ПО – от проектирования до производства любых необходимых компонентов. И здесь есть где потрудиться, так как встроенного ПО у нас практически нет по понятным причинам. А ведь этот класс ПО интегрирован в оборудование значительно глубже, чем видимый всем уровень BIOS (и часть встроенного ПО запускается раньше, чем BIOS). Наконец, надо набраться мужества и честно признать, что технологический суверенитет недостижим в полной мере только на базе свободного ПО с открытым кодом, приведенным в соответствие с требованиями ОГВ.

Учет и контроль

Четвертое условие достижения технологического суверенитета в области ИТ – обладание собственным доверенным и оцененным инструментарием. Тема инструментария специально вынесена отдельно. Невозможно обладать технологическим суверенитетом и при этом разрабатывать ПО для ОГВ на зарубежных компиляторах, равно как разрабатывать микроэлектронику для целей оборонной промышленности в зарубежных (недоверенных) средах разработки.

Пятое условие достижения технологического суверенитета в области ИТ: доверие к системе, типовым способом формирования которого является сегодня «доверие через оценку». Но, для того чтобы получать адекватные результаты, нужно понимать, в какой момент времени производить оценку. Мировая практика предусматривает оценку по мере необходимости. Переложение данного подхода на наши условия определяет необходимость отказаться от лицензирования деятельности в области защиты открытой информации (оставив только безусловное обеспечение безопасности ОГВ, что следует и из недавних разъяснений представителей ФСБ по применению «пакета Яровой») и выполнять оценку соответствия по мере необходимости в открытых и прозрачных системах оценки соответствия, поддерживаемых сообществом участников рынка ИТ. Целесообразно оценивать безопасность в ИТ в рамках ISO/IEC 15408, являющегося на сегодняшний день в мире стандартом де-факто и не имеющего альтернатив. В части управления безопасностью следует производить оценку процессов управления в рамках ISO/IEC 27001, который в своем сегменте также является мировым стандартом де-факто и не имеет альтернатив.

Целесообразно оценивать безопасность в ИТ в рамках ISO/IEC 15408, являющегося на сегодняшний день в мире стандартом де-факто и не имеющего альтернатив.

Шестое условие достижения технологического суверенитета в области ИТ: тесная кооперация сообщества производителей компонентов ИТ между собой. Иначе технологический прорыв в масштабе России невозможен, поскольку пока еще слишком малы объемы и компетенции каждого производителя в отдельности, рынок сбыта и отраслевая экспертиза. Ранее подобная проблема называлась «комплексированием» – специалисты СССР уделяли ей достойное внимание и отводили важное место в процессе создания надежных решений ИТ из различных компонентов.

Заключение

Заявленные в данной публикации цели могут показаться амбициозными и загоризонтными. Но если не ставить таких целей на уровне отраслей в России, не планировать четкие программы (хоты бы для ОГВ), а просто плыть по течению на волнах свободного ПО с открытым кодом, то и через много лет мы опять окажемся, к сожалению, на том же самом месте – в самом начале тяжелого и длинного пути к национальному технологическому суверенитету. ■