Импортозамещение ИТ- и ИБ-решений в ОПК

Андрей ПРОЗОРОВ,
руководитель экспертного направления, компания Solar Security

Несколько лет назад я принимал участие в разработке проекта документа «Концепция создания, развития и использования информационных технологий в оборонно-промышленном комплексе Российской Федерации на период до 2020 года». Документ содержал описание состояния, проблем и тенденций использования информационных технологий в ОПК, а также направления развития, цели и первостепенные задачи. К сожалению, итоговая версия документа не была принята и утверждена, но важные идеи, заявленные в нем, не потеряли актуальности.

Доктрина импортозамещения

Речь идет в первую очередь о необходимости обеспечивать информационную безопасность ИТ-инфраструктуры объектов ОПК и потребности в разработке и реализации программы импортозамещения. Эти задачи отражены в актуализированных верхнеуровневых документах, определяющих развитие отраслей ИТ и информационной безопасности в России: Доктрине информационной безопасности Российской Федерации (утверждена указом Президента Российской Федерации от 5 декабря 2016 г. № 646) (далее – Доктрина) и указе Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» (далее – Стратегия).

В частности, в Доктрине заявлена проблема «высокого уровня зависимости отечественной промышленности от зарубежных информационных технологий». Документ предлагает ориентироваться на «совершенствование методов и способов производства и безопасного применения продукции, оказания услуг на основе информационных технологий с использованием отечественных разработок, удовлетворяющих требованиям информационной безопасности». Это должно стать одним из основных направлений обеспечения информационной безопасности в области государственной и общественной безопасности.

В Стратегии развития информационного общества в качестве национального приоритета названо обеспечение безопасности граждан и государства. Один из методов достижения поставленной цели – создание и применение российских информационных и коммуникационных технологий. А для устойчивого функционирования информационной инфраструктуры РФ определена необходимость в «замене импортного оборудования, программного обеспечения и электронной компонентной базы российскими аналогами, обеспечение технологической и производственной независимости и информационной безопасности». Отмечена также необходимость в том, чтобы «обеспечить использование российских информационных и коммуникационных технологий в органах государственной власти РФ, компаниях с государственным участием, органах местного самоуправления».

Эти верхнеуровневые положения говорят о том, что компаниям оборонно-промышленного комплекса РФ уже сейчас стоит задуматься о разработке собственных программ импортозамещения.

Импортозамещение реестром

В России приняты Федеральный закон от 29 июня 2015 г. № 188-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статью 14 Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» и постановление Правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения,

происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (вместе с «Правилами формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных», «Порядком подготовки обоснования невозможности соблюдения запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»). Помимо прочего они устанавливают правила формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных (https://reestr.minsvyaz.ru, далее – Реестр). Именно на него и стоит ориентироваться организациям при выборе программного обеспечения. 16 сентября 2016 г. Председатель Правительства РФ Дмитрий Медведев подписал постановление о приоритете товаров российского происхождения.

Реестр функционирует с 1 января 2016 г., и на начало мая 2017 г. в нем уже зарегистрировано более 3500 наименований программного обеспечения по следующим классам:

- BIOS и иное встроенное программное обеспечение (33 зарегистрированных решения);
- встроенное программное обеспечение телекоммуникационного оборудования (14 зарегистрированных решений);
- геоинформационные и навигационные системы (86 зарегистрированных решений);
- операционные системы (30 зарегистрированных решений);
- утилиты и драйверы (63 зарегистрированных решения);
- средства обеспечения облачных и распределенных вычислений, средства виртуализации и системы хранения данных (47 зарегистрированных решений);
- серверное и связующее программное обеспечение (215 зарегистрированных решений);
- системы управления базами данных (31 зарегистрированное решение);
- системы мониторинга и управления (351 зарегистрированное решение);
- средства обеспечения информационной безопасности (323 зарегистрированных решения);
- средства подготовки исполнимого кода (19 зарегистрированных решений);
- средства версионного контроля исходного кода (10 зарегистрированных решений);
- библиотеки подпрограмм (SDK) (30 зарегистрированных решений);
- среды разработки, тестирования и отладки (62 зарегистрированных решения);
- системы анализа исходного кода на закладки и уязвимости (13 зарегистрированных решений);
- прикладное программное обеспечение общего назначения (489 зарегистрированных решений);
- офисные приложения (163 зарегистрированных решения);
- поисковые системы (70 зарегистрированных решений);
- лингвистическое программное обеспечение (52 зарегистрированных решения);
- системы управления проектами, исследованиями, разработкой, проектированием и внедрением (305 зарегистрированных решений);
- системы управления процессами организации (1172 зарегистрированных решения);
- системы сбора, хранения, обработки, анализа, моделирования и визуализации массивов данных (539 зарегистрированных решений);
- информационные системы для решения специфических отраслевых задач (2236 зарегистрированных решений).

Несмотря на то что Реестр постоянно пополняется и развивается, работать с ним не всегда удобно. Так, например, по классу «Средства обеспечения информационной безопасности» зарегистрировано 423 продукта, но как найти среди них отдельные типы программного обеспечения – средства антивирусной защиты, средства анализа защищенности, межсетевые экраны и др.? Для ориентира можно использовать таблицу.

Как видим, организациям, ориентирующимся на использование российских программных продуктов для обеспечения информационной безопасности, уже есть из чего выбирать. Аналогично и по другим классам программного обеспечения в Реестре.

Напомним, что существует ряд директив для государственных организаций в отношении преференций отечественному ПО, которые среди прочего содержат:

Таблица. Разбиение средств защиты по классам

Тип средства обеспечения ИБ	Примеры ПО в Реестре
Средства антивирусной защиты	Dr.Web, Kaspersky, NANO «Антивирус Pro», Positive Technologies MultiScanner
DLP-системы	Solar Dozor, InfoWatch Traffic Monitor, LanAgent, Kaspersky DLP, Zecurion DLP, КИБ «Серчинформ», «Гарда Предприятие»
SIEM-системы	MaxPatrol Security Information and Event Management, KOMRAD Enterprise SIEM («Эшелон»), Security Capsule SIEM
Средства анализа кода приложений	Solar inCode, InfoWatch Appercut, Positive Technologies Application Inspector, АК-ВС 2, IRIDA Sources
IDM-системы	Solar inRights, IDM-система «Куб», Avanpost IDM
Средства защиты от несанкционированного доступа / Средства доверенной загрузки	Secret Net, Dallas Lock, ПАК «Соболь», «Блокхост-МДЗ», «МДЗ-Эшелон»,
Средства анализа защищенности (сканеры)	«Сканер-ВС», MaxPatrol, xSpider, RedCheck
Межсетевые экраны и средства защиты каналов связи (VPN)	«Рубикон», TrustAccess, МЭ ИКС, ИВК «Кольчуга», «Интернет Контроль Сервер», Positive Technologies Application Firewall, «Континент», ViPNet Coordinator, Dozor Web-proxy

Мнение специалиста

Дмитрий БИРЮКОВ,
директор направления информационной безопасности, группа «Астерос»

Автор абсолютно справедливо поднимает вопрос о необходимости более жесткого регламентирования использования отечественных разработок программных и технических средств защиты предприятиями ОПК как в АСУ ТП, так и в той продукции, которую они выпускают. В качестве дополнения хотелось бы отметить, что современные программные средства вычислительной техники, в том числе средства защиты информации, носят многофункциональный характер. Поэтому для повышения удобства пользования Единым реестром российских программ для ЭВМ и баз данных было бы не лишним доработать заложенные в нем поисковые механизмы. Кроме того, для обеспечения информационной безопасности ИТ-инфраструктуры объектов ОПК следует обратить внимание на уже назревший вопрос о государственной поддержке вузов, ведущих подготовку специалистов в области программирования перспективных процессоров, которые будут использоваться в изделиях вооружения и военной техники.

- обязательство в десятидневный срок со дня получения указанных директив инициировать проведение заседаний советов директоров (наблюдательных советов) акционерного общества с включением в повестку дня вопроса «О закупках отечественного конкурентоспособного ПО, необходимого для деятельности акционерного общества»;
- текст о необходимости внесения изменений в Положение о закупочных процедурах, проводимых для нужд акционерного общества:
  - закупка «только такого ПО, сведения о котором включены в единый реестр российских программ для электронных вычислительных машин и баз данных…»;
  - за исключением случаев, когда «в реестре отсутствуют сведения о ПО, соответствующем тому же классу», или «ПО неконкурентоспособно (по своим функциональным, техническим и (или) эксплуатационным характеристикам не соответствует установленным заказчиком требованиям к планируемому к закупке ПО)»;
  - если ПО попадает под указанные исключения, то необходимо не позднее чем в течение семи дней с даты размещения информации о закупке опубликовать «обоснование невозможности соблюдения ограничения на допуск ПО, происходящего из иностранных государств».

Таким образом, если это пока не серьезные ограничения на закупку, то, во всяком случае, уже «строгая рекомендация» приобретать решения из реестра отечественного ПО.

Реестр промышленности

Однако в отечественном ОПК до сих пор используются в основном импортные решения. По данным TAdviser, зарубежные производители ПО ежегодно получают от российских потребителей около 285 млрд руб. лицензионных отчислений (45% общего объема российского ПО), 30% этих отчислений приходится на госсектор. Например, по статистике Минкомсвязи, доля импорта клиентских и мобильных операционных систем в целом в России составляет 95%, серверных – 75%. В отечественном ОПК 70% электронных компонентов – импортного производства. Между тем санкции, наложенные на оборонно-промышленные предприятия иностранными государствами, наглядно продемонстрировали все риски столь широкого и повсеместного внедрения зарубежных решений.

Виталий Сазонов, руководитель управления информационных технологий «Объединенной приборостроительной корпорации» ГК «Ростех», также отмечает, что доля иностранных решений в области военной техники, телекоммуникационного оборудования и ПО, применяемых сегодня в России, критически велика и достигает в большинстве сегментов 90% и выше. Причем не секрет, что зачастую зарубежная техника и ПО таят в себе незадекларированные возможности в части негласного доступа к информации и передачи данных. В связи с этим представляется разумным выполнение оборонно-промышленными предприятиями следующих процедур:

- инвентаризация ПО (общий перечень, срок окончания лицензий, стоимость продления, наличие сертификатов ФСТЭК, количество пользователей);
- определение своего подхода к импортозамещению: заменить все, заменить критичные узлы или заменить только базовые продукты, установить средства контроля российского производства;
- выбор классов ПО для импортозамещения, изучение ПО соответствующего класса;
- разработка и реализация стратегии и плана импортозамещения.

Заключение

Остается только выразить надежду, что программа импортозамещения ИТ- и ИБ-решений получит максимально широкое распространение в ОПК и дальнейшая информатизация оборонно-промышленных предприятий будет осуществляться на базе отечественных решений. Особенно это относится к средствам защиты информационных систем, выбор которых в приведенном выше реестре достаточно широк. ■