

Региональная и муниципальная информатизация

ЭКСПЕРТНЫЙ ЦЕНТР
ЭЛЕКТРОННОГО
ГОСУДАРСТВА

Сентябрь 2015 / № 3



Импортозамещение программного обеспечения в органах власти

Оглавление



Павел Хилов

Импортозамещение программного обеспечения: из точки А в точку Б 4



Илья Массух

Импортозамещение программного обеспечения: хорошо забытые старые задачи 10



Евгения Василенко

Об ограничениях на госзакупки иностранных программных продуктов, вводимых с января 2016 года 14

Система «Адванта» для управления проектами органов государственных организаций 19



Наталья Касперская

Об импортозамещении в области IT 26



Андрей Анненков

Импортозамещение софта: закон, постановление правительства, приказ по министерству 31



Леонид Филатов

Хищническая добыча данных, или Почему и как государство должно заботиться об информационной гигиене 36



Александр Архангельский

Как избавиться от зарубежных облачных сервисов и обрести больше возможностей 43



Дмитрий Гоков

Импортозамещение ПО – шаг на месте к IT-суверенитету 46



_Тос430611672

Дмитрий Курашев

О возможностях импортозамещения: взгляд участника российского рынка ПО.....50



Анатолий Дюбанов, Алексей Горобцов

Импортозамещение – это, в первую очередь, независимость 53



Константин Бажин

Единая защищенная мобильная платформа 57



Герман Клименко

Почему импортозамещение ПО следует начать с муниципалитетов 62



Михаил Альперович

Защита мобильных подключений к СЭД региональных органов власти 65



Сергей Ожегов

Информационная безопасность российских компаний: состояние дел в 2015 году 70

О журнале79

От редактора

Импортозамещение программного обеспечения: из точки А в точку Б



Павел Хилов,
главный редактор,
руководитель
Экспертного центра
электронного
государства

Тема эта важна во многих смыслах. К ней имеют непосредственное отношение технологическая независимость и конкурентоспособность страны, её безопасность, экономическое благополучие, зависящее от развития софтверной индустрии. Поскольку основная сфера интересов Экспертного центра электронного государства – это государственная информатизация, то основной темой журнала стала тема импортозамещения ПО в органах власти и местного самоуправления. Пока, к сожалению, оказывается, что именно в этой сфере ситуация далека от оптимистичной.

Точка А

Какой софт работает в органах власти РФ сегодня? Опрос региональных IT-министров, проведенный Экспертным центром электронного государства с целью выяснить, какое ПО используется в органах власти и муниципалитетах, выявило удручающую, как и можно было ожидать, картину.

На 95% рабочих мест в качестве операционной системы стоит Microsoft Windows, и Windows используется как серверная операционная система на 75% серверов. При этом 90% сотрудников региональных органов власти используют MS Office.

В 82% органов власти субъектов РФ в качестве почтовых серверов используют Microsoft Exchange, более 60% серверов СУБД - производства Microsoft или Oracle (остальные в основном – свободно распространяемые MySQL и PostgreSQL). Если же учесть, что разработку и

поддержку MySQL осуществляет также корпорация Oracle, то общая доля СУБД этих компаний составляет почти 80%.

Единственная категория общесистемного ПО, в котором преобладают российские продукты – это антивирусные программы (производства «Лаборатории Касперского» и DrWeb), которые вместе занимают 65% государственного сегмента российского рынка (но при этом словачкой ESET принадлежат 12%)

В категории web-серверов ситуация заметно отличается – почти 60% принадлежит Apache и NGINX. Впрочем, и здесь Microsoft IIS занимает 34%

Получается, что российское госуправление практически полностью зависит от зарубежных программных продуктов, причем по всем их классам, начиная от операционных систем и заканчивая прикладным ПО общего назначения, таким, как офисный софт. То, что «отраслевые» системы, используемые органами власти для управления в различных сферах госуправления (образование, здравоохранение, транспорт, общественная безопасность и т.п.), разработаны, как правило, российскими компаниями, несколько не меняет картину – все они используют импортные СУБД и операционные системы, а значит, ровно так же зависят от них.

Много раз уже говорилось, и будет сказано ещё раз в материалах этого номера журнала, что в негативных сценариях развития событий такая ситуация грозит тяжёлыми последствиями – от прекращения работоспособности отдельных сервисов и приложений до полной остановки госуправления.

Если даже год назад такие сценарии казались маловероятными, то сейчас они видятся вполне реалистичными, и это заставляет государственные органы обратиться к теме импортозамещения в сфере программного обеспечения.

Учитывая масштаб возможных угроз, было бы логично, если эти процессы инициировались и координировались с федерального уровня. Но на нём активность ограничивается только одним из аспектов импортозамещения, а именно поддержкой отечественной отрасли ПО.

Пока все меры сводятся к внесению поправок в закон «Об информации...» №149-ФЗ, посвященных определению понятия «российское программное обеспечение», и разработке проекта постановления правительства РФ, утверждающего правила ведения реестра отечественного ПО, устанавливающего ограничения на доступ иностранного ПО к госзакупкам, которое, как предполагается, вступит в силу с 1 января

2016 года (подробнее см. статью Евгении Василенко). Этого, по нашему мнению, недостаточно, чтобы запустить процесс импортозамещения ПО в масштабе страны.

Есть еще приказ Минкомсвязи России №61, который утверждает План импортозамещения программного обеспечения (подробнее об этом см. статью Андрея Анненкова), но не имеет никакой силы для федеральных органов власти и для регионов, поэтому его нельзя рассматривать в качестве отправной точки для формирования реалистичных планов.

Даже в самом оптимистичном пункте, в соответствии с которым планируется сократить долю импорта в группе «Интернет-сервисы, применяемые в корпоративной среде (электронная почта, сервис файлового обмена, интернет-браузер, картографический сервис, сервис обмена мгновенными сообщениями и т.д.)» к 2020 году до 25%, а к 2025 – до 10%. Хотя по каждой из подгрупп существуют либо СПО, либо чисто российские разработки.

На одну только федеральную власть надежды мало. Без активного участия регионов ситуацию будет не сдвинуть. А сдвинуть надо, и сделать это следует задолго до того, как угрозы, сегодня кажущиеся потенциальными, начнут реализовываться.

Путь из А в Б – ориентир

Примеры самостоятельного решения проблемы технологической зависимости уже имеются. Банковская сфера уже столкнулась с проблемами неблагоприятных внешних воздействий на IT-системы и, в отличие от госорганов, вынуждена была всерьез задуматься о практических шагах, чтобы преодолеть зависимость от зарубежного софта.

В «санкционные списки» США, напомним, попали четыре российских банка: «Россия», СМП Банк, Инвесткапиталбанк, Собинбанк. Международные платёжные системы MasterCard и Visa заблокировали карты этих банков. Под санкции ЕС попали пять банков: Газпромбанк, Сбербанк, Россельхозбанк, ВЭБ и ВТБ. В список тех, кому отказано в поддержке уже приобретённых сервисов и продуктов, а также в покупке новых, попали граждане России в Крыму.

Примеры последствий неблагоприятных внешних воздействий на российские IT-системы:

- блокировка расчетов через международные платёжные системы (более 320 тысяч человек не могли расплачиваться своими картами и использовать их в «чужих» банкоматах);
- отзыв SSL-сертификатов (нарушение работы клиент-банка и других систем);
- отказ от поставок и от обязательств по договорам сопровождения программного обеспечения и принуждение российских партнеров не заключать договора поддержки с организациями из санкционного списка;
- отказ от поставок компьютерного и сетевого оборудования и комплектующих к нему в организации из санкционного списка
- отказ от гарантийного обслуживания вышедшего из строя оборудования;
- ограничение на использование услуг хостинга и каналов передачи данных;
- отключение организаций от сервисов обновления версий ПО, в том числе в части получения исправлений уязвимостей безопасности.

По оценке аналитиков группы компаний «Диасофт», в случае введения со стороны США и ЕС технологических санкций против российских банков, максимальное время наработки на отказ (т.е. поддержания работоспособности информационных систем) составит не более 24 месяцев, реалистичное же (с вероятностью 50%) составит всего 4 месяца.

Однако, как показывает опыт первых пяти банков, уже попавших под технологические санкции, возможен и немедленный сбой в результате «прямых недружественных действий» (например, отзыв корневого SSL-сертификата).

Банкиры раньше других поняли (в отличие от наших государственных органов, IT-санкции против которых – вопрос времени), что в случае сбоя хотя бы одного критического для зарабатывания денег элемента последствия для бизнеса будут катастрофическими. Поскольку деятельность банков находится в абсолютной зависимости от IT, либо российские банки обеспечат контроль над своими IT-системами, либо разорятся. Отрасль предпочла первый вариант.

Государство должно первым прийти в точку Б

Под воздействием оказались отдельные банки и отдельные, хотя и важные, IT-сервисы. Чем грозит немедленный отказ Единого портала госуслуг и региональных порталов и прикладных систем, т.е. тех IT-

ресурсов, которые нечем заменить, читателю нашего журнала объяснить не надо – это была бы катастрофа.

Использование прикладных государственных IT-систем, как правило, регламентировано техническими службами органов власти и, хочется верить, службами безопасности, то есть софт, который используется в рабочих целях сотрудниками органов власти, находится внутри периметра информационной безопасности, хотя зачастую процессы обеспечения информационной безопасности носят формальный характер.

Но то, что происходит за пределами периметра, вызывает, мягко говоря, сильную тревогу. Почти 40% сотрудников госучреждений используют для рабочего общения бесплатную почту («Яндекс» – 13%, Mail.ru – 12%, Gmail и Rambler – по 6%).

Такая же доля региональных госслужащих используют для служебных коммуникаций Microsoft Skype, 21% - QIP, 14% - Telegram, по 9% - WhatsApp и Viber.

Примерно столько же - 41% - используют различные бесплатные сервисы для обмена и хранения служебными документами – DropBox, GoogleDocs, «Яндекс.Диск», «Файлы@Mail.ru» и даже группы в социальных сетях.

Владельцы таких сервисов не несут никакой ответственности за сохранность и конфиденциальность информации, которая хранится или

IT-руководители регионов согласны с необходимостью реализации превентивных мер по импортозамещению ПО

передается при их использовании, более того, пользователи никак не защищены от передачи этой информации третьим сторонам.

IT-руководители регионов согласны с необходимостью реализации превентивных мер по импортозамещению ПО, при этом самой важной целью опрошенные назвали обеспечение информационной безопасности - 87% из них считают, что это «важно» или «очень важно», причём на «очень важно» приходится 76%. На втором месте - развитие отечественной IT-отрасли (86%), на третьем - минимизация рисков введения санкций – 79%.

Но реальных мер на региональном уровне предпринимается исчезающе мало.

Можно пересчитать по пальцам регионы, которые на деле хотя бы изучают варианты перехода от проприетарного зарубежного ПО либо на СПО, либо на полностью отечественные продукты. Большинство же, ссылаясь на различные причины, начиная от нехватки бюджетов и отсутствия федеральной нормативной базы и заканчивая ссылками на наличие сертификатов и аттестатов, которые гарантируют безопасность существующего парка ПО, или отсутствием отечественных аналогов, ограничиваются формальным подходом к планированию и реализации мер по переходу на использование российского ПО.

Именно поэтому мы решили сделать специальный выпуск журнала «Региональная и муниципальная информатизация», посвященный этой теме.

В нем руководители региональных органов власти, представители российских компаний-разработчиков программного обеспечения, экспертного сообщества делятся своим видением пути движения государственных IT-систем из нынешней точки А к Б, в которой подлинный контроль над ними окажется в руках самих органов власти. ■

Импортозамещение ПО

Импортозамещение программного обеспечения: хорошо забытые старые задачи



Илья Массух,
президент Фонда
информационной
демократии

С недавних пор прочно занимавшие первое место в рейтинге государственных трендов «инновации» потеснило более консервативное «импортозамещение». В авангарде импортозамещения – информационные технологии, без которых сегодня не обходится ни один сектор экономики. Именно ИТ президент страны назвал в первую очередь в связи с импортозамещением на Петербургском международном экономическом форуме 2014 года.

Прошедший 2014 год для российской ИТ-отрасли во многом стал поворотным – в условиях технологических санкций на фоне девальвации рубля государство стало не просто регулятором, оно существенно упрочило свою роль крупнейшего игрока, формирующего огромную долю рынка.

На вопрос о целях импортозамещения в ИТ практически любой чиновник бодро рапортует о необходимости противостояния внешним угрозам, стимулировании отечественных разработчиков, цифровом суверенитете и патриотизме. Как грибы после дождя появляются отчеты об отечественных процессорах, серверах, СУБД, ЦОДах и «облаках».

Очевидно, что такое разнообразие отечественных решений не могло появиться в одночасье просто потому, что государством был объявлен курс на импортозамещение. Минкомсвязь только начинает реализацию мероприятий по поддержке отечественного ИТ-продукта. Большинство из того, что сейчас объявляется российской альтернативой иностранному, – результат разработок, которым, наконец, дали возможность проявить себя. Но основа этому движению была заложена задолго до нашествивших событий – таких, как отключения иностранных

IT-сервисов в Крыму и отказ иностранных платёжных систем обслуживать отечественные банки.

Российская специфика такова, что по многим направлениям именно государство выступает «застрельщиком», и импортозамещение не является исключением. Понимание необходимости снижения зависимости от иностранных IT было закреплено еще в государственной программе «Информационное общество (2011-2020 годы)», утвержденной в 2010 году.

В частности, в этом документе была предусмотрена подпрограмма «Безопасность в Информационном обществе», которой предполагалось:

- создание и поддержка отечественных защищенных технологий хранения и обработки больших массивов неструктурированной информации;
- развитие отечественной сборки операционной системы на свободном программном обеспечении;
- создание отечественной системы управления базами данных на основе открытых разработок;
- создание российской среды разработки программного обеспечения;
- разработка набора архитектурных стандартов и типовых компонентов для совместимости программ между собой;
- создание базового пакета прикладного программного обеспечения, включая драйверы и средства обеспечения информационной безопасности;
- создание национального фонда алгоритмов и программ;
- формирование территориально распределенной инфраструктуры технической и методической поддержки свободного программного обеспечения;
- разработка отечественного программного обеспечения для технологий проектирования и имитационного моделирования на супер-ЭВМ;
- создание системы подготовки высококвалифицированных кадров в области суперкомпьютерных технологий и специализированного программного обеспечения.

Идея этой части госпрограммы предусматривала «мягкое» движение по увеличению доли отечественных разработок и разработок на основе СПО. Было понимание, что нельзя в короткий срок изменить сложившийся уклад, но необходимо создать прецедент, который в дальнейшем стал бы катализатором процесса.

В том же 2010 году распоряжением Правительства № 2299-р был утвержден план перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование СПО к 2014-2015 гг. Планом предусматривалось создание единого репозитория программного обеспечения, формирование пакета базового СПО, используемого для решения типовых задач деятельности ФОИВ к 2012 году. А в 2014 году планировалось начать внедрение типовых пакетов базового ПО в ФОИВ и подведомственных им учреждениях.

В 2011 году на заседании коллегии Минкомсвязи Игорь Щёголев, занимавший тогда пост министра связи и массовых коммуникаций, объявил о налоговых льготах для аккредитованных IT-компаний.

Эти мероприятия, будь они осуществлены, позволили бы к 2018 году уже получить, во-первых, обкатанные типовые решения на базе российских продуктов, доработанные и соответствующие всем необходимым стандартам, а во-вторых – армию активных пользователей-евангелистов в лице сотрудников государственных учреждений. Для полноты картины можно добавить сюда и планы по внедрению СПО в образовательных учреждениях.

Однако в 2012 году со сменой команды Минкомсвязи курс изменился. Новое руководство посчитало, что целесообразно закупать иностранные решения. Значительная доля российских разработчиков вместо развития собственных продуктов занялась интеграцией зарубежных. Поддержка отечественных разработок по критически важным направлениям осуществлялась на минимальном уровне.

Сегодня в силу ряда причин мы наблюдаем ренессанс рынка отечественной разработки, более того – государством официально задан курс на импортозамещение IT-решений. Выяснилось, что, у нас есть достойные альтернативы распространенным решениям, есть разработка компонентной базы пусть и с зарубежным производством. Среди прочих позитивных тенденций – попытки поддержать отечественные разработки созданием преференций при госзакупках. Не может не радовать начало реализации плана подготовки высококвалифицированных кадров для отрасли.

Приведет ли это к победе отечественных IT на свободном рынке? Вряд ли. Необходимо учитывать ряд важных факторов: разработка зарубежных решений-лидеров велась непрерывно в течение десятилетий, а финансовые резервы транснациональных корпораций позволяют последним годами продавать их практически за бесценок ради сохранения доли рынка.

Таким образом, эффект от действий, которые сейчас активно ведутся на федеральном уровне, мы сможем увидеть лишь в перспективе 10-15 лет. В то же время обстановка требует видимых изменений уже в течение следующих двух-трёх лет. Каким образом этого добиться?

Во-первых, нам необходимо формировать спрос на отечественное. У российского разработчика сегодня есть все для успешного старта – поддержка государства, сложная, но благоприятная экономическая об-

Ключевой элемент – это поддержка со стороны лиц, принимающих решения – IT-директоров и директоров по закупкам. Пока в их головах не «щелкнет выключатель», переломить ситуацию в пользу отечественных продуктов будет сложно

становка. Но ключевой элемент – это поддержка со стороны лиц, принимающих решения – IT-директоров и директоров по закупкам. Пока в их головах не «щелкнет выключатель», переломить ситуацию в пользу отечественных продуктов будет сложно. Подход к выбору решений должен быть инженерным и отталкиваться от конкретных задач, а не шаблонным – просто потому что этим все пользуются.

Во-вторых, нужно формировать аудиторию пользователей. Активных пользователей, которые дадут разработчикам реакцию, необходимую для совершенствования продукта, доведения его до уровня конкурентоспособности и выхода на экспортный уровень. Такие примеры в отечественной IT-отрасли есть.

В-третьих, следует создавать экосистему отечественных продуктов, дополняющих друг друга. Речь идет именно о «базовых» продуктах, с которыми каждый день сталкивается любой пользователь ПК, и владения которыми чаще всего требуют от соискателя при приеме на работу – офисный пакет, браузер и т.д.

В-четвертых, завершить переход на СПО, как в образовании, так и в органах власти – это даст необходимый толчок к развитию «жизненно важных» составляющих: стандартов и сред разработки и проектирования, типовых компонентов и т.п.

Наконец, нужно просто начать с себя. Несмотря на многочисленные примеры утечек, многие российские чиновники продолжают пользоваться импортными или бесплатными отечественными продуктами и сервисами для ведения дел и пересылки рабочих документов. Может ли быть эффективным импортозамещение IT при таком подходе? ■

Нормативка

Об ограничениях на госзакупки иностранных программных продуктов, вводимых с января 2016 года



Евгения Василенко,
исполнительный ди-
ректор Ассоциации
разработчиков про-
граммных продуктов
«Отечественный
софт»

Президент России Владимир Путин 1 июля 2015 года подписал закон о предоставлении преференций российским разработчикам программного обеспечения (ПО) при госзакупках.

Предпосылки введения ограничений на госзакупки импортного софта

По данным Минкомсвязи РФ, сегодня 75% используемого в России программного обеспечения является иностранным. Международные компании на протяжении многих лет вели системную работу, чтобы не дать локальным конкурентам вырасти, отвоевать свою долю рынка. В отсутствии государственного регулирования закупок программного обеспечения сложилась ситуация тотального доминирования иностранных продуктов в большинстве сегментов рынка ПО, что угрожает технологической и информационной безопасности России. Помимо слежки за пользователями, использование иностранного программного обеспечения ведет к риску внешнего отключения большинства информационных систем. Это уже происходит – в качестве примеров можно привести ситуацию с отключением платежных систем и отказом обслуживания пользователей в Крыму.

Вопрос технологической независимости России требует системного решения на государственном уровне. Один из первых очевидных шагов, который можно реализовать уже сейчас – прекратить закупать иностранные продукты там, где возможно применение отечественных решений. На текущий момент во многих сегментах ПО есть российские продукты, которые не пользуются должным спросом у российских

заказчиков. И дело зачастую не в качестве продуктов, не в их функциональных возможностях. Заказчики продолжают по привычке покупать иностранное, предпочитая не тратить время на изучение российских альтернатив.

Безусловно, невозможно реализовать единовременный переход на отечественные решения. Процесс перехода должен быть системным и

**Заказчики продолжают по привычке покупать
иностранное, предпочитая не тратить время
на изучение российских альтернатив**

поэтапным. Если реализовать задачи государственного заказчика на данный момент можно только с помощью иностранных продуктов, заказчик в праве их использовать.

Чтобы изменить вектор госзакупок в сторону отечественного программного обеспечения, разработаны меры поддержки отечественных решений.

Реестр отечественного ПО как инструмент исполнения закона

С 1 января 2016 года Минкомсвязь России будет вести реестр отечественного программного обеспечения. В него войдут продукты, которые соответствуют критериям, определённым постановлением правительства РФ. Экспертизу соответствия решений критериям будет проводить экспертный совет, сформированный при Минкомсвязи. В состав совета войдут представители ведомств, институтов развития, образовательных и научных учреждений, российских разработчиков ПО. Утверждать включение программных продуктов в реестр будет Минкомсвязь.

Правообладатели программных продуктов, попавших в реестр, будут обязаны уведомить министерство связи об изменениях, которые ведут к несоответствию их продуктов критериям отнесения ПО к отечественному.

Наличие программного обеспечения в реестре будет свидетельством его российского происхождения для заказчиков.

В реестр российского программного обеспечения включаются сведения о программах для электронных вычислительных машин и базах данных, которые соответствуют следующим требованиям:

1) исключительное право на программу для электронных вычислительных машин или базу данных на территории всего мира и на весь срок действия исключительного права принадлежит одному либо нескольким из следующих лиц (правообладателей):

а) Российской Федерации, субъекту Российской Федерации, муниципальному образованию;

б) российской некоммерческой организации, высший орган управления которой формируется прямо и (или) косвенно Российской Федерацией, субъектами Российской Федерации, муниципальными образованиями и (или) гражданами Российской Федерации...;

в) российской коммерческой организации, в которой суммарная доля прямого и (или) косвенного участия Российской Федерации, субъектов Российской Федерации, муниципальных образований, российских некоммерческих организаций, указанных в подпункте "б" настоящего пункта, граждан Российской Федерации составляет более пятидесяти процентов;

г) гражданину Российской Федерации;

2) программа для электронных вычислительных машин или база данных правомерно введена в гражданский оборот на территории Российской Федерации, экземпляры программы... либо права использования программы... свободно реализуются на всей территории Российской Федерации;

3) общая сумма выплат по лицензионным и иным договорам, предусматривающим предоставление прав... в пользу иностранных юридических лиц и (или) физических лиц, контролируемых ими российских коммерческих организаций и (или) российских некоммерческих организаций, агентов, представителей иностранных лиц и контролируемых ими российских коммерческих организаций и (или) российских некоммерческих организаций составляет менее тридцати процентов от выручки правообладателя (правообладателей) программы для электронных вычислительных машин... за календарный год;

4) сведения о программе для электронных вычислительных машин или базе данных не составляют государственную тайну, и программа для электронных вычислительных машин или база данных не содержит сведений, составляющих государственную тайну.

Статья 12.1. Федерального закона от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации»

Госзакупки ПО

В настоящее время на рассмотрении в правительстве находится проект постановления, утверждающий правила ведения реестра отечественного ПО и устанавливающий ограничения на доступ иностранного ПО к госзакупкам. Предполагается, что постановление вступит в силу с 1 января 2016 года.

Постановление правительства установит запрет на закупку иностранного программного обеспечения за исключением случаев, если не существует российского программного обеспечения нужного класса, или оно не соответствует требованиям заказчика.

При осуществлении закупки программного обеспечения заказчик должен будет изучить реестр отечественного ПО на предмет наличия нужных решений.

Все продукты в реестре будут сгруппированы по классам. Ключевым параметром поиска отечественных решений будет класс ПО. Соответствие ПО определенному классу или классам находится в компетенции экспертного совета.

В помощь заказчику в реестре также будет реализована функция поиска российских решений того же класса, что и иностранные продукты. Указав название иностранного продукта, заказчик получит перечень отечественного ПО того же класса.

Помимо названий российских продуктов реестр будет содержать ссылку на сайт правообладателя с описанием продукта и контактной информацией о поставщике.

Если заказчику подходит одно или несколько российских решений, закупка ограничивается только отечественным ПО, а иностранные продукты не участвуют в тендере.

Если заказчику не подходят российские решения или российские решения соответствующих классов ПО не представлены в реестре, применяется исключение из запрета допуска иностранного ПО к госзакупкам. В таком случае заказчик должен сформировать в рамках тендерной документации обоснование невозможности выбора отечественных продуктов. В обосновании заказчик должен указать класс или классы закупаемого ПО, установленные заказчиком требования к ПО, функциональные, технические и эксплуатационные характеристики, по которым не подходят отечественные продукты. Обоснование должно быть опубликовано на сайте госзакупок.

В целях защиты внутреннего рынка Российской Федерации, развития национальной экономики, поддержки российских товаропроизводителей установить запрет на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд, за исключением следующих случаев:

а) если в реестре отсутствуют сведения о программном обеспечении, соответствующем тому же классу программного обеспечения, что и программное обеспечение, планируемое к закупке;

б) если программное обеспечение, сведения о котором включены в реестр и которое соответствует тому же классу программного обеспечения, что и программное обеспечение, планируемое к закупке, по своим функциональным, техническим и (или) эксплуатационным характеристикам не соответствует установленным заказчиком требованиям к планируемому к закупке программному обеспечению;

в) если исключительное право на программное обеспечение, планируемое к закупке, принадлежит российской организации, и сведения о таком программном обеспечении и (или) о закупке составляют государственную тайну.

Проект постановления Правительства Российской Федерации «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»

Решение для органов власти

Система «Адванта» для управления проектами органов государственных организаций

В последние годы в государственных органах все активнее развивается проектное управление. Утверждены методические рекомендации по внедрению проектного управления в органах исполнительной власти, создаются проектные офисы в регионах, утвержден и развивается российский стандарт по управлению проектами. Сейчас перед государственными органами власти стоит острая потребность в эффективных инструментах технологической поддержки проектной деятельности. Мы хотим рассказать о российском продукте, замещающем западные аналоги и во многом предоставляющем более широкие возможности – системе управления проектами «Адванта».

Система «Адванта» является российской разработкой компании «Адванта Консалтинг», она обеспечивает новые возможности для планирования и контроля проектов, организации межведомственного взаимодействия и контроля целевых показателей. Платформа развивается уже более 10 лет и легко адаптируется под задачи региональных органов власти без программирования. «Адванта» решает задачу импортозамещения продуктов Microsoft Project Server (сама по себе и в сочетании с Sharepoint) и её аналогов. При этом её стоимость в 3-5 раз дешевле западных систем.

Артемий Кызласов, генеральный директор УК «Титановая долина»:

Система «Адванта» автоматизирует и упрощает управление проектами и коммуникации между сотрудниками. Для того чтобы отследить ход проекта или обсудить текущие задачи, не обязательно встречаться – достаточно включить программу. При этом сотрудники могут находиться в разных офисах и даже городах. Мой рабочий график предполагает частые перелеты, и с помощью «Адванты» я оперативно получаю сообщения, читаю документы и ставлю задачи сотрудникам.

«Адванта Консалтинг» является не только разработчиком платформы «Адванта», но и оказывает услуги по ее внедрению. Большой опыт в развертывании системы в компаниях различного масштаба и государственных структурах гарантирует, что система «Адванта» приживется и будет использоваться. При этом в системе «Адванта» можно полноценно работать уже через месяц после запуска проекта внедрения, тогда как на развертывание «классических» систем управления проектами может уйти больше года.

Когда перед правительством Забайкальского края встала непростая задача – обеспечить в сжатые сроки жильем всех пострадавших при стихийных бедствиях, выбор системы управления проектом был сделан в пользу «Адванты». Уже через неделю после начала проекта внедрения в системе был создан реестр задач, по которому велась активная работа. Руководство смогло получать оперативные данные о состоянии проекта для принятия быстрых и эффективных управленческих решений в самые кратчайшие сроки.

Руководитель секретариата первого заместителя председателя правительства Забайкальского края М.В. Ведерников:

«Планируя переход на автоматизацию процесса управления проектной деятельностью в исполнительных органах государственной власти региона, правительство Забайкальского края проанализировало весь спектр специализированных программных продуктов, представленных на российском и зарубежном рынках IT-услуг.

Выбор системы «Адванта» был обусловлен ее соответствием ключевым критериям - широкая сервисная поддержка и готовность компании к совершенствованию программного обеспечения по просьбам клиентов. Процесс эксплуатации данной системы подтвердил обоснованность выбора: в кратчайшие сроки удалось организовать эффективное межведомственное взаимодействие в целях исполнения поручения президента Российской Федерации о строительстве жилых домов и выплатах компенсационной помощи забайкальцам, пострадавшим в результате природных пожаров в апреле текущего года, и автоматизировать процессы оперативного управления и контроля.

В настоящее время ведется работа по дальнейшему внедрению системы в исполнительных органах государственной власти Забайкальского края, с автоматизацией процессов управления иными значимыми инвестиционными и организационными проектами».

ADVANTA

Моя работа

Команда

Организация

Иконка сообщения

Иконка лайка

Профиль Олега

Олег

Главная

Гантт

Дискуссии (5)

Документы (10)

Согласования (2)

Участники (4)

Формы (1)

Затраты (4)

Учет времени (9)

Поступления (4)

Отчет о статусе Проекта (1)

Поставки (2)

Лента событий

Воронцов Олег удалил(а) запись в справочнике Учет времени в Проект для заказчика Комплексное переоснащение цеха для ООО "Спецтехника"

1 июля в 13:05

Воронцов Олег создал(а) документ Договор на изготовление турбокомпрессора с ОАО "Регионгаз" в Контакте с подрядчиком или поставщиком Договора на изготовление турбокомпрессора

30 июня в 16:46

Воронцов Олег создал(а) документ Договор на поставку с ОАО "Регионгаз" в Контакте с подрядчиком или поставщиком Договора на поставку комплектующих КР/1 от 12.05.2014

30 июня в 16:45

Воронцов Олег создал(а) документ Договор на ПНР с ОАО "Регионгаз" в Контакте с заказчиком Договора на пусконаладку

30 июня в 16:44

Воронцов Олег создал(а) документ Договор на реконструкцию с МУП "Трансмаши" в Контакте с заказчиком Договора на реконструкцию

30 июня в 16:43

Жуков Андрей создал(а) ответ на дискуссию Доступ в нашу Аванту внешним участникам проектов в Проект для заказчика Комплексное переоснащение цеха для ООО "Спецтехника"

30 июня в 14:46

Жуков Андрей создал(а) ответ на дискуссию Проблема с

Все проекты / Проекты для заказчиков / Новые проекты

Комплексное переоснащение цеха для ООО "Спецтехника"

Воронцов Олег Куратор

Жуков Андрей Руководитель проекта

Статус 17% В работе

Бюджет проекта 5 300 000 руб. Оплачено 5 050 000 руб.

Трудозатраты 2 280 чел./час. Выработано 2 332

Начало 11.06.2014 в 8:00

Завершение 14.07.2015 в 18:00

Жизненный цикл проекта

1. ИНИЦИАЦИЯ И ПЛАНИРОВАНИЕ

2. ПРОЕКТИРОВАНИЕ

3. ЗАКУПКИ

4. ПОСТАВКИ

5. СМП

6. ПНР

7. ЗАПУСК ОБЪЕКТА

← ВЕРНУТЬСЯ НАЗАД

ПЕРЕВЕСТИ НА СЛЕДУЮЩИЙ ЭТАП →

Реквизиты

Цель\Описание

Возвести два новых помещения для ремонта спецтехники и оснастить цеха оборудованием до 12.07.2015.

Техническое задание

Техническое задание

Настраиваемый атрибут проекта

В разделе Администрирование/Реквизиты, Вы можете создать самые различные атрибуты для проектов системы.

Заказчик изменить

ООО "Спецтехника"

Иерархическая структура

загрузить из excel | выгрузить в excel

Добавить

Найти... [иконка лупы]

открыть фильтр

развернуть все узлы

свернуть все узлы

подробный вид

[-] План проекта

[+] 1. Инициация проекта 49 % Жуков Андрей

[+] 2. Разработка ТЗ 100 % Ковалева Светлана

[+] 3. Разработка проектной документации 100 % Жуков Андрей

[-] 4. Поставка оборудования 100 % Жуков Андрей

- [+] 4.1. Заказ оборудования 100 % Воронцов Олег
- [+] 4.2. Контроль поставки 100 % Воронцов Олег
- [-] 4.3. Оборудование поставлено 100 % Воронцов Олег

[+] 5. Выполнение СМР 47 % Жуков Андрей

[+] 6. ПНР 0 % Жуков Андрей

[+] 7. Запуск объекта 0 % Жуков Андрей

[-] Контракты с заказчиком

- [+] Договор на реконструкцию 0 % Воронцов Олег
- [+] Договор на пусконаладку 0 % Ковалева Светлана

[+] Контракты с подрядчиками 0 % Жуков Андрей

[+] Совещания проекта 100 % Жуков Андрей

[+] Поручения 0 % Жуков Андрей

На базе платформы «Адванта» создано пять решений для государственных органов:

1. Система управления проектным офисом региона:
 - реестр ключевых проектов региона;
 - планирование мероприятий по достижению целевых показателей;
 - организация эффективного межведомственного взаимодействия;
 - электронные архивы документов по проектам;
 - управление рисками, проблемами, изменениями.
2. Система управления целевыми программами:
 - формирование плана реализации мероприятий программы;
 - формирование бюджета программы с учетом источника финансирования;
 - контроль достижения плановых индикаторов;
 - оперативное определение отклонений от плана;
 - автоматическое формирование отчетности.
3. Система поддержки инвестиционной деятельности корпораций развития:
 - оценка и отбор поступивших инициатив и формирование реестра проектов;
 - управление жизненным циклом инвестиционного проекта;
 - интеграция с порталом поддержки инвестиционной деятельности;
 - формирование сводных отчетов по проектам;
 - персональный онлайн-кабинет инвестора.
4. Система управления проектами строительства объектов:
 - формирование реестра строительных объектов региона;
 - контроль проведения конкурсных процедур по заключению контрактов на выполнение строительных работ;
 - контроль выполнения договоров в режиме реального времени;
 - автоматическая отчетность по финансированию и освоению денежных средств.
5. Система управления проектами внедрения инвестиционного стандарта:
 - формирование дорожных карт по внедрению стандарта;

- эффективная площадка для коммуникаций участников процесса;
- организация онлайн-анкетирования экспертного сообщества для оценки достигнутых результатов;
- мониторинг хода реализации мероприятий дорожной карты;
- электронные протоколы заседаний экспертных групп.

В 2013 году по заказу АСИ по продвижению новых проектов на базе системы «Адванта» была создана система «Диалог» для организации процесса управления внедрением инвестиционного стандарта. Система позволила организовать единое информационное пространство для представителей АСИ, органов исполнительной власти и экспертов бизнес-сообщества в 85 субъектах РФ, а также предоставила наглядную отчетность для министерства экономического развития РФ и администрации Президента РФ.

Решения на базе «Адванты» внедрены в органах власти более чем в 10 регионах России. Среди них корпорации развития, органы исполнительной власти, министерства и IT-департаменты государственных организаций. Помимо прочего стоит выделить уникальные решения для правительства Свердловской области – платформу u2020, и Агентства стратегических инициатив (АСИ) – платформу «Диалог».

Статус выполнения		Раздел стандарта											
Показать показатели		01. Наличие инвестиционной стратегии			02. Утверждение плана строительства инфраструктуры			03. Ежегодное послание главы региона о достижениях и инвестиционных планах			04. Принятие закона о защите прав инвесторов		
Проект 1		Экспертная группа	Минрегион	Контрольная закупка	Экспертная группа	Минрегион	Контрольная закупка	Экспертная группа	Минрегион	Контрольная закупка	Экспертная группа	Минрегион	Контрольная закупка
Южный федеральный округ	Краснодарский край												
	Республика Калмыкия												
	Ростовская область												
Центральный федеральный округ	Брянская область												
	Владимирская область												
	Воронежская область												
	Костромская область												
	Курская область												
	Орловская область												
	Рязанская область												
	Смоленская область												
	Тамбовская область												
	Тульская область												

Система «Адванта» - скриншот

Л.Ю. Белова, начальник отдела развития информационного общества министерства информационных технологий, связи и средств массовой информации Нижегородской области:

«Министерством информационных технологий, связи и средств массовой информации Нижегородской области в целях координации работ по проектам в рамках государственной программы «Информационное общество Нижегородской области» используется автоматизированная информационная система комплексного управления проектами в сфере информационных технологий на базе решения «Адванта Груп». Большим плюсом при внедрении системы стало понимание разработчиками специфики реализации мероприятий в государственных органах. Необходимо отметить удобство и простоту использования системы для отражения этапов ведения работ по проектам, предоставления сведений о реализуемых проектах (финансировании, сроках, показателях, исполнителях и др.), возможность настройки системы в режиме кон-

ADVANTA

система управления проектами



Российская
разработка



Запуск
за один месяц



Дешевле западных
аналогов в 3-7 раз



Более 15 успешных
проектов в гос. органах

5 решений для гос. органов*

- Система управления проектным офисом региона
- Система управления целевыми программами
- Система поддержки инвестиционной деятельности корпораций развития
- Система управления проектами строительства объектов
- Система управления проектами внедрения инвестиционного стандарта

*Разработано в соответствии с методическими рекомендациями Минэкономразвития по внедрению проектного управления в органах государственной власти

Об импортозамещении в области IT



Наталья Касперская,
генеральный
директор компании
InfoWatch

Автор рассматривает проблему импортозамещения с самых общих позиций. К сожалению, за год, прошедший со времени написания статьи, ни одно из её положений не утратило актуальности.

Преамбула. Проблема

Сейчас в государстве все яснее становится осознание необходимости срочного импортозамещения в ключевых IT-областях. Это понимание пришло как после введения санкций со стороны иностранных государств, так и после разоблачений Эдварда Сноудена по поводу тотальной прослушки Агентством национальной безопасности США всех устройств, поисковых систем, бесплатных почтовых служб, служб размещения фотографий и пр. Никакая тайна частной жизни не ограничивает АНБ в сборе данных абсолютно обо всех гражданах как своего, так и других государств. Если же гражданин представляет какой-то интерес для данного агентства (являясь, к примеру, канцлером Германии, или крупным российским чиновником, или бизнесменом), то пристальный контроль всех коммуникаций ему гарантирован. При этом АНБ становятся известны данные о массовых перемещениях и предпочтениях граждан. Российские граждане в связи с современной политической ситуацией становятся объектом особенно пристального наблюдения.

Помимо слежения, нельзя исключать сценарий (в случае ухудшения политической ситуации) полного выключения американских устройств или работающих на американских технологиях компьютерных систем (а это 90% всех имеющихся в России устройств) – настольных компьютеров и ноутбуков, планшетов и смартфонов, устройств или роботов, имеющих выход в Интернет, да и самого Интернета, который тоже в значительной мере является американским. Заметим себе, что даже компьютеры или устройства, собранные не в США, а, например, в Китае, также зависят от Америки, поскольку используют чипы, BIOS, операционные системы американского производства. Это дает Штатам ровно такую же возможность удаленного влияния.

Что говорят?

Хорошим ответом на тотальную зависимость от США могло бы стать импортозамещение американских технологий отечественными аналогами. Мы (Ассоциация разработчиков программных продуктов «Отечественный софт», АРПП) неоднократно говорили о необходимости подобного импортозамещения, но эта инициатива, к сожалению, не находила должного понимания среди государственных мужей. Сейчас я часто участвую в различных мероприятиях, посвященных импортозамещению, и вижу огромный разброс мнений по поводу того, что же делать. Мнения колеблются от «всё пропало, ничего уже не исправить и никогда не догнать» до «давайте выделим 100 миллиардов долларов и сделаем все своё лет за 10-15».

Мне бы хотелось обсудить оба этих мнения, а также предложить свой взгляд на решение проблемы.

Итак, по поводу того, что «всё пропало». Россия всегда славилась ассиметричными ответами и умением находить выход из, казалось бы, невозможных ситуаций. Вспомним историю индустриализации стра-

**Мы можем сразу перешагнуть на ступеньку
создания, например, мощных планшетов, минуя этап
создания персонального компьютера**

ны, когда за 15 лет в абсолютно разоренной после гражданской войны стране была построена промышленность и дан старт нескольким научным школам. Вспомним историю создания атомной бомбы сразу после тяжелейшей войны, унесшей почти 10% населения. Историю запуска первого в мире космического корабля с человеком на борту и проч. Когда мы хотим, мы можем. А это значит, что нужна политическая воля и желание. Тогда находятся и гении, и необходимые ресурсы, и неординарные способы решения сложнейших задач.

Так вот и по поводу современных IT – нам вовсе не надо пытаться восстановить всю историю разработки компьютерных технологий за последние 30 лет. Мы можем сразу перешагнуть на ступеньку создания, например, мощных планшетов, минуя этап создания персонального компьютера. Возможно, на начальном этапе это придется сделать вместе с нашими друзьями-китайцами, которые не меньше нас заинтересованы в избавлении от технологической зависимости.

Второе замечание – по поводу стоимости разработки и необходимости разработки всего с нуля. Если мы возьмем программные продукты,

то в России есть довольно много из того, что составляет цифровой суверенитет. Есть несколько клонов Linux. Есть свой антивирус. Есть ключевые разработки в области СУБД и ERP. Есть офисные приложения, основанные на открытом ПО. Есть множество специализированных разработок для промышленности, в т.ч. военной.

Китайский опыт, кстати, весьма интересен. Китайцы гораздо дальше нас продвинулись в создании собственной элементной базы и развития своего цифрового суверенитета. Однако, по меткому замечанию одного чиновника, их слабость состоит в том, что ядро технологии (а именно – чип и процессор), как игла, где лежит жизнь у Коцея Бессмертного, им не принадлежит.

Что делать?

Для начала я предлагаю разделить задачу по импортозамещению в области ключевых IT на две части:

- разработки, аналоги которых имеются в РФ;
- разработки, аналогов которых в РФ нет.

Очевидно, что стратегия для этих двух частей должна быть различной.

Импортозамещение в областях, где у России есть готовые продукты

По п. 1 задача решается довольно просто. По сути, здесь лишь нужна государственная воля. Начать надо, естественно, с ключевых объектов, находящихся в государственной собственности или контролируемых государством (т.е. тех, которые в первую очередь могут попасть под санкции). Для них в регламент по госзакупкам должен быть внесен пункт о необходимости закупки отечественного продукта при его наличии. При этом соответствующему пункту при тендерной закупке должен назначаться максимальный вес.

В качестве критерия «отечественности» предлагаю считать нахождение компании-разработчика в определенном Реестре отечественных IT-разработчиков, который сейчас разрабатывается совместно Минкомсвязью и АРПП.

Импортозамещение в областях, где у России нет готовых продуктов

Здесь ситуация более сложная. Мне представляется разумным следующий алгоритм.

Для начала определить технологии, которые действительно необходимы и без которых страна не может обойтись в случае самого худшего сценария (например, полностью исключили все иностранные ИТ-системы в стране). Это должен быть список, причем он не может быть длинным. Мне представляется, что в список могут войти:

- чип;
- процессор;
- BIOS;
- СУБД;
- системы управления производственными процессами (АСУ ТП).

Объявить эти темы приоритетными и выделить на них госфинансирование хотя бы в рамках существующих программ или фондов (ФРИИ, РВК, «Сколково», «Лидер2, ФЦП ИР по ИТ при Минобразовании). Если в рамках существующих программ это невозможно, то открыть специализированную программу поддержки ключевых разработок.

Мне не кажется, что задача реализации областей, где у нас нет заделов, может быть осуществлена силами НИИ хотя бы по той причине, что нам необходимы продукты, которые бы имели не узкоспециализированное применение, а массовое. НИИ, как правило, не отличаются способностью делать массовый продукт. Следовательно, необходимо частно-государственное партнерство. Это можно сделать, используя сразу три пути:

- понятным, четким и простым механизмом выделения средств на разработку;
- гарантированным госзаказом;
- созданием рабочей группы, которая бы координировала развитие ключевых разработок. Группа должна быть создана под эгидой правительства РФ, чтобы избежать межведомственных распрей. В нее должны войти представители заказчиков (госкопаний или компаний с госучастием), которые должны рассказать о своих потребностях, представители министерства связи и другие регуляторы, и собственно ИТ-

разработчики. Последнее важно для того, чтобы все заказы не ушли в НИИ на перспективы в 20-30 лет.

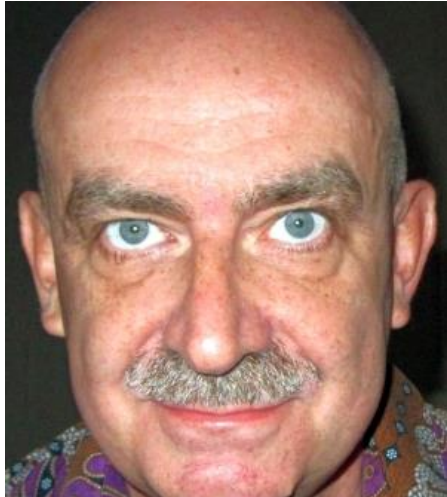
Из всех вышеперечисленных пунктов ключевым является госзаказ. Работать просто за деньги, выделяемые на разработку, разработчикам неинтересно, т.к. это не дает никакой прибыли, а ввергает компанию в постоянные расходы по развитию, поддержке и настройке произведённых продуктов. Нужен именно госзаказ. Тогда эта модель становится вполне рыночной, и у разработчиков появляется стимул разрабатывать недостающие элементы.

Вывод

На мой взгляд, дальнейшее промедление в этой области подобно смерти государства. И поэтому мы все должны максимально быстро начать решать проблему. На мой взгляд, она может быть решена относительно небольшими вложениями. Разработанные у нас элементы можно потом продавать в дружественные к нам страны, озабоченные доминированием США в технологиях. Как то: Китай, Малайзия, Индонезия, Индия, Бразилия и др. В том числе, кстати, Ближний Восток. Арабы хотя и любят говорить о своей дружбе с Америкой, но не преминут заменить часть IT-продуктов не-американскими. А поскольку своих у них вообще нет, то сотрудничество с Россией может быть очень перспективным. ■

Нормативка

Импортозамещение софта: закон, постановление правительства, приказ по министерству



Андрей Анненков,
Шеф-редактор
портала d-russia.ru

Минкомсвязь 1 апреля 2015 года издала приказ №96 «Об утверждении плана импортозамещения программного обеспечения». Смысл события – не инженерный, а бюрократический, он состоит в том, чтобы Минкомсвязь выполнила распоряжение правительства от 27 января №98-р, где приведён план первоочередных мероприятий по обеспечению экономического развития и социальной стабильности в 2015 году. П. 41 этого плана требует от Минкомсвязи к 1 апреля «утверждения и обеспечения реализации отраслевых программ (планов) импортозамещения».

Десять лет с правом импортозамещения

Давайте посмотрим в прилагаемую к приказу таблицу, там написано, что, к какому сроку и в какой степени должно быть импортозамещено. Горизонт планирования впечатляет – целых 10 лет. Промежуточные результаты, правда, должны быть уже через пятилетку.

Обсуждать цифры не приходится, их надо обеспечить, и всё тут – приказ есть приказ. Через пять лет офисный софт в России должен быть на четверть нашим, а через 10 лет – наполовину. Но тут есть вопросы.

Во-первых, в чём измеряются проценты импортозамещения? Хочется верить, что в деньгах. Представители отрасли, во всяком случае, другого измерителя не видят.

Во-вторых, что значит – «при согласовании и финансовом обеспечении реализации проектов импортозамещения»? Приходится пред-

положить, что разработчики документа допускают неисполнение приказа при определённых условиях.

Приложение к приказу
Министерства связи и массовых коммуникаций
Российской Федерации
от № 96
01.04.2015

План импортозамещения программного обеспечения

№ п/п	ОКПД (преимущественно)	Направление	Срок реализации проекта	Доля импорта в 2014 г.	Максимальная доля импорта к 2020 г.	Максимальная доля импорта к 2025 г.
Сегменты рынка корпоративного программного обеспечения, по которым уже имеется задел в виде конкурентоспособных отечественных продуктов - предпочтений отечественной продукции информационных технологий при осуществлении закупок за государственный счет						
1	58.29.21.000	Бизнес-приложения (ERP, CRM, BI, СЭД, управление проектами и т.д.)	2015-2025	75%	50%	25%
2	58.29.21.000	Антивирусное программное обеспечение и программное обеспечение информационной безопасности	2015-2025	60%	50%	40%
3	58.29.12.000	Интернет-сервисы, применяемые в корпоративной среде (электронная почта, сервис файлового обмена, интернет-браузер, картографический сервис, сервис обмена мгновенными сообщениями и т.д.)	2015-2025	50%	25%	10%
Сегменты рынка корпоративного программного обеспечения, по которым нет достаточного задела в виде конкурентоспособных отечественных продуктов - поддержка коллективной разработки программного обеспечения						
4	58.29.11.000	Клиентские и мобильные операционные системы	2015-2025	95%	75%*	50%*
5	58.29.11.000	Серверные операционные системы	2015-2025	75%	60%*	50%*
6	58.29.13.000	Системы управления базами данных	2015-2025	86%	70%*	50%*
7	58.29.21.000	Средства управления "облачной" инфраструктурой и виртуализацией	2015-2025	93%	75%*	50%*
8	58.29.21.000	Пользовательское офисное программное обеспечение	2015-2025	97%	75%*	50%*
Сегменты рынка программного обеспечения, связанные с отраслевой спецификой						
9	58.29.21.000	Программное обеспечение для промышленности (PLM, CAD, CAM, CAE)	2015-2020	88%	60%*	50%*
10	58.29.21.000	Программное обеспечение для ТЭК	2015-2020	95%	70%*	50%*
11	58.29.21.000	Программное обеспечение для строительства (BIM, CAD, CAM)	2015-2020	80%	60%*	50%*
12	58.29.21.000	Программное обеспечение для здравоохранения	2015-2020	90%	70%*	50%*
13	58.29.21.000	Программное обеспечение для финансового сектора	2015-2020	70%	60%*	50%*
14	58.29.21.000	Программное обеспечение для транспорта	2015-2020	80%	65%*	50%*

* при согласовании и финансовом обеспечении реализации проектов импортозамещения, в соответствии с параметрами паспортов проектов (п. 2.6 Приказа)

Правильный ответ на эти вопросы состоит в том, что лучше их не задавать. Приказ министерства имеет, увы, лишь символический смысл. Минкомсвязь, как было сказано, исполняет поручение правительства, и делает это вполне формально. Важен не план как таковой, а то, что под него дадут деньги, льготы и иные важные вещи, вплоть, наверное, до орденов.

Об этом говорил Николай Никифоров на упомянутой встрече с представителями софтверной индустрии в марте 2015 года: Минпромторг под импортозамещение получит средства, надо и Минкомсвязи этого добиться. Об этом же как о наиболее вероятном мотиве издания приказа говорят и представители индустрии, с которыми Экспертному центру электронного государства удалось поговорить.

Президент РУССОФТ Валентин Макаров говорит, что, во-первых, до тех пор, пока у государственных потребителей не определены критичные технологии, важные для безопасности и технологической независимости страны, не выделены ресурсы и не составлены планы по замещению критичного ПО, составление планов разработки ПО для импортозамещения не имеет большого смысла. Во-вторых, насколько известно президенту РУССОФТ, у Минкомсвязи на импортозамещение нет бюджета, все средства сконцентрированы в Минпромторге и, скорее всего, большая их часть уйдет в госкорпорации на нерыночные проекты вроде разработки инженерного софта парой вузов вместе с «Ростехнологиями» — с невысокой вероятностью успеха и без надежды на коммерциализацию программного продукта.

За день до опубликования приказа Минкомсвязи на IT-саммите в Ереване тоже обсуждалось импортозамещение. По словам заместителя гендиректора Фонда содействия развитию малых форм предприятий в научно-технической сфере Павла Гудкова, ведущая роль — у Минпромторга, там уже готовы целых 18 планов, они с грифом «ДСП». И Минпромторг на софтверную индустрию смотрит как на отрасль, обеспечивающую эти планы, а не как на объект государственной заботы. Минкомсвязь же решает «локальные задачи импортозамещения».

Желающих поучаствовать в импортозамещательном движении вообще немало. Это и Роснано во главе с неувядающим Чубайсом, и «Росатом» с его проектом операционной системы, и Рогозин с Фондом перспективных исследований (его, как и Минпромторг, заботит инженерный софт). Открытый министр Михаил Абызов тоже старается не оставаться в стороне. У Минобороны «научные роты», что-то программируют. И Минэкономразвития тоже стейкхолдер, вносит посильный вклад.

Инновации в приказе

Приказ для отрасли стал пусть не самой большой (не сравнить с осенней идеей создания спецфонда для разработки софта за счёт по-

боров с производителей софта), но всё-таки неожиданностью. В тексте документа – два существенных новшества.

Речь не о п.п. 2.б и 2.в, где закреплено ожидаемое отраслью намерение регулятора обеспечить преференциями отечественного производителя программного обеспечения. Это-то как раз обсуждалось с отраслью, она давно этого ждёт.

Но неизвестно, что такое «автономная некоммерческая организация, деятельность которой будет направлена на организацию коллективной разработки программного обеспечения для сегментов с высоким уровнем зависимости от иностранного программного обеспечения», о которой говорится п. 2.г, и которую предполагается создать аж постановлением правительства?

Министр на встрече с отраслью вскользь об этом, т.е. о новой отраслевой ассоциации, говорил. У части присутствующих создалось впечатление, что это в его планах не главное, есть же отраслевые партнерства, и не одно, регулятор с ними и будет, наверное, сотрудничать.

Но случилось неожиданное. В добавление к РУССОФТ, АРПП, РАСПО, АПКИТ подготавливается ещё одно объединение, государственное. С какой идеей – непонятно. В ассоциации разработчиков программных продуктов «Отечественный софт» об этом ничего не знают, сказала нам исполнительный директор Евгения Василенко.

Валентин Макаров придерживается того же мнения. По его словам, то, что Минкомсвязь ведёт диалог с отраслью – хорошо, и в приказе учтено мнение специалистов, которые предлагали стимулировать внутренний спрос, требуя у госзаказчика мотивировать закупки импортного софта при наличии отечественного аналога. Что же касается намерения министерства создать «автономную некоммерческую организацию», то это неочевидная затея – такая структура не станет тратить выделенные ей государственные деньги с той эффективностью, которую обеспечивают опытные отраслевые ассоциации: «Они за 5 миллионов проведут одно мероприятие, а мы на те же деньги проводим 10».

Можно предположить, что государственная «автономная некоммерческая организация» для регулятора просто удобнее. С объединениями, созданными отраслью снизу и существующими уже много лет, договариваться сложно, а проводить через них свою отраслевую политику и вовсе высший министерский пилотаж, не всякий сумеет (хотя, как показывает предшествующий опыт, отрасль к такому сотрудниче-

ству открыта, даже с программистской вольницей из ISDEF государство может продуктивно работать).

Ключевой вопрос – кто эту «автономную некоммерческую организацию» будет финансировать. Получим на него ответ — и всё сразу станет ясно.

Пункт 2.д приказа, предполагающий закрепить постановлением правительства роль ОАО «Росинфокоминвест» в финансировании разработок программного обеспечения, обсуждать по горячим следам не возьмёмся. Заметим только, что отрасль просила у государства не финансировать разработку (на это она сама готова тратиться), а обеспечить внутренний спрос.

По гамбургскому счёту

Если оставить за скобками мнение «у Минкомсвязи нет ни бюджета, ни власти влиять на программу импортозамещения софта, поэтому не важны ни указанные в приказе сроки, ни проценты» и попытаться рассмотреть план по существу, обнаружатся критические уязвимости документа.

Главное – время. Пять и тем более 10 лет – прекрасный срок, за это время можно на Марс слетать, не то что офисный пакет отладить. Хотелось бы всё же обоснования. Например, почему за пять лет доля отечественных продуктов на внутреннем рынке антивирусов повысится только до 60% против нынешних 50%, а к 2025 году – ещё на 10%.

Своей СУБД, равной импортным, у нас нет, и едва ли она за пять лет появится – ситуация кардинально отличается от того, что мы имеем на рынке антивирусов и систем безопасности. Однако Минкомсвязь хочет заместить импорт СУБД к 2020 году сразу на 16%.

Мнения экспертов из софтверной отрасли по поводу сроков расходятся кардинально. Есть те, что считают намеченные планы нереалистичными, рискованными. Есть и другие, кто полагает неоправданным намечать результаты на пять лет вперёд, хотя бы потому, что к этому времени импортозамещать надо будет уже не ОС и не СУБД, а что-то другое.

Так или иначе, нужны обоснования. Судя по тому, что с отраслью авторы министерского плана проценты импортозамещения и сроки не обсуждали, таких обоснований не существует. ■

Безопасность

Хищническая добыча данных, или Почему и как государство должно заботиться об информационной гигиене



Леонид Филатов,
основатель хостинговой компании masterhost, сервиса статистики «Openstat» и аналитического сервиса index.ru

Промышленная разработка данных различной степени персонализации приняла масштаб, позволяющий назвать происходящее цифровой вакханалией. Например, для идентификации пользователя Интернета – даже если он сменит мобильный телефон и компьютер и не возобновит ни одной учётной записи – гарантированно хватит восьми различных геолокационных наблюдений: где и в какое время человек побывал. Восемь выходов в Сеть или «чекинов» (а множество мобильных приложений фиксируют данные геолокации без ведома пользователя, который не читая принял пользовательское соглашение), и про вас знают всё – ваше имя, где вы живёте, за какую команду болеете, чем болели (уже в медицинском смысле) последние полгода, кто ваша любовница или любовник и пр., и пр., и пр.

Добыча этих данных ведётся у всех на виду, последствия – непредсказуемы, но точно не положительны. Однако почти никого происходящее не тревожит. Ситуация равна той, что имела место в европейских роддомах

полтора века назад: несмотря на открытие доктора Земмельвейса, которое сделало, казалось бы, совершенно обязательными простейшие правила гигиены, роженицы тысячами продолжали гибнуть ещё пару десятилетий из-за того, что их осматривали не мывшие рук «врачи», перед этим вскрывшие труп.

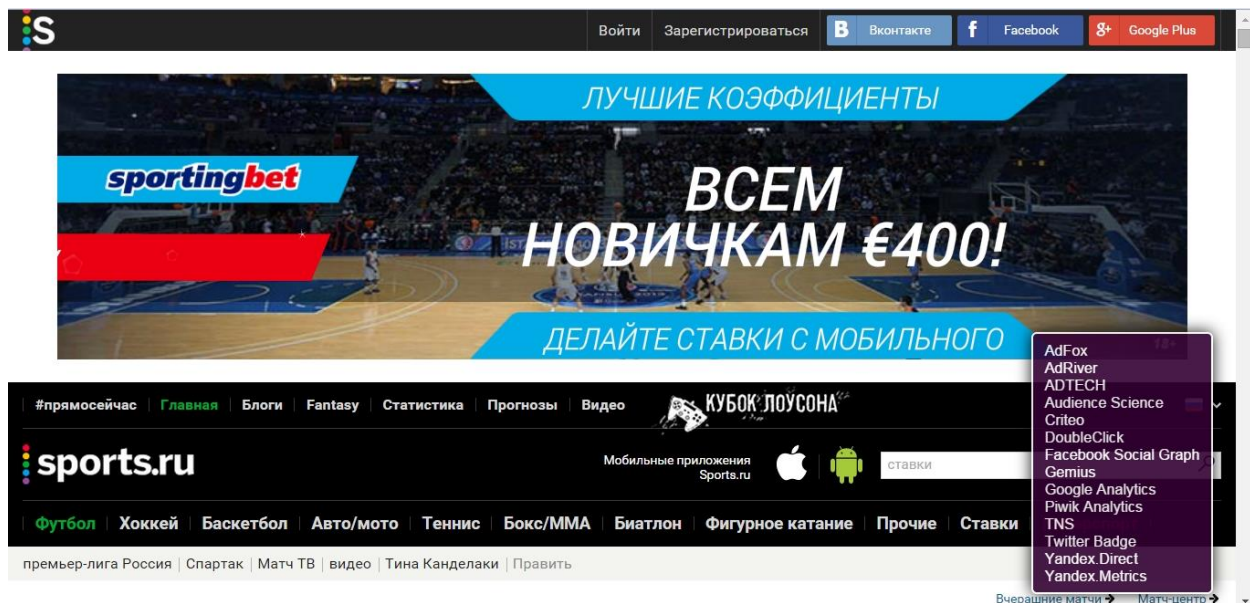
Кто и как

Добывают персональную информацию немногие, проблема, однако, в том, что добычей эти немногие готовы делиться (и делятся) со всеми, кто пожелает.

Первыми – по степени близости к персональным данным – среди добытчиков идут владельцы браузерных плагинов. Им проще всего добраться до ваших данных. Плагины имеют дело с данными уже после того, как пользователь вошёл в браузер, т.е. шифрование трафика, например, никак не поможет. История посещений, круг общения, привычки – всё, что «знает» браузер, потенциально доступно коду плагина. Защиты от этого кода нет, вы же сами его поставили.

Далее – внешний код, загружаемый для обработки браузером. Это счётчики посещаемости (Google Analytics, Яндекс.Метрика, Liveinternet, OpenStat и пр.), кнопки социальных сетей, рекламные системы – все они загружают на ваш компьютер инструкции, исполняемые браузером. Беда в том, что эти инструкции, в свою очередь, загружают другие инструкции – как собственные (если код, например, счётчика модифицируется – он делает это без ведома пользователя), так и чужие, чаще всего рекламных систем.

Владельцу сайта не возбраняется и самостоятельно загружать на ваш компьютер код рекламных систем, и вообще любой исполнимый код.



Сайт спортивных новостей «вживляет» в браузер сразу 14 самостоятельных фрагментов исполняемого кода – фактически приложений, о большинстве которых пользователь ничего не знает (данные получены благодаря сервису www.ghostery.com)

Сайт, загрузивший на ваш компьютер внешний код, в итоге отправляет собранную информацию (а она разнообразна – фиксируется всё, вплоть до траектории указателя «мыши») на серверы рекламной системы или статистического сервиса, а также оставляет ее в файлах – для себя и для «смежников».

Да, браузер имеет функцию удаления или блокировки cookies, но автор внешнего кода не обязан соблюдать правила – в его распоряжении другие способы сохранить cookies без разрешения. Например, с использованием технологии Adobe Flash. Если ваш браузер, что скорее всего так и есть, несёт на борту вами же установленный плагин Adobe Flash (мощный интерпретатор со своим языком программирования, с его помощью можно много что сделать, причём бесконтрольно), вы никогда не узнаете, что и где о вашем онлайн-поведении записано на вашем же диске, и кто эти сведения выкачивает.

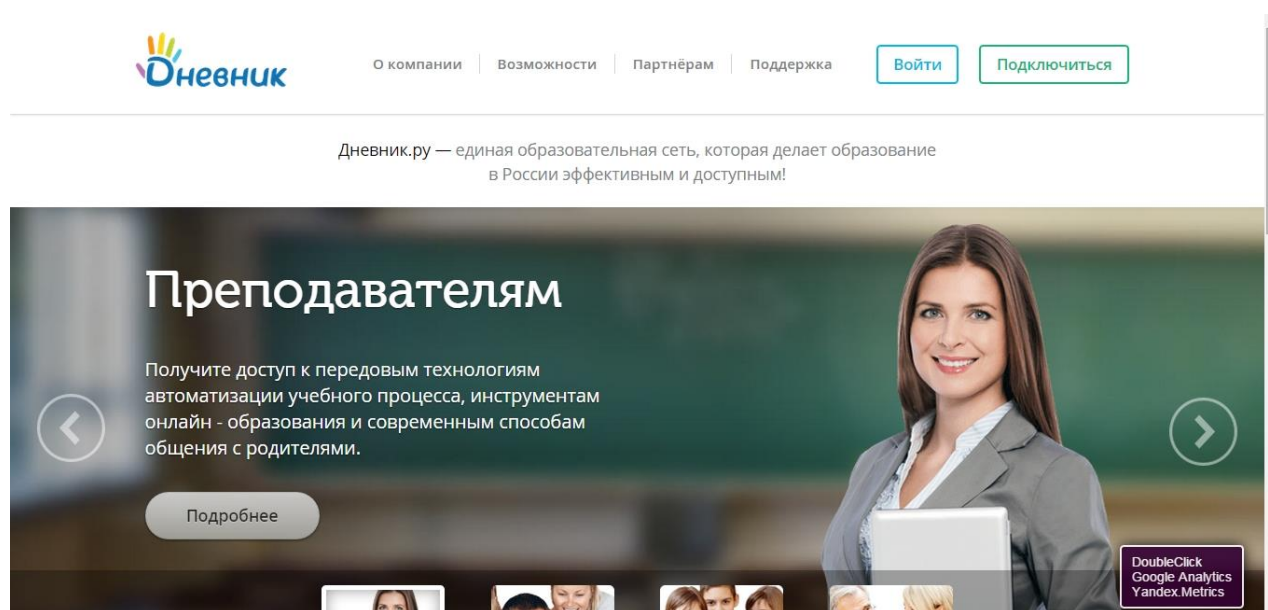
Третьими после владельцев браузерных плагинов и хозяев внешнего кода в пищевой цепочке идут провайдеры, как хостинговые, так и магистральные. От магистральных, впрочем, есть защита – например, трафик можно шифровать. Но возможности защититься сильно ограничены. Провайдер хостинга на своём веб-сервере – а это он взаимодействует с браузером – может устроить собственную ловушку для данных. Незашифрованный же трафик успешно анализируется в канале «глубокой инспекцией» IP-пакетов (Deep Packet Inspection, которая определяет, какой IP-какому пользователю принадлежит).

Кому выгодно

Данные, собираемые всеми этими способами, нам же и нужны, утверждают владельцы сайтов, счётчиков и рекламных систем – ради правильной («таргетированной») рекламы.

Это неправда. Не пользователю собранные данные предлагают, а посредникам между ним и абстрактными «заинтересантами». Ими могут быть и продавцы услуг и товаров, но вовсе не обязательно – посредник, собравший сведения о вас, продаст их не только продавцу, а кому угодно. Ни закон, ни технические средства этому никак не препятствуют. Как следствие, существует целая высокоразвитая индустрия данных, отчуждённых от интернет-пользователей. Насчитывается 20 тысяч систем, предназначенных для сбора данных о пользователях Интернета.

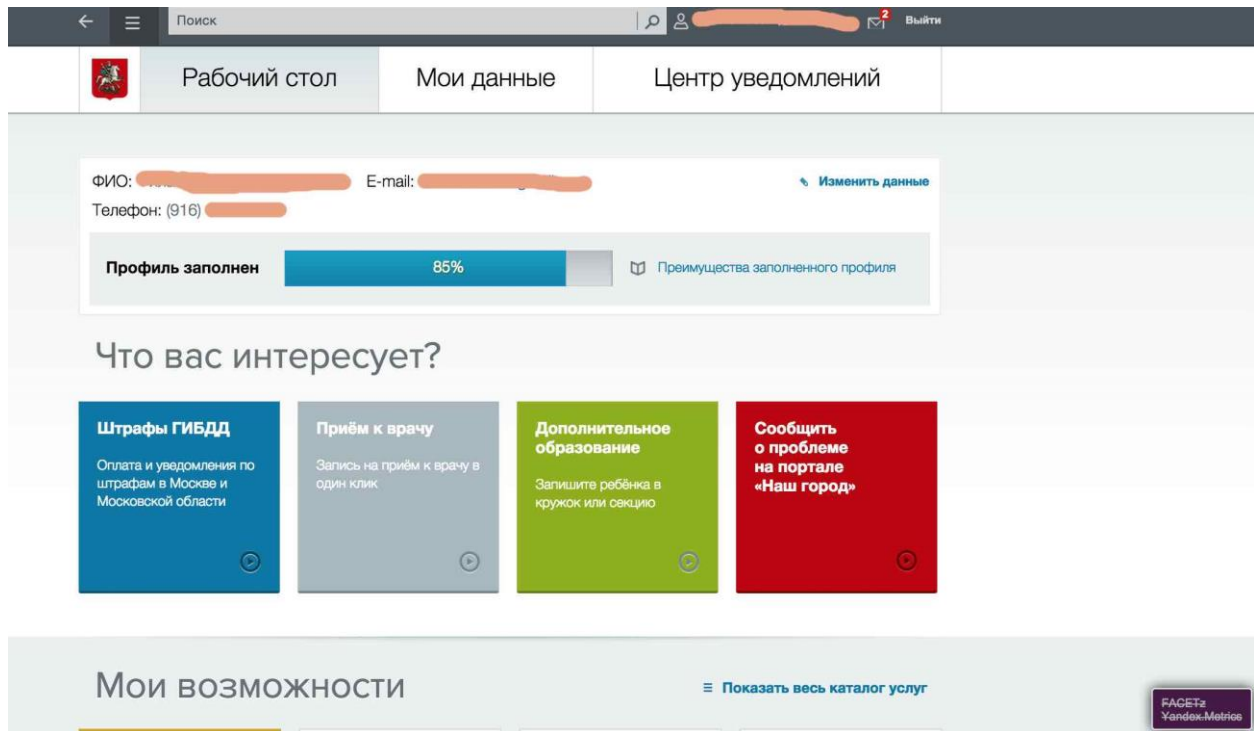
Но это ещё не проблема. Проблема в том, что в ближайшем будущем нас поджидает ситуация, когда персональные данные – фактически украденные, потому что даже легальные владельцы сервисов, подсовывающие пользователю своё пользовательское соглашение, действуют как воры на доверии – привлекут внимание криминалитета. Представьте, что у уличного преступника, желающего вас ограбить, появилась возможность недорого узнать, много ли денег в вашем бумажнике – и вы получите достаточно точную аналогию с тем, что уже происходит в киберпространстве, где содержимое вашего бумажника, и не только оно, уже сосчитано.



Электронный дневник – данные, которые видит (и вводит) родитель, потенциально доступны владельцам двум статистических сервисов и одной рекламной системы – указаны внизу справа

Способы корыстного использования персональных данных ограничены только фантазией мошенника. Ну, например. Внешний код в браузере добывает строки символов, которые вы вводите на сайте медицинской лаборатории – и у кого-то в руках оказываются диагнозы тысяч людей. Деятельность сыскных агентств, чьё благополучие обеспечивают главным образом ревнивые супруги, упростится до последнего предела, стоит только добраться до заботливо собранных статистическими системами пользовательских данных. Ещё пример – электронный дневник вашего ребёнка. Взгляните сами, кто кроме вас следит за его успеваемостью.

Хотите знать, кто еще собирает сведения о вашем имуществе, жилищных условиях, о том, в какую школу или детский сад ходит ваш ребенок? Пожалуйста в личный кабинет московского портала госуслуг – pgu.mos.ru:



Московский портал госуслуг позволяет собирать данные о посетителе счётчику статистики и рекламной системе

Как видим, кроме вас ваши данные доступны сервису статистики «Яндекса» и рекламной системе. Вы давали им разрешение на доступ к своим персональным данным?

Наивно думать, что это не страшно. За сведения о талантливом ребёнке заплатят вузы и работодатели. За сведения о нерадивом – изготовители фальшивых дипломов. И т.д. Маловероятно, что Google.Analytics и Яндекс.Метрика отдадут собранные данные на сторону, они им самим нужны (хотя АНБ не придётся, скорее всего, долго уговаривать Google поделиться сведениями о гражданах РФ), но за рекламные системы ручаться нельзя. Они уже открыто торгуют этими данными.

Отдельная тема – шпионаж, в том числе государственный, именуемый разведкой. Да, с помощью СОПМ спецслужбы контролируют внутри страны все сколь-нибудь крупные IT-системы. Но СОПМ не обеспечит тотальную, на протяжении всей жизни, слежку за каждым, а именно такая слежка открывает принципиально новые возможности, и дают их массовые IT-сервисы. Следи за всеми – и когда сегодняшний студент станет премьер-министром, у тебя в руках окажутся его связи, пристрастия, пороки, анамнез и бог знает, что ещё.

Что делать

Прежде всего, следует немедленно усовершенствовать закон: пора запретить врачам не дезинфицировать руки. Деятельность сборщиков чужих данных надлежит регламентировать, не дожидаясь жареного петуха, даже если технические средства контроля исполнения такого закона ещё не подоспели. Факт принятия закона создаст условия для их возникновения.

Следует законом или подзаконным актом запретить установку не прошедших сертификацию внешних кодов, чей функционал не может быть проконтролирован, на сайтах органов власти, госучреждений и, возможно, компаний с государственным участием.

Далее – и это тоже задача государства – следует предоставить гражданам надёжные средства личной информационной гигиены. Таким средством должен стать защищённый браузер со встроенной системой блокировки внешних исполнимых кодов. Этот браузер должен быть обязателен для посещения государственных информационных ресурсов – например, сайта госуслуг.

Наконец, необходимо популяризировать средства шифрования трафика, и вообще вести просветительскую работу с населением, 60%

**Деятельность сборщиков чужих данных надлежит
регламентировать, не дожидаясь жареного петуха,
даже если технические средства контроля исполнения
такого закона ещё не подоспели**

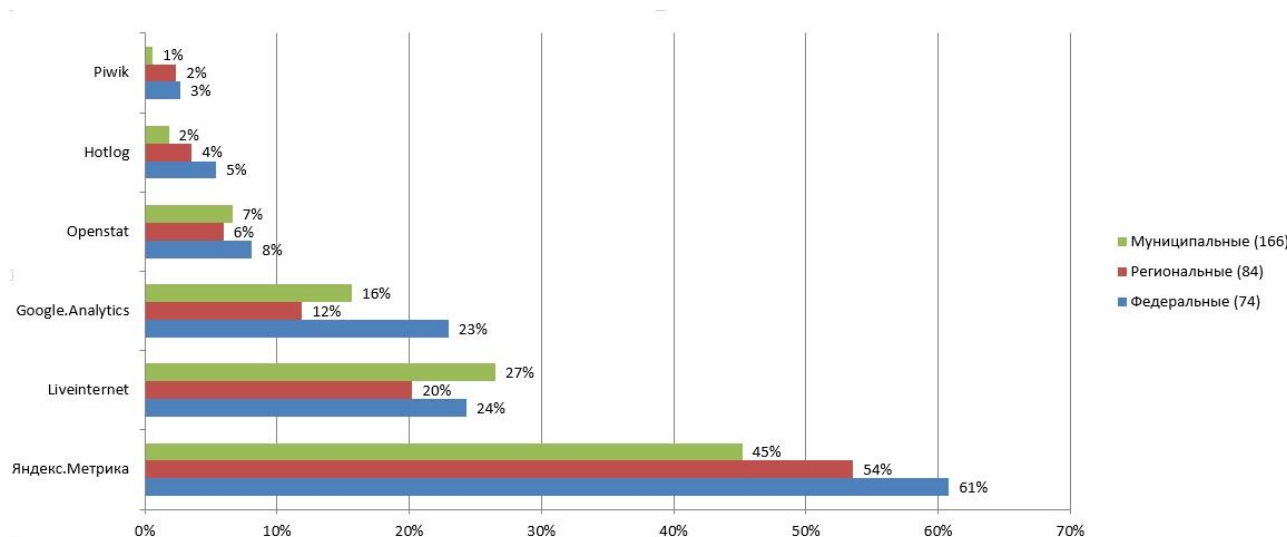
которого в нашей стране уже стали пользователями Интернета. Настоящее положение дел таково, что пользователь, желающий избежать неконтролируемого использования информации о себе самом, может рассчитывать только на себя. А для обеспечения эффективной личной IT-гигиены необходимо знать, что и как угрожает здоровью персональных данных.

Госайты и не думают защищаться

Отдельно следует обратить внимание на недопустимость использования внешних кодов на государственных сайтах. Существующее положение дел свидетельствует о недопустимой беззаботности их разработчиков – например, на 12% официальных сайтов региональных правительств используется счётчик Google Analytics. Из 84 региональных

правительственных сайтов 83 используют счётчики для сбора статистики.

Полные данные об использовании счётчиков (которые, повторим, могут загружать в браузер пользователя исполняемый код) сайтами федеральных, региональных и муниципальных органов власти см. на диаграмме. В анализируемую выборку вошли 324 сайта.



Данные об использовании счётчиков сбора статистики на сайтах государственных органов власти РФ

Если бы только Интернет

Тему деперсонализации персональных данных и безопасности государственных веб-ресурсов мы рассмотрели весьма поверхностно и довольно узко. По сути, лишь обозначили. За пределами изложения остались многие связанные вопросы, такие, в частности, как защита персональных данных на мобильных сервисах и устройствах, а также доступ к пользовательской информации на уровне не веб-сервисов, а настольных операционных систем. Рассмотреть все эти вопросы в одном тексте не позволяет объём публикации.

Это, впрочем, и не было нашей целью. Она состояла в том, чтобы аргументированно привлечь внимание к опасности и недопустимости нынешнего положения дел с безопасностью государственных онлайн-ресурсов, о беспечности, с которой их владельцы отдают вовне контроль над сайтами органов власти. ■

Решение для органов власти

Как избавиться от зарубежных облачных сервисов и обрести больше возможностей



**Александр
Архангельский**
Коммерческий
директор
ООО «Интеллекту-
альный резерв»

На рынке существуют два направления организации ИТ. С одной стороны, оптимизируя затраты на информационные технологии, органы государственной власти и коммерческие компании переходят на публичные облачные сервисы. С другой, в целях обеспечения безопасности и контроля над своими данными они ищут решения для собственного «частного облака». Например, востребованы решения по организации, хранению и доступу к данным с более богатым функционалом, чем у сервисов Dropbox, One Cloud, GoogleDrive и др. Компания «Интеллектуальный резерв», изучив эти тенденции, создала уникальный по сочетанию функционала [продукт VALO](#). Он может использоваться и как «частное облако», развернутое на собственной инфраструктуре организации, и как платформа для дата-центров, предоставляющих публичные сервисы.

VALO - частный облачный сервис для федеральных и региональных органов государственной власти (ОГВ), а также органов местного самоуправления (ОМСУ).

VALO является российской разработкой и обеспечивает следующие функциональные возможности:

VALO - частный облачный сервис для федеральных и региональных органов государственной власти (ОГВ), а также органов местного самоуправления

- автоматизированное непрерывное резервное копирование/архивирование рабочей информации (файлы);

- синхронизация файлов между любыми устройствами, используемыми сотрудниками (стационарные рабочие станции, ноутбуки, планшеты, мобильные устройства);
- предоставление пользователям совместного доступа и работы с файлами с любых устройств.

VALO разрабатывался и отлаживался в пилотных проектах на предприятиях коммерческого сектора, а также в региональных администрациях Российской Федерации. Был реализован принцип «простоты использования и администрирования», обусловленный существующими кадровыми проблемами и уровнем подготовки госслужащих в области ИТ.

VALO легко адаптируется под задачи ОГВ и ОМСУ, не требует дополнительного программирования, предъявляет минимальные требования к подготовке пользователей, обеспечивает легкость обучения работе с ним.

VALO является более функциональным решением для трех классов ПО иностранных вендоров и решает задачу их импортозамещения:

- резервное копирование (Back up): EMC, CommVault, Symantec, IBM, Veeam Software и др.;
- синхронизация и доступ к файлам (EFSS): Symantec, EMC, Veeam Software, Acronis, Citrix и др.
- облачные сервисы (Cloud-based Services): Dropbox, ownCloud, Box, Google Drive, Microsoft OneDrive и др.

VALO, построенный на базе классической архитектуры клиент-сервер, представляет собой веб-сервер, устанавливаемый у заказчика, и набор клиентского ПО на устройствах пользователей, привязываемого к учетной записи на сервере.

Серверная часть VALO устанавливается на физический или виртуальный сервер (2ГГц 3ГГц; 4Гб оперативной памяти) с ОС Linux (Ub-untu 14.04; Red Hat 6.0, 7.0). Для хранения данных приложения и файлов пользователей, используется БД PostgreSQL. Серверу VALO для хранения пользовательской информации рекомендуется выделять на пользователя порядка 10Гб дискового пространства.

VALO позволяет решать ряд типовых проблем, среди которых:

- проблема использования иностранных публичных сервисов государственными служащими для работы и обмена служебной информацией;

- возможность резервирования, безопасного доступа и контроля над служебной информацией сотрудников, в том числе работающих удаленно и в их отсутствие (инспекторы, выезды на места, командировки, отпуска и пр.);
- инструмент проектного управления в органах государственной власти. VALO позволяет организовывать проектные группы для совместной работы с документами проекта не только внутри организации, но и с привлечением, где необходимо внешних контрагентов. При этом сохраняется требуемый уровень безопасности;
- возможность контролируемого использования личных устройств для рабочих целей.

Стоимость VALO ниже иностранных аналогов и позволяет внедрять его и на муниципальном уровне, с учетом крайне ограниченных местных бюджетов.

VALO проходит пилотирование в региональных ОГВ и ОМСУ, а также в коммерческих организациях.



Дмитрий Разумовский,
министр развития
информационного
общества Калужской
области

«В последнее время мы стали внимательно изучать отечественный рынок программного обеспечения, используемого органами государственной власти в повседневной деятельности, – отмечает министр развития информационного общества Калужской области **Дмитрий Разумовский**. – Сегодня уже невозможно представить работу руководителей и государственных служащих среднего звена без использования сервисов коллективного доступа к корпоративному контенту, безопасного хранения и отображения информации на различных устройствах. К сожалению, сейчас для этого часто применяются зарубежные облачные сервисы. О безопасности информации, которая хранится на таких ресурсах, говорить не приходится. Именно поэтому отечественный продукт VALO показался нам наиболее удачным решением, позволяющим пользователям работать с документами, как в офф-лайн, так и в он-лайн режимах. Сейчас мы начинаем опытную эксплуатацию VALO, по результатам которой будет принято решение о масштабах и сроках его внедрения в органах власти Калужской области. Но уже сейчас мы совершенно четко представляем сферу и перспективы его использования».

Импортозамещение ПО

Импортозамещение ПО – шаг на месте к IT-суверенитету



Дмитрий Гоков,
генеральный директор
«AT Consulting
Сибирь»

Стоит начать с того, что сам термин «импортозамещение», возведенный сейчас в ранг некоего лозунга, не вполне продуктивен применительно к сфере программного обеспечения. Во-первых, большинство передовых проектов, задающих тон в мировой индустрии ПО, давно стали трансграничными и осуществляются международными сообществами разработчиков. Взять, к слову, свободные программистские сообщества Linux, GNU, Apache или, например, PostgreSQL, в котором неплохо представлены россияне. Сознательно отгораживаться от этого тренда и пытаться создать некий сугубо российский дублёр интернациональных разработок было бы, мягко говоря, странно. Ведь, как говорится, у Интернета нет таможни.

Во-вторых, понятие «импортозамещение», примененное к софтверной индустрии, несколько искажает смысл текущей государственной политики в IT-сфере, превращает одно из её средств в самоцель. Ключевая задача этой политики – обеспечение технологической независимости

Для обретения IT-суверенитета в сфере ПО нужно не только уметь создавать программные продукты, но и обеспечить полную подконтрольность их исходного кода, если они используются в госуправлении и стратегических отраслях экономики

РФ. Конечно, такая независимость тесно связана с импортозамещением, но ему не тождественна, и им не заменяется. Для обретения IT-суверенитета в сфере ПО нужно не только уметь создавать программные продукты, но и обеспечить полную подконтрольность их

исходного кода, если они используются в госуправлении и стратегических отраслях экономики. А вот способы, которыми данная цель будет достигнута – это, как говорится, вопрос техники.

Если принять за отправную точку контроль над программным кодом, то импортозамещение само по себе вряд ли решит эту задачу. Что принципиально изменится, если в госкорпорациях и ведомствах на смену проприетарному ПО иностранных разработчиков придет проприетарное ПО разработчиков российских? С точки зрения государственного IT-суверенитета – это шаг на месте. Исходный код по-прежнему останется в руках отдельных сторонних компаний. Причем в условиях глобального рынка не исключен потенциальный сценарий вхождения в их капитал иностранных участников, что вновь приведет к ситуации внешней технологической зависимости.

Можно, конечно, как-то регулировать IT-рынок, вводить ограничения на иностранное участие. Но это ограничит и инвестиционную активность, заведомо сократит потенциал развития отрасли. Рассматривать же в качестве источника инвестиций само государство вряд ли будет правильно, хотя это и обеспечит искомый контроль кода. Создание IT-бизнесов (как, впрочем, любых других) – не та сфера, где государство в силу своей сути может проявить себя эффективно, и примеров тому в российской действительности достаточно. Однако есть ли альтернативы?

Альтернативы, безусловно, имеются. Одна из них вполне очевидна и соответствует тренду мировой программной разработки двух последних десятилетий – распространению свободного программного обеспечения. Как известно, главная особенность СПО – открытый программный код, т.е. возможность его просмотра и неограниченной доработки. По сути, данное фундаментальное требование должно соблюдаться в любом программном продукте, используемом в стратегически значимых отраслях и госуправлении. Без этого государственный IT-суверенитет просто не возможен.

Исходя из такой логики, последовательная политика IT-суверенитета должна привести всё используемое в госсекторе ПО в соответствие с требованием открытого кода. Помимо обеспечения контроля это принесет бесспорные экономические выгоды, т.е. развитие рыночной конкуренции, а, следовательно, снижение стоимости внедрения, поддержки и доработки программных продуктов для госуправления.

Не стоит и говорить об актуальности этого обстоятельства при текущем дефиците финансирования государственных ИТ. Ведь какова сегодня типичная ситуация с развитием ПО в госорганах? Условное региональное ведомство обращается к своему подрядчику за разработкой дополнительного модуля ведомственной системы и предлагает бюджет «х», исходя из рыночной стоимости подобных работ. «Нет, – говорит подрядчик, – нам для этого нужен бюджет «3х». И в большинстве случаев заказчик вынужден соглашаться, жертвуя другими проектами, чтобы изыскать запрошенную подрядчиком сумму. А почему? Потому, что программный код большинства ведомственных систем закрыт, и среди разработчиков торжествует известный девиз «Никто, кроме нас».

Скажу больше – для обеспечения полноценного ИТ-суверенитета требования к ведомственным системам должны включать не только открытый код, но и наличие инструментов его доработки силами пользователя. Имеются в виду средства визуального программирования, легкие в освоении и позволяющие дорабатывать ПО вплоть до создания новых модулей, не затрачивая бюджетные средства на сторонних исполнителей. Данная возможность необходима как воздух, учитывая объем изменений, регулярно вносимых в ведомственные НПА. Без средств автономной доработки соответствующая актуализация информационных систем превращается в хронические «догонялки», когда госзаказчику «ещё вчера» нужно и средства изыскать, и конкурс провести, и в график разработчика встроиться.

Вместе с тем на российском рынке уже существуют автоматизированные СПО-платформы, позволяющие быстро погасить этот перманентный «пожар», заменив сложное длительное кодирование доступным и быстрым визуальным проектированием. С помощью таких решений зависимость потребителя ПО от специальных навыков разработчика сводится к минимуму. Заказчику обеспечивается не только прозрачность и безопасность программного продукта, но и возможность самостоятельно управлять его изменениями.

Еще одна особенность СПО, достойная введения в практику региональной информатизации РФ – технологии совместной разработки программных продуктов. В этом плане представляет интерес идея открытых репозиторий ведомственных систем, выполненных на основе СПО. Посредством таких хранилищ регионы смогут обмениваться программными разработками, при необходимости адаптируя их под свои особенности. Подобный репозиторий, например, уже создается на базе ИТ-кластера новосибирского Академпарка.

Надо сказать, Новосибирская область сегодня выступает своего рода полигоном, где решения СПО для госсектора проходят проверку практикой, и, кстати, небезуспешно. В техническом плане эти продукты уже вполне готовы к тиражированию в другие регионы, но для реализации данного проекта одной лишь инженерной составляющей мало. В частности, необходимы законодательные инициативы по введению СПО в правовое поле РФ. Ведь сегодня право пользователей свободно распространять и модифицировать СПО-продукты в России базируется, по сути, лишь на доброй воле их разработчиков и никак не подкреплено юридически. Однако, думаю, при наличии политической воли правовые основания для использования СПО могут быть сформированы достаточно быстро, тем более, что предпосылки для этого давно назрели.

Таким образом, подлинный государственный IT-суверенитет в сфере ПО никак не сводится к одной лишь замене импортных разработок на отечественные. Для его обретения нам предстоит ни много ни мало принять новую парадигму государственных IT-систем, основанную на СПО, участии в сообществе разработчиков, визуальном программировании. Парадигму, которая не отмежёвывается от мировых трендов, а напротив, максимально им соответствует. ■

Безопасность

О возможностях импортозамещения: взгляд участника российского рынка ПО



Дмитрий Курашев,
генеральный
директор компании
Entensys, член
правления ISDEF

Тема импортозамещения ПО в последнее время стала крайне популярной, в некоторых случаях она создает серьезные возможности отечественным компаниям, в некоторых – является предметом спекуляций, а иногда и объектом иронических насмешек. Понятно, что есть сферы, где на данный момент нереально полноценно заменить иностранные продукты и технологии, однако есть и такие классы программных продуктов, где это возможно сделать прямо сейчас.

В IT важно разделять сегменты, связанные с производством аппаратной части, где у нас возникло значительное отставание, и разработку программного обеспечения. Известно, что в России есть ряд компаний, разрабатывающих программные продукты, востребованные во всем мире. Есть также и значительное число грамотных разработчиков, имеющих существенно более высокую квалификацию чем те, кто занимается банальным аутсорсингом, и способных разрабатывать сложные продукты. Особенно это касается сегмента информационной безопасности (ИБ).

Как правило, проекты в области ИБ реализуются довольно крупными системными интеграторами, и основная доля рынка приходится на несколько десятков компаний. В конце 1990-х и в начале 2000-х годов сложилась устойчивая практика использования известных западных решений – работал принцип «ещё никого не уволили за покупку продуктов компании IBM». Интеграторы по сути выступали посредниками, обеспечивающими лишь обслуживание информационных систем, а ещё – реализацию многочисленных коррупционных схем. Часто работал принцип «чем дороже, тем лучше». При этом основная часть ассигнований на IT уходила за рубеж, что никоим образом не способ-

ствовало развитию российских технологий, а также высокотехнологических компаний.

Можно воспринимать данное положение вещей как объективную реальность, которую практически невозможно изменить, но можно и увидеть в текущей ситуации ряд новых возможностей. В области сетевой безопасности, где как раз работаем мы, многие известные западные компании используют многочисленные проекты с открытым кодом, лишь адаптируя его к своим платформам, другие приобретают небольшие стартапы, интегрируя их продукты в свою продуктовую линейку. В обоих случаях часто рынку предлагаются заурядные продукты под известным брендом. Многие такие продукты продаются уже более десяти лет и основаны на устаревшей архитектуре. Вообще в этой сфере невероятно широко используются общедоступные технологии, поэтому именно здесь имеет место высокая турбулентность и есть наибольшие возможности «догнать и перегнать».

Считаю, что разработка программного обеспечения – это как раз та самая сфера, где можно легче и быстрее ликвидировать отставание. Намного проще разработать качественный и конкурентоспособный

**Во многих случаях выбор ПО производится
исключительно между зарубежными продуктами.
Часто заказчику попросту неизвестны возможности
российских продуктов**

программный продукт, чем аппаратную платформу, процессор и вообще всё, что связано с электроникой. Для разработки ПО не нужна столь дорогая и нетривиальная аппаратная база, многие основные технологии общедоступны и могут позволить создать базовый продукт в сжатые сроки.

Основная проблема, стоящая перед отечественными разработчиками – это получение опыта реализации масштабных внедрений и тестирование своих технологий в рамках крупных проектов.

Уверен, что в ряде областей возможна разработка продуктов нового поколения российскими разработчиками. Если отечественная компания в текущей ситуации смогла разработать хотя бы сопоставимый по качеству с зарубежными аналогами продукт, это практически позволяет быть уверенным в возможности его дальнейшего успешного развития в случае реального увеличения внутреннего спроса. Вложение средств российских компаний в российские же продукты в любом случае приведет к быстрому росту их характеристик и функционально-

сти. По крайней мере, это возможно в сегменте ИБ, который, кстати говоря, особо важен для обеспечения IT-суверенитета страны.

Отдельно хотелось бы сказать о сертификации ФСТЭК. С одной стороны, она может считаться определенным барьером для проникновения иностранных продуктов, содержащих недеklarированные возможности. С другой – за последние десять лет сертификаты ФСТЭК получили многие сотни продуктов, и здесь уже по сути нет никаких преференций отечественным разработчикам (за исключением ПО для работы с данными, содержащими гостайну, и связанным с криптографией).

Очень надеюсь, что текущая ситуация повысит общий уровень информационной безопасности и поможет развитию высокотехнологичных российских IT-компаний. К сожалению, пока еще во многих случаях выбор ПО производится исключительно между зарубежными продуктами. Часто заказчику попросту неизвестны возможности российских продуктов, так как наши компании существенно уступают иностранным конкурентам по маркетинговым бюджетам.

Возможно, реестр отечественного ПО окажется действительно полезен отрасли. Со стороны власти важно не просто говорить о поддержке российских IT, но и реально общаться с разработчиками, используя, например, отраслевые ассоциации, такие как ISDEF (Форум независимых разработчиков программных продуктов). В любом случае поддержка существующих проектов, особенно тех, которые известны не только в России, будет существенно продуктивнее, чем продолжение почти тотального использования зарубежного ПО или же разработка новых систем с нуля, например, в рамках специального госзаказа. ■

Опыт региона

Импортозамещение – это, в первую очередь, независимость



Анатолий Дюбанов,
– член правительства
Новосибирской области –
руководитель департамента
информатизации и развития
телекоммуникационных тех-
нологий Новосибирской об-
ласти

Емкое и громкое слово «импортозамещение», в последнее время приобрело большое значение. Эта тема касается всех сфер нашей жизнедеятельности, но с определенным акцентом. В сфере информационных технологий, в первую очередь, речь идет о независимости от иностранных разработчиков программного обеспечения, поставщиков оборудования

Для департамента информатизации и развития телекоммуникационных технологий Новосибирской области вопрос импортозамещения прежде всего связан с достижением независимости от вендора, разработчика лицензионной модели, ну и по возможности – поддержкой новосибирских IT-компаний.



Алексей Горобцов,
заместитель руководителя де-
партамента информатизации
и развития телекоммуникаци-
онных технологий Новосибир-
ской области

О независимости мы задумались еще в 2011 году, когда разговоров об импортозамещении еще не было. Для реализации Федерального закона от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» программистами – резидентами Технопарка новосибирского Академгородка на базе свободного программного обеспечения (СПО) была разработана и внедрена информационная система. Система была создана менее чем за полгода и была внедрена в более чем 15 органах власти и 490 муниципальных образованиях Новосибирской области, количество пользователей превысило 2000 чело-

век. К сожалению, по прошествии некоторого времени компания-разработчик перестала существовать, но нам, как заказчику, это не доставило больших проблем, так как по завершении работ нам были переданы неисключительная лицензия и программный код данной информационной системы. Последующая доработка и модернизация системы была произведена уже другими разработчиками, выигравшими конкурс. Самое главное в этой ситуации, это то, что не потребовалось проводить перевнедрение системы на такое количество пользователей, ведь внедрение любого, даже очень нужного программного продукта, всегда очень сложный процесс для пользователей. И это, на наш взгляд, является классическим преимуществом модели СПО.

Еще к одному способу достижения независимости от вендоров можно отнести задачу последовательного замещения проприетарного программного обеспечения на свободное ПО. У нас есть положитель-

**Мы получаем независимость от вендора,
что в свою очередь гарантирует нам, что программный
продукт будет развиваться в любом случае**

ный опыт по замене баз данных (например, Oracle, Microsoft, IBM и т.д.) и переводу систем на облачные решения. Процесс длительный, трудозатратный, но на выходе получается открытая система с аналогичным функционалом.

Делается это, во первых, для ухода от лицензионной модели, ведь известно, что лицензия на каждое рабочее место обходится в определенные бюджетные расходы, а количество пользователей во всех системах сейчас стремительно растет. А во вторых, мы получаем независимость от вендора, что в свою очередь гарантирует нам, что программный продукт будет развиваться в любом случае.

В качестве примера можно привести систему электронного документооборота и делопроизводства правительства Новосибирской области. В настоящий момент ведутся работы по развертыванию открытой конфигурации СЭДД CompanyMedia, где в качестве слоя хранения данных будет использоваться СУБД PostgreSQL (ранее система базировалась на сервере IBM Domino).

Также сейчас мы завершили двухлетний переход на полностью СПО решение, без замены информационной системы, которая отвечает в Новосибирской области за все услуги социального характера, а это более 100 учреждений и более 2000 пользователей.

Имеет право на жизнь и способ понуждения исполнителя к переизданию существующих систем, созданных на СПО. Данный вариант приемлем при работе с крупными информационными системами, которые в процессе доработки архитектуры становятся своего рода конструктором. С помощью такого конструктора без помощи разработчика квалифицированные специалисты департамента могут собрать конфигурацию собственной информационной системы для автоматизации деятельности какого-либо министерства или ведомства. В основу берутся отработанные элементы, такие как реестры, порталные решения, печатные формы, элементы межведомственного взаимодействия и др., интегрируются с друг с другом и получается новая подсистема, актуальная для конкретного министерства. Вот представьте, вам нужна система управления очередью по реестру определенных категорий граждан с учетом определенных бизнес-процессов. В таком случае можно заказать новое решение, доработать существующее, но все эти варианты связаны с длительными конкурсными процедурами, выискиванием бюджетных средств, а ситуация такова, что решение вам нужно «здесь и сейчас». Мы на сегодняшний день в такой ситуации просто возьмем и соберем своими силами все это на конструкторе, обучим пользователей, получим обратную связь, ещё раз пересоберем систему по пожеланиям пользователя - и вопрос решен, и мы не от кого не зависим. По такому принципу в Новосибирской области разработаны и запущены в эксплуатацию уже две системы. Еще одним примером такого подхода служит типовой шаблон, разработанный для официального сайта губернатора Новосибирской области и правительства Новосибирской области. На типовом шаблоне запущены не только официальные сайты исполнительных органов государственной власти и частично сайты органов местного самоуправления Новосибирской области, [но и сайт контрольно-счетной палаты Новосибирской области, уполномоченного по правам ребенка Новосибирской области и уполномоченного по правам предпринимателей Новосибирской области](#), а также по обращению глав создано несколько сайтов сельских поселений Новосибирской области. ■

LantaPro®

Платформа автоматизации
учётных систем

ООО «ЛантаПро»
г. Тюмень, ул. Семакова, 10

+7 (3452) 69-52-05
+7 (3452) 63-88-63

director@lantapro.ru
www.lantapro.ru

ИМУЩЕСТВЕННЫЙ УЧЁТ

- Реестр имущества
- Аренда имущества
- Имущество юридических лиц
- Реестр объектов культурного наследия
- Реестр ветхого и аварийного жилья
- Балансодержатели
- Продажа имущества
- Акционерные общества

ЖИЛОЙ ФОНД

- Бюджетники
- Очередники
- Спецфонд
- Молодые семьи
- Социальный найм
- Приватизация

ЗЕМЕЛЬНЫЙ УЧЁТ

- Земельные участки
- Землеустроительные дела
- Аренда земельных участков
- Контроль использования земельных участков
- Дежурная карта
- Застройщики
- Совместная комиссия
- Сады и гаражи

ДОКУМЕНТООБОРОТ

- Документооборот
- Архив
- СМЭВ+Госуслуги
- Инвентаризация

СПЕЦИАЛЬНЫЕ МОДУЛИ

- Аукционы
- Поступления УФК
- Адресный реестр
- Судебно-исковая работа
- Документы
- Субъекты

Ключевые технологии платформы



Технология
интегрируемых
модулей



Технология
настраиваемых отчётных
и выходных форм



Технология
расширенных
выборок



Технология
пользовательских
профилей

Единая защищенная мобильная платформа



Константин Бажин,
генеральный
директор
ООО «КБ-информ»

Программный продукт Единая защищенная мобильная платформа (ЕЗМП) разрабатывается компанией [«КБ-Информ»](#), инновационном предприятии, организованном на базе Института математики и компьютерных наук Тюменского государственного университета.

ЕЗМП – интеграционная шина (англ. enterprise service bus, ESB) для органов государственной власти, связующее программное обеспечение с повышенными требованиями к безопасности информации. Мобильность платформы достигается за счет масштабируемости, эффективного ресурсопотребления и возможности использования в качестве клиентов любые мобильные устройства.

ЕЗМП позволяет объединить в единое инфопространство существующие информационные системы (ИС) и базы данных (БД). Это позволит:

- снизить стоимость разработки и сопровождения ИС за счет использования ранее разработанных модулей и стандартизации процессов разработки программного обеспечения (ПО), включая его тестирование;
- создать благоприятный климат для разработчиков ПО за счет возможности безопасного доступа к государственным сервисам;
- увеличить объем услуг, оказываемых в электронном виде за счет нового уровня сервиса (интерактивная связь, SMS и push-уведомления, USSD) и современных технологий мотивации (акции, бонусы, геймификация и т.п.)

ЕЗМП является продуктом импортозамещения программного обеспечения категории «Сервисная шина предприятия». Функционально ЕЗМП способна решать все задачи, возникающие перед продуктами данной категории. Наиболее известные зарубежные представители: IBM WebSphere ESB, Oracle Enterprise Service Bus, SAP NetWeaver Process Integration.

Архитектура

Схематично архитектура решений на базе ЕЗМП представлена на рисунке 1. На верхнем уровне решений, построенных на базе ЕЗМП, находятся поставщики/потребители услуг:

- веб-порталы и приложения (веб, мобильные);
- информационные системы и базы данных;
- сервисы СМЭВ (ЕСИА и др.), МФЦ;
- SMS-, USSD-, платежные шлюзы и т.п.;
- взаимодействие потребителей/поставщиков осуществляется на уровне веб-сервисов.



Рисунок 1. Архитектура решений на базе ЕЗМП

Сама же ЕЗМП состоит из четырех подсистем:

Подсистема информационной безопасности. Реализует функции межсетевого экрана и системы обнаружения вторжений на уровне веб-сервисов. Реализует дискреционную и мандатную модель разграничения доступа с уровнем детализации до метода определенного сервиса, приложения или пользователя.

Подсистема обмена данных (шина данных). Подсистема реализующая возможность обмена информацией между участниками с гарантированной доставкой сообщений. Для взаимодействия экземпляров ЕЗМП используется собственный закрытый шифрованный протокол взаимодействия. Протокол обеспечивает однозначное определение доверенного источника/получателя сообщения («свой-чужой»).

Подсистема базовых компонент. Набор функциональных блоков, реализующих базовые возможности ЕЗМП, такие, как авторизация, управление пользователями, конструктор бизнес-процессов, мониторинг и ведение логов, администрирование и т.п.

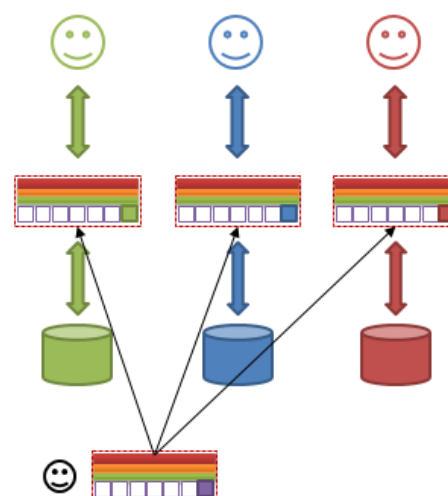


Рисунок 2. Распределение ролей между экземплярами ЕЗМП

Подсистема функциональных модулей. Подсистема функциональных блоков, реализующих необходимую логику взаимодействия различных систем/сервисов друг с другом, либо возможность подключения к ЕЗМП сторонних служб, например, SMS-рассылок или авторизации с помощью ЕСИА.

Подсистемы информационной безопасности, обмена данных и базовых компонент носят закрытый характер. Это исключает возможность внесения изменений в штатный режим работы. Подсистема функциональных модулей свободна для расширения. Функциональные модули могут создаваться как владельцем ЕЗМП, так и сторонними разработчиками.

Особенности системы и ее возможности

Архитектура ЕЗМП позволяет создать единую сеть из экземпляров ЕЗМП с различными активированными ролями и уровнем подчиненности.

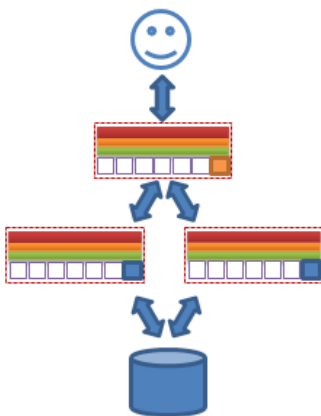


Рисунок 3. Распределение нагрузки

На рисунке 2 роль администрирования выведена на отдельный экземпляр ЕЗМП, что позволяет в единой консоли управлять другими решениями. Такая необходимость может быть обусловлена обработкой различных несовместимых категорий персональных данных.

На рисунке 3 один из экземпляров ЕЗМП используется с активированной ролью балансировщика нагрузки. Распределение нагрузки и функций между экземплярами ЕЗМП необходимо в реализации особо нагруженных систем с большим количеством запросов/ответов.

На рисунке 4 пример агрегации данных от подчиненных экземпляров ЕЗМП в родительский. Иерархия подчиненности может быть свободной, что позволяет создавать распределенные ЕЗМП-сети.

ЕЗМП позволяет использовать функциональные модули одного экземпляра другим.

ЕЗМП разработана на базе свободно распространяемых информационных технологий с от-

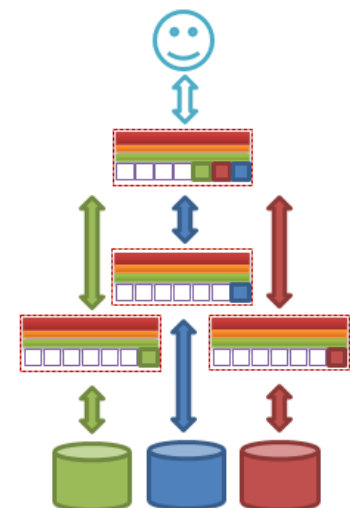


Рисунок 4. Агрегация данных

крытым исходным кодом: Java, JavaScript, СУБД PostgreSQL, Nginx, ОС Debian Linux.

Использование современных технологий обеспечивает низкие требования к вычислительным мощностям. Для запуска системы регионального масштаба достаточно серверных мощностей, сопоставимых с характеристиками ноутбука (Intel Xeon x64 или аналог, 4 Гб ОЗУ, НЖМД 100 Гб).

Отзывы пользователей



Директор департамента информационных технологий Тюменской области Александр Албычев:

«Безусловно, внедрение современных технологий значительно увеличивает доступность электронных государственных услуг. ЕЗМП позволяет подключать коммерческие медицинские учреждения к единой сети. А гражданин получает возможность в одном месте записаться на бесплатный и платный приемы к врачу».

Примеры решений на базе ЕЗМП

В Тюменской области с помощью ЕЗМП проведена интеграция разнородных систем в области здравоохранения и образования с общим количеством активных пользователей свыше 20 тысяч. Мобильное приложение «Медицина 72» получило третье место рейтинга CNews в номинации «Лучшее приложение для госсектора» и первое место в номинации «Государственные электронные услуги, предоставляемые территориальными органами федеральных органов власти и региональными органами исполнительной власти».

Отзывы пользователей



Директор центра информационных технологий Тюменской области Артур Усманов:

«ЕЗМП обеспечивает высокий уровень доступности в ходе ее промышленной эксплуатации, а служба технической поддержки прекрасно справляется с поставленными задачами».

Ханты-Мансийский автономный округ - Югра. Осуществлена пилотная разработка ИС учета малочисленных народов. Планируется интеграция с ТИС Югра.

Минприроды РФ. Разработана и проходит тестирование ИС «База данных государственного охотхозяйственного реестра». В качестве клиентского приложения для регионального уровня власти разработана ИС «Охотуправление.РФ», внедрение которой проходит в более чем десяти регионах РФ. ■

Импортозамещение ПО

Почему импортозамещение ПО следует начать с муниципалитетов



Герман Клименко,
председатель совета
Института развития
Интернета, основа-
тель и владелец
LiveInternet

Причина, по которой Институт развития Интернета (ИРИ) заинтересован в импортозамещении ПО, очевидна. Пояснить можно на примере – недавний выход Windows 10. В пользовательском соглашении Microsoft в обмен на бесплатную операционную систему требует у пользователя отдать все свои данные. Всего-то.

А следом идёт Интернет вещей, который будет знать о нашем поведении всё.

Сегодня у нас наших же данных нет, мы отдаём их другим – Google, Apple, Microsoft, а ведь после Сноудена и истории с цифровой дискриминацией Крыма совершенно ясно, что данные эти всюю используются.

Дискуссия о том, что лучше – Windows или Linux – была бы разумна, если бы не риск появления принципиально новых аргументов. Таких, которые появились в пользу НСПК, когда два российских банка отключили от иностранных платёжных систем.

В ближайшее время все страны будут озабочены персональными данными своих граждан. Между государствами построят виртуальные границы. В этом деле никто не хочет быть первым, но рано или поздно всем странам придётся это сделать.

Интернет стал настолько всемогущ, что государству приходится его регулировать. Например, раньше нельзя было ввезти товар и продать его здесь, не заплатив пошлину. А в Интернете таможня в какой-то момент прекратила существование. Но государство, которое не заботится о границах, само перестаёт существовать. Оно оказывается не в

состоянии, в данном примере, защитить своих онлайн-продавцов от нечестной конкуренции из-за рубежа.

Так получилось, что интересы государства совпадают сейчас с интересами развития национальной интернет-экономики.

Кроме того, Интернет – это программисты, прежде всего. Нельзя взять в штат 100 человек и написать «Яндекс». Нельзя написать Mail.ru штатом в 50 разработчиков. Из России в год вывозят за продажи и сопровождение импортных программных продуктов до 3 миллиардов долларов в докризисных ценах. Если бы хоть часть этих денег оставалась для наших программистов, последних было бы больше.

Только 22 тысячи муниципалитетов у нас ежегодно тратят на софт по госзакупкам 400 миллионов долларов. Общая сумма в зависимости от источника колеблется от 30 до 100 миллиардов рублей.

И надо иметь в виду, что рубль на софтверном рынке даёт ещё не менее пяти рублей в экономике страны. Купим своё ПО – эти деньги вернутся сторицей, купим за рубежом – уйдут безвозвратно.

Забота ИРИ – программисты. Пока не будет своего класса программистов, развиваться не сможем. У «Яндекса» штатная численность 4-5 тысяч человек, и этого катастрофически мало, будь все они программисты, а там далеко не все программисты. Скоро появится Интернет

**Начать импортозамещение ПО следует,
по нашему мнению, с муниципалитетов**

вещей, придётся программировать стыковку по данным между операторами связи и многочисленным «железом» – где взять людей, где найти деньги на программистов, если мы у них ничего не покупаем, а покупаем у их конкурентов за рубежом?

Начать импортозамещение ПО следует, по нашему мнению, с муниципалитетов. Там нет ничего такого, что нельзя было бы заменить переходом с Windows на Linux – работа с документами, почта, цифровая связь. Современный Linux вполне удобен и функционален, использовать СПО в муниципалитетах – реальная цель.

Дело тут не в экономии на покупке софта, а в том, что деньги за его поддержку останутся в стране.

К настоящему времени все госорганы уже должны были бы работать на Linux, [на сей счёт есть решение правительства](#). Но единствен-

ное ведомство, которое выполнило решение правительства о переходе на СПО к 2015 году, – федеральная служба судебных приставов.

Тенденция к переводу данных и ПО в облака также способствует переходу на СПО: если всё в облаке, то невелика разница, с какой ОС в него входить.

Основная проблема перехода на Linux на рабочих станциях – эмоциональная, т.к. пользователю придётся сменить привычки. Что до серверного софта, это другая история – она технологическая. Всё это посильные, решаемые задачи. Если все муниципалитеты не перейдут на Linux, бессмысленно будет ратовать за СПО в госорганах.

Тенденция к переводу данных и ПО в облака также способствует переходу на СПО: если всё в облаке, то невелика разница, с какой ОС в него входить

Да, это история не на один день. Мы не можем за год перейти на Linux. Но если создадим массовый спрос на СПО, спрос на отказ от импортного проприетарного софта там, где это возможно – успех станет делом ближайшего времени. Надо начать потреблять отечественный софт. Без государства это невозможно. ■

Безопасность

Защита мобильных подключений к СЭД региональных органов власти



Михаил Альперович,
директор лабора-
тории защищенной мо-
бильности компании
Digital Design

Современные средства коммуникации позволяют решать многие задачи, не покидая рабочего места, но необходимость командировок никуда не исчезла. Важно, чтобы отсутствие госслужащего в кабинете не приводило к остановке в его работе с документами. Иными словами, требуется обеспечить мобильный доступ к системе электронного документооборота (СЭД).

Многие СЭД располагают мобильными клиентами, которые могут быть реализованы как «тонкий» клиент или мобильное приложение. «Тонкий» клиент - это, как правило веб-приложение, то есть на мобильном устройстве пользователь работает с ним через веб-браузер. Плюс такого решения в меньшей трудоемкости разработки. А минус - в отсутствии возможности работы офлайн. Мобиль-

ное приложение лишено этого недостатка и, кроме того, оно эргономичнее браузера.

Требования безопасности

При мобильном доступе к СЭД информация покидает периметр, выходит из вычислительной сети организации и может быть перехвачена. Кроме того, появляется внешняя точка доступа в периметр, что может быть использовано для атаки на внутреннюю сеть.

Для защиты информации в системах, используемых в органах государственной власти, должны применяться российские средства шифрования - сертифицированные СКЗИ (средства криптографической защиты информации), часто также называемые «средства шифрования

по ГОСТ». Рассмотрим подходы к решению указанных задач по защите информации с использованием сертифицированных СКЗИ.

Защита периметра сети

Для защиты периметра сети лучше всего подходит эшелонированная защита, которую можно построить путем размещения шлюзов доступа мобильных устройств в демилитаризованных сегментах сети (ДМЗ). Эти сегменты отделены от Интернета и внутренней сети передачи данных межсетевыми экранами, а шлюзы поддерживают аутентификацию каждого подключения по цифровому сертификату. Таким образом, анонимный трафик не будет допущен во внутреннюю сеть, что радикально затрудняет внешнюю атаку. В качестве дополнительного средства защиты можно организовать такой режим, когда канал между шлюзом в ДМЗ и сервером СЭД внутри корпоративной сети будет однонаправленным и обеспечит передачу данных только по запросам сервера СЭД. Иными словами, порт будет открыт изнутри сети наружу, но не наоборот. Это в принципе исключает атаку извне.

При описанном сценарии работы внутренний сервер устанавливает персистентное (непрерывное) соединение с ДМЗ и поддерживает его для получения данных от мобильных устройств. Такой подход не требует открытия входящих портов на межсетевых экранах, что минимизирует риски сетевой безопасности.

Защита данных, передаваемых по сети

Данные, передаваемые по сети, защищаются за счет использования одного из протоколов – SSL/TLS или IPSec. Эти протоколы шифруют данные, передаваемые по сети.

Сегодня в России есть ряд сертифицированных средств организации защищенного SSL/TLS-подключения, например от компаний StoneSoft, Checkpoint, Trusted TLS. Также доступны VPN-решения, поддерживающие более низкоруровневые протоколы, такие как IPSec или собственные проприетарные протоколы – примером может служить система ViPNet от российской компании «Инфотекс».

Все упомянутые решения используют сертифицированные СКЗИ.

Защита данных на мобильном устройстве

Защита локальных данных на мобильном устройстве обеспечивается путем организации «в песочнице» приложения зашифрованной об-

ласти, где хранится конфиденциальная информация. Даже если устройство окажется в руках злоумышленника и данные, размещенные на устройстве, будут похищены, прочитать их не удастся.

Особенности поддержки сертифицированных СКЗИ на мобильных устройствах

Особенностью использования сертифицированных СКЗИ на популярных мобильных платформах iOS и Android является то, что (в отличие, например, от ОС Windows) эти средства нельзя встроить на системный уровень ОС – так, чтобы ими могли пользоваться все приложения. В Windows есть возможность установить в систему CSP – Cryptographic Service Provider; в iOS и Android приходится встраивать CSP в каждое приложение. (Из этого правила есть отдельные исключения, мы рассмотрим их ниже). В данном материале рассмотрена реализация применения сертифицированных СКЗИ на примере продукта КриптоПРО CSP от компании «КРИПТО-ПРО».

Доступ к зашифрованным областям памяти мобильного приложения, а также организация защищенного канала связи осуществляются с использованием ключа пользователя, размещенного в криптографическом контейнере. Ключевые контейнеры защищены паролем (пин-кодом). Данный подход также используется для аутентификации пользователей в приложении – если устройство попадет в руки постороннему человеку, он не сможет войти в приложение без пин-кода. Поскольку аутентификация пользователей в приложении организована с помощью цифрового сертификата, необходимо также контролировать статус сертификата (он должен быть актуален), периодически обращаясь к соответствующему ресурсу – точке распространения списков отзывать сертификатов или службе актуальных статусов сертификатов.

Сертификат может быть отозван по разным причинам (увольнение сотрудника, компрометация ключа, завершение срока действия), что в соответствии с правилами использования сертификатов и ключей делает невозможным их дальнейшее использование.

Расшифровка информации из зашифрованной области должна производиться на короткий промежуток времени и только по запросу пользователя, а по завершении работы расшифрованные данные должны быть удалены из памяти. Также следует применять технологии очистки памяти, при которой области памяти не просто очищаются, но и многократно перезаписываются случайными данными, чтобы избежать возможности восстановления блоков расшифрованной информации.

В качестве дополнительной меры усиления безопасности используются отчуждаемые носители для хранения ключевой информации. В случае iOS могут применяться считыватели смарт-карт, подключаемые физически через разъем или через Bluetooth-соединение. Кроме этого применяются носители (токены), имеющие встроенный Bluetooth-модуль – в этом случае не требуется применять дополнительные считыватели. Примерами таких решений могут служить продукты компаний «Аладдин Р.Д.» (смарт-карта и ридер для мобильных устройств) и компании «Актив» - «Рутокен ЭЦП Bluetooth». Такие решения обеспечивают поддержку многофакторной аутентификации - для доступа к информации одновременно необходимы само устройство (с установленным ПО), токен и пин-код.

Поскольку теоретически устройство может быть подвержено воздействию вредоносного кода, необходимо контролировать целостность исполняемых модулей. Для этого путем сравнения контрольных сумм проверяется целостность кода приложения, модулей защиты информации и среды исполнения (операционной системы). Если контрольные суммы не совпадают с эталонными, программа должна прекратить работу и уничтожить всю критически важную информацию, включая криптографические ключи.

Можно ли обойтись без встраивания криптографии?

Встраивание сертифицированных СКЗИ в приложения – достаточно трудоемкая задача. Если защита данных на устройстве обеспечивается организационными мерами, то защиту канала можно обеспечить, применяя имеющиеся на рынке средства построения VPN-подключений с шифрованием данных по ГОСТ.

На сегодня на рынке доступны два таких средства:

[ViPNet Client](#)

[Защищенный Туннель](#)

Оба они создают защищенный канал, в котором информация шифруется по ГОСТ. Благодаря этому мобильный клиент работает в привычном для него режиме, то есть в его программном обеспечении ничего менять не требуется. Могут только потребоваться изменения в настройках подключения.

Оба решения поддерживают операционные системы iOS и Android, то есть покрывают большую часть парка мобильных устройств, приме-

няющихся сегодня в коммерческих и государственных организациях. Отметим, что VipNet также подходит для реализации защищенных подключений с ноутбуков под управлением ОС Windows (но для этой платформы выбор решений гораздо шире).

Типовая схема работы мобильного клиента СЭД через защищенное подключение показана на рисунке:

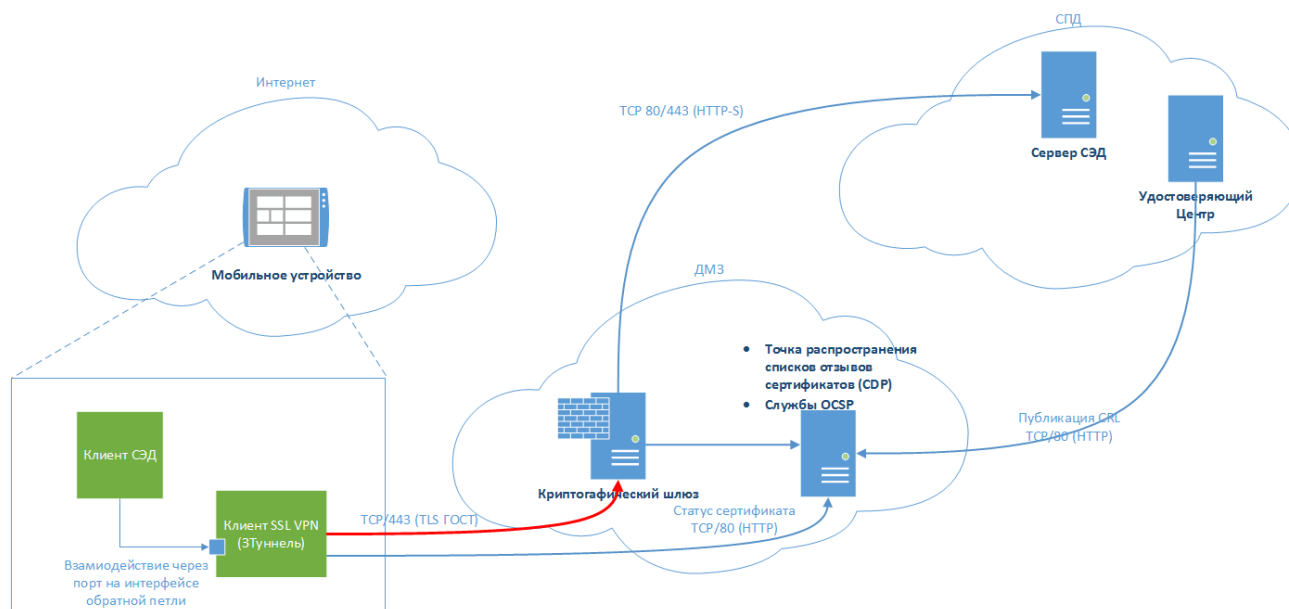


Схема подключения мобильного клиента в СЭД

Выводы

Необходимость обеспечения конфиденциальности служебных данных – не препятствие для использования госслужащими мобильных устройств при удалённой работе. На рынке есть российские программные продукты, способные надёжно защитить данные и (или) канал их передачи за периметр локальной компьютерной сети организации. В сочетании с достаточной квалификацией пользователя – он должен понимать общую схему и принципы защиты служебной информации на мобильном устройстве – эти программные продукты с приемлемой надёжностью, т.е. гарантированно, обеспечат безопасную работу госслужащего вне стационарного рабочего места. ■

Безопасность

Информационная безопасность российских компаний: состояние дел в 2015 году



Сергей Ожегов,
коммерческий дирек-
тор Searchinform

Результаты опроса, проведенного аналитическим центром SearchInform (отечественная компания, специализация – средства контроля доступа к корпоративной информации. – ред.) в рамках весеннего RoadShow компании, прошедшего в 27 городах России (более 1500 респондентов – специалисты и начальники отделов ИБ, собственники бизнеса, руководители), показывают серьезное ухудшение информационной безопасности (ИБ) российских компаний и государственных учреждений.

Каналы утечек и отстающие от них средства контроля

По традиции чаще всего для «слива» информации инсайдеры используют электронную почту. Именно ее ИБ-специалисты контролируют в первую очередь (контролируется в 36% организаций). Далее следуют внешние носители (18%), документы, отправленные на печать (15%) и интернет-мессенджеры (15%).

В 53% компаний есть запреты на использование сотрудниками отдельных программных продуктов и онлайн-сервисов (например, Skype и социальных сетей). Запреты вводятся, впрочем, не только для предотвращения утечек, но чаще для того, чтобы люди не тратили рабочее время на развлечения и общение с друзьями. Однако оставлять такие каналы без контроля как минимум неразумно. Очень многие сервисы, например, Dropbox, Google Drive и т.п. представляют серьезную угрозу, особенно для государственных организаций – в первую очередь из-за того, что контролируются зарубежными компаниями, а загружаемые

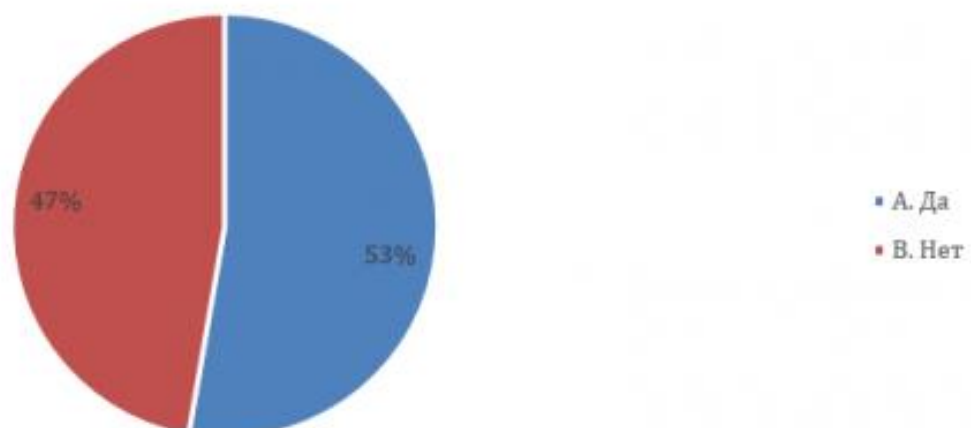
данные физически размещаются на серверах не на территории России. По сути, любая информация, загруженная на такой сервис, может быть просмотрена спецслужбами иностранных государств. Кроме того, сотрудники могут использовать облачные сервисы для копирования служебной информации, например, для «подстраховки» в случае увольнения.

Какие каналы передачи данных контролируются в вашей организации для предотвращения утечек информации?



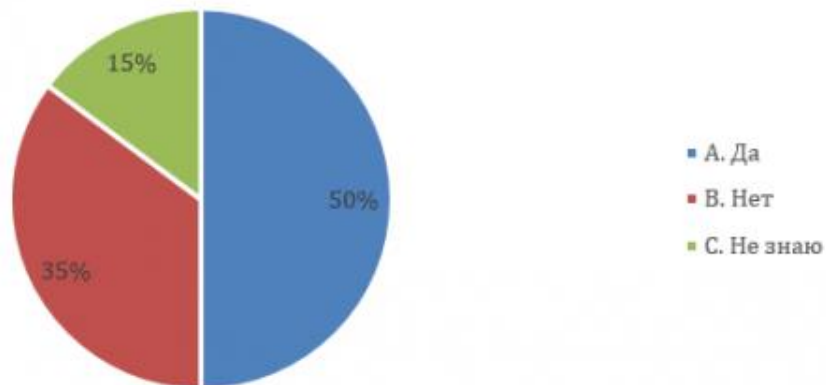
Несмотря на наличие соглашений о неразглашении и других административных мер контроля, 50% компаний, тем не менее, сталкивались с утечкой корпоративных данных. Представители более половины организаций сталкивались с ситуацией, когда уволившиеся сотрудники пытались унести с собой не только личные вещи и трудовую

Существуют ли в вашей компании запреты на использование определенных информационных ресурсов (соцсетей, ICQ, Skype и т.д.) в связи с рисками ИБ?



книжку, но и конфиденциальную информацию компании. В 2013-м году, в значительно более благоприятных экономических условиях, с таким поведением персонала столкнулись лишь 28% компаний, что свидетельствует о значительном росте агрессивности среды, в которой сегодня работает бизнес.

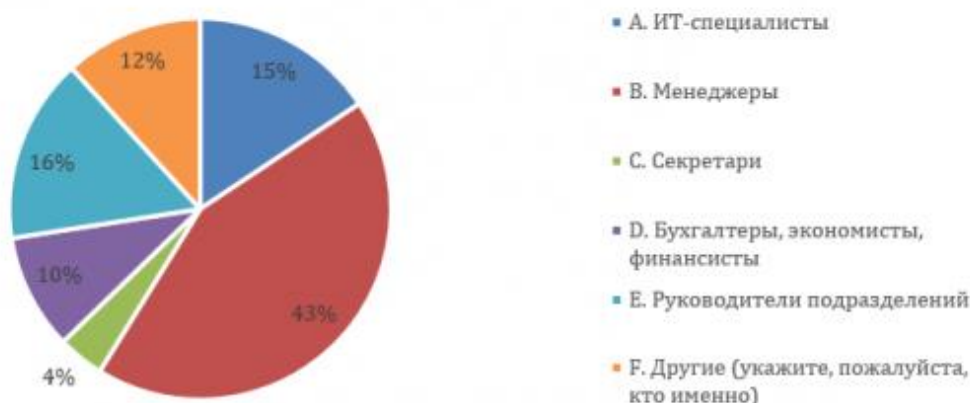
Случались ли в вашей организации утечки конфиденциальных данных?



Как показал опрос, чаще всего политику корпоративной информационной безопасности нарушают менеджеры (43%). Значительно меньше, но, тем не менее часто на такое идут руководители подразделений (16%). Реже всего ИБ нарушают секретари (4%). Общая закономерность: утечки данных чаще всего происходят «благодаря» тем, кто так или иначе связан с деньгами.

Двумя годами ранее менеджеры и руководители среднего звена суммарно «генерировали» лишь около 33% утечек данных.

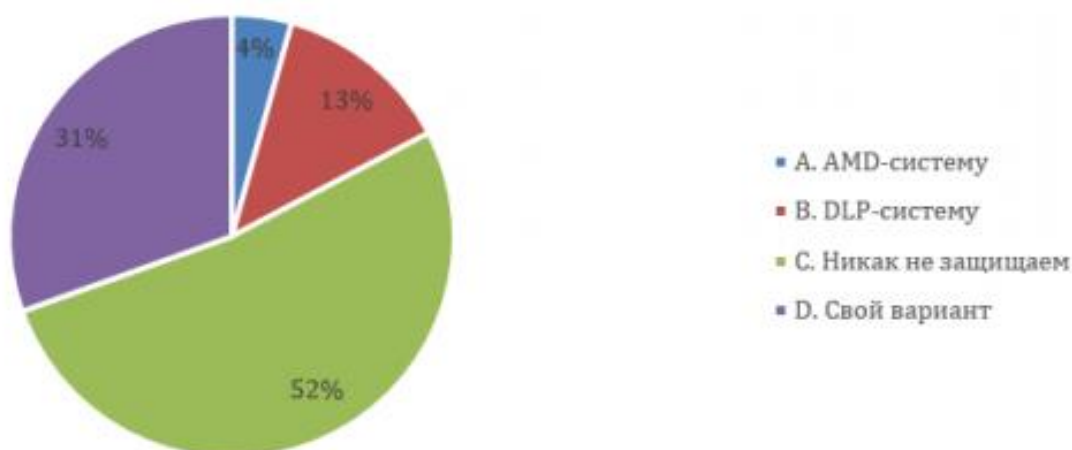
Кто из сотрудников в вашей организации был уличен в нарушении корпоративных политик информационной безопасности?



Как выясняется, 70% сотрудников используют личные устройства для работы – это ещё один канал утечки, который в 52% организаций никак не контролируется.

Практически все современные смартфоны поставляются с некоторыми предустановленными программами. Неопытные в вопросах информационной безопасности пользователи могут забыть или вовсе не знать о том, какие функции тех или иных приложений активны на их телефонах (синхронизация календаря, заметок, контактов, данных о местоположении, автоматическая загрузка фотографий в облако и т.п.). Телефоны государственных служащих представляют особый интерес для зарубежных спецслужб и могут подвергаться целенаправленным атакам – после разоблачений Сноудена это должно быть ясно тем, кто прежде в такое не верил.

Осуществляется ли контроль за такими устройствами.
Если ДА, то какие решения вы используете для защиты
от утечек информации?



Электронная почта как источник повышенной опасности

Точной статистики о взломах корпоративных почтовых ящиков и почты госслужащих нет, но мы не сомневаемся, что в России счёт идёт на миллионы. Достаточно вспомнить [громкие утечки паролей от почтовых сервисов «Яндекса», Google, Mail.ru и др. осенью 2014 года](#).

Ящики на бесплатных почтовых сервисах во множестве взламывают, если можно так выразиться, «прямо» и «перекрёстно».

Прямой взлом – [с помощью фишинговых писем и вирусов](#). Примерная схема: потенциальной жертве посылается фишинговое письмо,

содержащее ссылку на или непосредственно заражённое вложение. После заражения вирус собирает и отправляет взломщику все пароли, которые вводит пользователь.

При перекрёстном взломе делается ставка на то, что пользователь использует [один и тот же пароль на различных ресурсах](#). Примерная схема: хакер скомпрометировал ресурс, «слил» базу пользователей с паролями. При регистрации пользователи обычно указывают электронный ящик. Многие используют один и тот же пароль «для всего». Поэтому велика вероятность, что пароль от взломанного ресурса подойдёт и к почте.

Средства профилактики известны: использование SSL, двухфакторная аутентификации и т.п. Всё это можно объединить под общим названием «Система контроля доступа» (Access Policy Management – APM).

Пример возможностей одного из решений: при подключении пользователя к сети или приложению имеется возможность осуществления дополнительного контроля доступа за счет реализации endpoint-политик и проверки пользовательских устройств на соответствие политикам безопасности компании (версия ОС, наличие антивируса, актуальность антивирусных баз, членство в домене, содержимое реестра и т. д.). В зависимости от результатов проверки система может назначать динамические списки доступа для обеспечения должного уровня безопасности. Поддерживается функционал создания защищенного рабочего пространства — иными словами, пользователь не может сохранять файлы за пределами этого пространства, а созданные локально временные файлы и папки удаляются при завершении сессии.

Обеспечение ИБ государственных IT-ресурсов: что на практике

Среди мер обеспечения ИБ в госучреждениях в абсолютных лидерах практика запретов – чиновникам не разрешают пользоваться теми или иными сервисами, и не только почтовыми. К примеру, в Белоруссии существует так называемый «чёрный список» сайтов, куда может попасть практически любая веб-страница, нарушающая «Положение о порядке ограничения доступа к информационным ресурсам (их составным частям), размещенным в глобальной компьютерной сети Интернет».

В России с 1 июля 2015 года законом установлена обязанность для государственных органов и органов местного самоуправления, подве-

домственных организаций и учреждений размещать технические средства используемых ими [информационных систем исключительно на территории России](#), что делает невозможным использование в госучреждениях внешних онлайн-сервисов, даже некоторых отечественных.

Запретами на основании законов дело не ограничивается, есть ещё отраслевые стандарты и другие нормативные акты на всех уровнях госуправления.

Статистики использования внешних онлайн-сервисов (таких, как почтовые сервисы, облачные хранилища и социальные сети) в российских госучреждениях и компаниях у нас нет, но есть основания считать, что она распространена весьма широко. Год назад 80% государственных организаций в России пользовались внешними почтовыми сервисами, в том числе зарубежными.

Головоотяпство или воровство – IT-специалисту не понять

Примеров утечек данных из госучреждений, к сожалению, очень много – о чём свидетельствует и наш опыт, и результаты других исследований – [согласно которым в 2014 году число инцидентов в России выросло на 73%](#). И это только то, о чём стало известно.

Пренебрежение правилами ИБ может быть следствием неудобства внутренних сервисов. Беда наступает в момент, когда сотрудники осознают, что корпоративная система не позволяет быстро обмениваться сообщениями: письма уходят, но появляются не моментально в ящиках. Поэтому для обмена служебными сообщениями часто используется Gmail или Mail.ru (основные утечки информации, включая бюджет компании и другие ценные документы, происходили именно с Mail.ru). Зачастую нельзя понять: это головоотяпство человека, который через мейл отправляет такие конфиденциальные документы, или злонамеренное похищение данных под видом утечки.

Приведём некоторые громкие примеры.

[Нарушение банковской тайны в Амурской области.](#)

[Сливы информации похоронным конторам из полиции. «Скорая помощь», кстати, тоже часто на этом попадается.](#)

[Сливы персональных данных на башкирской таможне.](#)

[Использование Хиллари Клинтон почтовых сервисов, недопустимых для госслужащего](#)

Случайно разосланные письма о времени визита Обамы в Кению.

Тот факт, что не только российские госслужащие подвергают себя риску, используя недопустимые сервисы, не может служить даже слабым утешением.

Главная опасность использования сторонних сервисов – утечка служебной информации:

- всё, что человек загрузил в свой аккаунт, остаётся там навсегда;
- если вы удалили информацию, это ещё не значит, что сервис удалил ее безвозвратно;
- если аккаунт взломают – информацию могут выложить в открытый доступ;
- если человека уволят или он сам захочет уйти, загруженная информация останется с ним, т.к. это его личный аккаунт;
- кто владеет сервисом, тот может иметь доступ к вашей информации. А сервисами владеют зарубежные компании;
- если человек использует один и тот же пароль для различных сервисов, при взломе одного пароля, что само по себе может быть некритично, под угрозу попадают все остальные.

Статистика инцидентов

Полной информации по России нет и не будет, пока компании и учреждения законодательно не обяжут информировать надзорные органы об утечках. Абсолютно все компании предпочитают у нас замалчивать инциденты.

Но самое интересное, что даже за рубежом, где эти законы есть, ситуация не идеальна.

Например, 20% участников американского исследования признали, что компания, в которой они работают, в последнее время пострадала от утечки данных, однако скрывает этот факт. Более того, 9% респондентов заявили, что именно сокрытие происшествия является лучшим способом реагирования на кибератаки.



Справочно: некоторые нормативные документы, регламентирующие работу с конфиденциальной информацией

1. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» (в ред. от 08.11.2011 № 309-ФЗ)
2. Постановление Правительства РФ от 15.04.1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» (в ред. Постановления Правительства РФ от 03.11.2011 № 898)
3. Сто бр иббс-1.0-2014 обеспечение информационной безопасности организаций банковской системы российской федерации
4. Федеральный закон Российской Федерации от 29.07.2004 г. N 98-ФЗ «О коммерческой тайне»
5. Федеральный закон Российской Федерации от 27.07.2006 г. N 152-ФЗ «О персональных данных»
6. Приказ ФСТЭК России от 11.02.2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
7. Приказ ФСТЭК России от 18.02.2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Главная угроза – человек

Согласно исследованиям SearchInform, сегодня более 55% сотрудников в России, странах СНГ и Прибалтике готовы передать важную для компании конфиденциальную информацию конкурентам, журналистам или контролирующим органам. При этом почти 20% из них делают это безвозмездно.

Такое положение дел тем более опасно, если принимать во внимание тот факт, что доля сотрудников, решившихся на «слив» данных, растёт, если у них есть уверенность в собственной безнаказанности.

Вот ещё результаты исследования: 35% сотрудников готовы продать на сторону корпоративную информацию, если сойдутся в цене с покупателями. При этом 22% «предателей» могут отдать необходимую информацию сравнительно задешево — за 155 тысяч долларов. Но не все так низко себя ценят: 55% сотрудников назначили бы цену на уровне 1500 долларов, а 70% оценили бы инсайд в 7–8 тысяч долларов. Подавляющее большинство потенциальных инсайдеров (81%) не согласились бы на сумму меньше 15,5 тысяч долларов (эквивалент стоимости новой машины). 19% опрошенных оценивают доступные им данные более чем в 75 тысяч долларов (группы респондентов перекрываются).

Также стоит добавить, что согласно опросу, проведённому аналитическим центром компании SearchInform 27 мая в Москве, в первой половине 2015 года в каждой четвертой компании сотрудники начали активно посещать специализированные сайты в поисках новой работы; всего 35% опрошенных ответили, что ничего не изменилось, но при этом в 15% организаций возросла напряженность внутри коллектива и снизилось качество работы сотрудников. ■

О журнале

Электронный журнал «Региональная и муниципальная информатизация» издается ежеквартально

Издатель: [Экспертный центр электронного государства](http://d-russia.ru) (d-russia.ru)

Главный редактор: Павел Хилов

Адрес редакции: rmi@d-russia.ru

Телефон редакции: 915 366 08 49

Приглашаем авторов – представителей органов власти субъектов Российской Федерации, муниципалитетов, компаний-разработчиков, экспертного сообщества. Нам интересны статьи, рассказывающие о положительном и отрицательном опыте решения проблем и задач, с которыми вы сталкиваетесь в своей работе, начиная от управленческих и нормативных и заканчивая техническими и технологическими. Статьи и предложения по темам, которые на ваш взгляд, актуальны и требуют освещения и экспертной проработки, а также предложения по информационному сотрудничеству присылайте на адрес редакции rmi@d-russia.ru.

Первый номер журнала



Второй номер журнала



Об Экспертном центре электронного государства

Экспертный центр обеспечивает работу открытой площадки для обсуждения и подготовки предложений и рекомендаций по реализации государственной политики по различным аспектам использования информационных технологий в органах власти всех уровней.

Сайт Экспертного центра электронного государства d-russia.ru (DigitalRussia) – единственное в стране информационно-аналитическое издание, полностью посвященное вопросам и проблемам государственной информатизации.

Решением VII Международного IT-Форума, прошедшего в Ханты-Мансийске в июле 2015 года, Экспертному центру электронного государства рекомендовано создание на его основе центра компетенции по координации процессов импортозамещения в сфере IT в федеральных и региональных органах власти и органах местного самоуправления Российской Федерации.

Экспертный центр взаимодействует с Администрацией Президента РФ, Аппаратом Правительства РФ, Министерством связи и массовых коммуникаций Российской Федерации, Министерством экономического развития Российской Федерации, органами власти субъектов Российской Федерации и др. Налажены устойчивые деловые контакты с научными институтами, общественными объединениями и организациями, работающими в сфере информационных технологий.

Сегодня Экспертный центр объединяет более 100 экспертов по ключевым направлениям развития информационно-коммуникационных технологий.

Деятельность Экспертного центра направлена на консолидацию экспертного сообщества в сфере информационных технологий, развитие технологий электронного государства на всех уровнях власти, а также обеспечение независимого общественного контроля за данным процессом. ■