Автор: Артур Скальский © ПОЛИТ.РУ ИНТЕРНЕТ И ИТ, РОССИЯ 3215 18.04.2013, 01:04 337

Интернет-независимость РФ

В последнее время много говорится об угрозах национальной безопасности. Заражение компьютерных сетей дипломатических представительств, атаки хакеров, подозрительно напоминающие действия спецслужб, — все это реалии нашего мира.

Развитие криминальных технологий проникновения перевело стрелки с вопроса «взломают ли меня?» на «когда меня взломают, и как минимизировать ущерб?»

В течение последних лет правительство неоднократно декларировало задачи по защите локального сегмента сети Интернет. Наибольшую известность получили попытки добиться внедрения регулирования на уровне стран и создания системы защиты от сетевых атак. Да, эти попытки не достигли результата. Да, они во многом справедливо критиковались. Но будем честными — наступление часа X, когда против страны в целом может быть развернута та или иная акция, вполне вероятно. Несмотря на мир между всеми крупными государствами, ни одно из них не собирается полностью отказываться от вооруженных сил.

Вооруженные силы сейчас немыслимы без современных средств связи и управления. Средства связи объединяют чиновников, разработчиков средств вооружения и т. д. Стране есть что защищать и есть от кого защищаться. Попробуем оставить в стороне политический вопрос «зачем» и поговорим о том, как в принципе можно защититься в современном цифровом мире.

Начнем с того, что на самом деле руководство нашего государства осознает необходимость перемен. В стране есть деньги, постоянно объявляется о создании новых проектов и развитии ранее объявлявшихся, только в Москве действует порядка десяти бизнес-инкубаторов (не считая Сколково). Почему же не видно результатов?

Ошибка в системе

Допустим, одна девушка может стать мамой за 9 месяцев, но девять девушек за один месяц мамами не станут. Как правило, все громогласно объявленные проекты развиваются по схожему сценарию: объявление проекта — тендер — выкатка победителем тендера некого сайта или сервиса — возмущенное удивление общественности по типу «где они такого криворукого студента нашли» и «сколько же они попилили». Наверху же отнюдь не дураки сидят, чтобы постоянно наступать на одни и те же грабли! Почему же все повторяется раз за разом?

Если разобраться, то получится, что в низком качестве сервисов и сайтов победители тендеров не виноваты. Если кто-то хочет получить новую операционную систему, то под заказ нужно составить спецификацию, описывающую весь функционал до мельчайших подробностей, все варианты действий пользователей, вид всех возможных окошек, протоколы взаимодействия всех компонентов и т. д. и т. п. Попробуйте представить объем необходимой работы и время на подготовку одной только документации. Ведь это многие тома и даже, возможно, шкафы талмудов! Кто-то видел примеры такого количества документов в качестве приложений к тендерам? Соответственно, победитель в ответ на слово «хочу» выкатывает минимум возможного. Зачем реализовывать лишнее, если его никто об этом не просил? А денег за работу, естественно, просят по-максимуму. Бизнес есть бизнес! Времена, когда работали за идею, остались в прошлом.

Правда, нужно сказать, что есть модель разработки, учитывающая вариант отсутствия техзадания. В этом случае пишется минимальное ядро системы, показывается заказчику, заказчик думает, что еще ему хочется добавить, замечания согласовываются, выпускается следующая итерация и так продолжается, пока у заказчика не остается пожеланий или не кончается бюджет. Но тут к ранее озвученной добавляются еще две проблемы.

А судьи кто?

Лучше всего иллюстрирует проблему одна история. В ноябре 2008 года было закрыто 184 военных представительства на предприятиях ОПК. В марте 2009 директивой Генерального штаба № 314/9/1000 вдвое

сокращено число офицерских должностей там, где военпреды уцелели. В военных представительствах 1-й и 2-й категорий директива оставляла лишь по два офицера, в военных представительствах 3-й категории — по одному с одновременным уменьшением численности гражданского персонала военной приёмки. Также в 2009 году штатные категории военпредов сокращены до категорий «старший лейтенант» и «капитан». В апреле 2011 года вышла директива Генштаба № 314/9/1547. Она предписывала еще сильнее «поджать» штаты — в два и более раз!

Это в Министерстве обороны. В гражданских организациях есть еще одна проблема — зарплата. Все заказчики, как правило, располагаются в Москве, а предлагаемая зарплата порядка 10 тыс. рублей работающих в Москве не прельщает.

В итоге просто некому ни составлять ТЗ, ни принимать выполненные работы с достаточным уровнем качества. А если качество не спрашивают, то зачем его обеспечивать?

Сроки

Как правило, после того, как озвучивается очередная инициатива, заказчик хочет мгновенно получить желаемое. Но если мы хотим получить, скажем, операционную систему, то ее нужно разработать. Как бы мы ни относились, например, к Windows, но на ее создание ушли годы. Поэтому, если заказчик хочет получить что-то уже вчера, то ему можно предложить только уже готовое. Естественно, не подогнанное под его реальные потребности и нужды. Скажем, нужна операционная система. Не вопрос — предлагаются клоны имеющихся ОС Linux. Заказчик их даже внедряет. И напарывается еще на две проблемы.

Совместимость

Полученная типовая реализация может не учитывать типовые потребности. Скажем, имеющийся в Linux OpenOffice вполне подходит для работы, но если вам нужно обмениваться документами с теми, у кого установлен, скажем, Microsoft Office, могут возникнуть проблемы. Документы, созданные в одном «офисе», могут не открыться или неправильно отобразиться в ином. Типичный пример — доработка 1С под требования покупателей.

Поддержка

Тут, в свою очередь, тоже две проблемы. Типовое решение может поставляться не его разработчиком. Скажем, в ОС Linux — тысячи программ, и далеко не все из них разработаны поставщиком. Да, исходный код доступен. И разобраться в чужом коде тоже можно. Но как же это бывает сложно, и сколько на это нужно времени!

Предположим, заказчик-таки удовлетворен, внедрил систему и использует ее. Проходят годы. Систему нужно обновить (причин может быть много — найдена уязвимость, проведена доработка в связанных компонентах и т. д.). А поставщика уже нет. Или исходные коды потеряны. Или ушел ведущий разработчик, создававший систему. Желающие могут погуглить на тему ошибки тысячелетия и зарплат специалистов по Коболу на тот период. То есть мало систему разработать — ее нужно поддерживать все время ее работы у заказчика.

Именно поэтому в Советском Союзе и разработкой ТЗ, и поддержкой занимались специальные институты.

Подведем итоги вышесказанного. Если государство хочет получить комплекс ПО, предназначенного для обеспечения независимости и безопасности, то сиюминутным желанием тут не обойтись. Нужно воссоздавать институт заказчика, поднимать зарплаты, учиться действовать в соответствии с процедурами и выстраивать долговременные взаимоотношения. Нужна стратегия развития и дорожный план на годы вперед. С четкими задачами и ответственными лицами за каждый этап. А сделать можно все. Вопрос в цене.

***

Предположим, мы создали систему формирования заказа, определили стратегию развития программного обеспечения на пятилетку вперед. Никакой иронии — желающие могут посмотреть, сколько ушло времени на разработку последней стабильной версии Windows. О загадочном продукте под названием Longhorn стало известно в мае 2001 года — почти за полгода до релиза Windows XP. Первый показ Longhorn прошел в конце октября 2003 года, 30 ноября 2006 года состоялся релиз Windows Vista, но в связи с многочисленными претензиями можно считать, что стабильности система достигла только в Windows 7, поступившей в продажу 22 октября 2009 года. Не менее 8 лет разработки, 5 миллионов человек, участвовавших в тестировании бета-версий. Впечатляет? Если мы хотим получить нечто подобное — задумаемся о сроках и бюджете. Но начать

нужно с основы.

Бытие определяет сознание

Программы не работают просто так. Нужна аппаратная часть. Процессоры, материнские платы, микросхемы, винчестеры, модули памяти, оптические приводы, флешки, мониторы… И это только для рабочих станций! А еще принтеры и факсы, сетевое оборудование… В составе Windows Vista поставлялось 1,5 миллиона драйверов, и то это не позволило охватить все возможные используемые устройства. Если о российских процессорах мы знаем — и даже был анонс о начале выпуска компьютеров на их основе, то все остальное поставляется в большинстве своем из стран Азии. Сейчас у нас отношения с Китаем и прочими странами-поставщиками нормальные. Но мы-то рассчитываем на десяток лет вперед и более! Можем ли мы гарантировать, что через 15–20 лет отношения будут столь же теплыми? А в софт уже будут вложены весьма и весьма значительные суммы.

Если для большинства использующих ГЛОНАСС место производства этих устройств не имеет значения, то, скажем, для вооруженных сил это критично. Даже если не предполагать возможность аппаратных закладок — любая страна может в любой момент запретить экспорт конкретного товара. Думаете, это фантазия? Вспоминаем недавний скандал, когда группа американских бизнесменов российского происхождения была объявлена в США шпионами. А они всего лишь экспортировали в Россию ряд микросхем, запрещенных к вывозу. Мы традиционно гордимся нашими космическими успехами, но уже сейчас наши радары и средства связи работают на запрещенных к вывозу американских микросхемах. Что будет, если Америка будет более тщательно контролировать экспорт?

Естественно, это не повод переводить всех пользователей на компьютеры и оборудование собственного производства. Большинство компаний и тем более домашние пользователи не обрабатывают критически важную информацию и не имеют доступа к сервисам, от которых зависят судьбы страны и мира (злоумышленникам зачастую интересна не только информация на взломанном компьютере — гораздо важнее может быть доступ к почте, внутренним базам данных, системе управления и т. д. — всему тому, к чему пользователь обычно получает доступ благодаря сохраненным на компьютере паролям). Но даже если считать только вооруженные силы, чиновников и локальные сети критически важных объектов (атомные станции, ГЭС и т. д.) — это все равно очень и очень много.

Что делать, чтобы исправить ситуацию?

Как минимум — избавиться от системы тендеров. По закону в тендере должен победить предложивший более низкую цену. Но будем честными: мы никогда не сможем сделать так же дешево, как в Китае. У нас и зарплаты, и издержки куда выше. Нужно ориентироваться на более высокие цены. А качество? — спросите вы. Качество обеспечивается наличием нормальной приемки, что возвращает нас к вопросу о воссоздании системы контроля качества — институте заказчика, ведущего проекты от инициации до приемки и далее, весь жизненный цикл.

Нельзя просто заказать новую систему. Нужно провести исследовательскую работу — НИРы, чтобы определить возможные варианты будущего, оценить их реализуемость и только после этого начинать работу с поставщиками и разработчиками. Перекладывать этап НИРов на разработчика — в корне неправильно. Поставщикам невыгодно вкладываться в НИРы: большая часть их них — это списанные деньги, кто из НИРов «выстрелит», предсказать нельзя. Именно поэтому гораздо выгоднее все время предлагать немного улучшенное старое — альтернативы ведь у заказчика нет. Поставщиков обычно — не более одного. Невыгодно и улучшать качество. Ведь это траты на улучшение технологий и их контроль, на обучение сотрудников и повышение их жизненного уровня. Зачем тратить больше? У нас капитализм.

Много говорилось о том, что у нас низкое качество оружия, так как мало заказывают. Стали заказывать много. Качество улучшилось? Онищенко борется за качество грузинских и молдавских вин, украинского сыра. А как вам качество нашего молока? Заказчик (мы с вами) покупает то, что имеется, так зачем выпускать более качественную продукцию?

Система контроля развалена, и поднять ее очень и очень трудно даже при наличии политической воли и осознанной необходимости.

Вернемся к программному обеспечению.

Что нужно для безопасной работы?

Если кратко, то три вещи: чтобы ПО делало все, что требуется по должностной инструкции, чтобы не сломалось или не могло быть сломано в час X (отсутствие закладок), чтобы обеспечивало защищенную заботу (отсутствие утечек). Первую часть должна обеспечивать уже упоминавшаяся приемка, вторую — система сертификации. А вот с третьей интереснее. Большинство из нас работает, как правило, в офисных приложениях, использует для общения социальные сети, для поиска информации - поисковую систему, расплачивается пластиковыми картами онлайн. Все это ПО работает на операционной системе. Взаимодействие осуществляется через Интернет. Не будем рассматривать иные варианты (их много, но подход будет аналогичным), остановимся на всем знакомом процессе обработки персональных данных. Что нужно сделать, что бы эти данные не попали куда не надо?

Казалось бы, ответ очевиден: сертифицированная операционная система и сертифицированные офисные приложения плюс защищенный канал обмена данных при передаче их между компьютерами. Сертификация подтверждает отсутствие неописанного функционала и известных уязвимостей, настройки операционной системы позволяют ограничить возможности по проникновению — хакер не пойдет! Но возможен и иной подход.

Все уязвимости никогда не могут быть известны. Постоянно выходят обновления для продуктов Microsoft, Adobe… Сертифицированная система может обновляться, но обновления тоже должны проходить процедуру сертификации — мало ли что в них можно засунуть! Поэтому хакер имеет фору по времени. Соответственно, можно использовать несертифицированные офисные приложения и операционную систему, а защиту обеспечить с помощью сертифицированных средств, например файервола, антивируса и системы ограничения доступа. Называется все это — оценка рисков и составление модели угроз. Какое отношение имеет пример к статье? Самое непосредственное.

Правительство объявляло проекты создания национальной операционной системы. Дело благое, но, как было показано ваше, — предельно сложное, долгое и дорогое. При этом нет никакой гарантии, что в приемлемые сроки удастся создать полный аналог всего ПО, которое предлагают нам Microsoft или Apple — ведь если будет не полный аналог, придется переучивать всех пользователей (вплоть до президента) и администраторов. А это еще более трудная задача, чем разработать свое ПО.

Но при правильно поставленной процедуре оценки рисков можно не ставить столь грандиозных задач и существенно сократить список ПО, для начала ограничив его средствами защиты.

Цифровой суверенитет достижим

Цифровой суверенитет достижим — если правильно подходить к делу и уметь добиваться результата. Не нужно рубить с плеча, делать громкие заявления и резко объявлять тендеры — необходим поэтапный стратегический подход по постепенному замещению зарубежных технологий национальными. В стране разрабатываются антивирусы (лучшие в мире! — ничуть не преувеличивая), средства шифрования и многое другое. Но будем опять же честными — наши продукты зачастую по качеству лучшие в мире, но по количеству продуктов в продуктовой линейке мы уступаем западным вендорам. В стране просто нет платежеспособного спроса, способного окупить редко используемые продукты, — а их разработка и поддержка зачастую отнимает больше, чем разработка и поддержка флагманских решений. Вот где нужна поддержка и стратегия.

Пока нет своего — можно не свое, но после тщательной проверки. Но только пока. Вечно жить в мире блаженной неги не выйдет. Так или иначе, нефти осталось на считанное количество лет.

P.S.

На следующий день после написания статьи появилась информация о том, что «Ростелеком» создает поисковую систему, которая будет базироваться на домене Sputnik.ru.

P.P.S.

Уже в момент правки статьи вышла новость о том, что президент США Барак Обама нанес удар по Китаю, запретив американским ведомствам и правительственным организациям закупать там ИТ-оборудование. Как было сказано — в ответ на хакерские атаки. Заметим, что никакой суд — а у нас и в США правовая система — официально не подтвердил обвинения. Русские хакеры считаются еще более опасными, чем китайские, — а потому нельзя быть уверенным в том, что на столе президента США не лежит похожее распоряжение – о запрете экспорта ИТ-технологий в Россию.

Вячеслав Медведев

Автор: Артур Скальский © ПОЛИТ.РУ ИНТЕРНЕТ И ИТ, РОССИЯ 3215 18.04.2013, 01:04 337
URL: https://babr24.com/?ADE=114255 Bytes: 16357 / 16245 Версия для печати Скачать PDF

Автор текста: **Артур Скальский**.