IT-TECHNOLOGIES IN THE SYSTEM OF STATE MANAGEMENT: DOMESTIC OR FOREIGN SOFTWARE?

Tsurankova M.N. (Russian Federation) Email: Tsurankova52@scientifictext.ru

Tsurankova Marina Nikolaevna - Graduate Student,
FACULTY OF ECONOMICS,
RUSSIAN STATE UNIVERSITY OF JUSTICE, MOSCOW

Abstract: *this article discusses the problem of information security in the public administration system when using foreign information technologies, the positive and negative factors of the introduction of domestic software, the reasons for the ineffective implementation of the Decree on domestic software, the strategic importance of the development of domestic technologies for internal and external security of the state.*
Keywords: *information security, information technology, software, confidentiality.*

IT-ТЕХНОЛОГИИ В СИСТЕМЕ ОРГАНОВ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ: ОТЕЧЕСТВЕННЫЙ ИЛИ ЗАРУБЕЖНЫЙ СОФТ?

Цуранкова М.Н. (Российская Федерация)

Цуранкова Марина Николаевна – студент магистратуры,
экономический факультет,
Российский государственный университет правосудия, г. Москва

Аннотация: *в этой статье рассматривается проблема информационной безопасности в системе государственного управления при использовании информационных технологий иностранного производства, позитивные и негативные факторы внедрения отечественного программного обеспечения, причины неэффективной реализации Постановления об отечественном софте, стратегическое значение развития отечественных технологий для внутренней и внешней безопасности государства.*
Ключевые слова: *информационная безопасность, информационные технологии, программное обеспечение, конфиденциальность.*

Современный этап развития общества характеризуется интенсивной информатизацией всех сфер жизнедеятельности: производство и управление, оборона и связь, транспорт и энергетика, финансы и политика, наука и образование – все зависит от интенсивности информационного обмена, полноты сведений, своевременности и достоверности информации. В современном обществе информационные технологии играют все более заметную роль. Интернет объединяет более ста стран мира и можно говорить уже о том, что информация рождает власть и правит миром. IT-технологии позволяют осуществлять интегрирование рынка товаров и услуг, труда, инвестиций и финансов на международной арене, становятся одним из решающих факторов эффективного функционирования государственного управления, социально-экономического развития общества.

Информационные ресурсы становятся стратегически важным объектом в современном мире, поэтому информатизация государственных и муниципальных органов власти сегодня является непосредственно одной из приоритетных задач государства. Их возрастающая значимость обусловила переход вопросов использования IT-технологий в разряд приоритетных направлений государственной политики России, а внедрение в сферы государственного и муниципального управления становится задачей общей безопасности государства. Сейчас жизнедеятельность государственного организма целиком определяется уровнем развития, качеством функционирования и безопасностью информационной среды.

Говоря о позитивных факторах применения информационных технологий в деятельности госорганов, стоит отметить повышение качества предоставления государственных услуг населению, повышение эффективности предоставляемого спектра услуг (за счет сокращения временных затрат на получение запросов, оповещение граждан и другое), обеспечение прозрачной деятельности органов госвласти, создание электронного документооборота и т.д. Помимо плюсов всегда есть и отрицательные аспекты, которые могут нести необратимый характер, если не предупредить их возникновение. Угроза информационной безопасности федеральных, региональных и местных органов власти – это основной негативный фактор в этом вопросе. Обеспечение информационной безопасности госуправления играет важную роль, как во внешней, так и во внутренней политике государства [1].

Явными причинами, отрицательно влияющими на создание эффективной системы информационной безопасности в органах власти, являются такие, как отсутствие достаточного уровня квалификации персонала или недобросовестное отношение сотрудников к безопасности в IT- структуре (понимание необходимости процесса со стороны участников, т.к. информационные системы могут подвергаться

угрозе не только из-за их технического несовершенства, ни из-за ошибок при использовании), пренебрежение некоторыми органами власти нормативно-закрепленными требованиями, затраты на переоснащение при использовании инновационных подходов, общая информационная среда, средствам которой можно воспользоваться информацией, в том числе и государственной важности.

В течение многих лет проблемы IT-безопасности в значительной мере игнорировались, но ситуация начала меняться. Сейчас безопасность считается одной из главных проблем. Интерес к этому вопросу повышается ввиду растущего использования глобальной сети, что вызывает опасность внешнего вмешательства и затрагивает важные аспекты. Возрастающая сложность IT-инфраструктуры обуславливает большую уязвимость по отношению к техническим сбоям, человеческим ошибкам, злоумышленным действиям и другим внешним атакам. Кроме обеспечения безопасности такими мерами, как верификация пользователя или шифрование данных необходимо предпринимать более глобальные меры.

Нельзя не сказать, что сейчас превосходство государства во многом зависит от его позиций на рынке IT-технологий и возможностью государства контролировать и управлять информационными процессами. Так западный мир, в частности - США, рассматривают доминирование в IT - среде, как необходимое условие эффективных межгосударственных отношений и внешней (а может, и внутренней) политики. По моему мнению, при этом ставится не только задача нанесения ущерба национальным интересам нашей страны, но создание и поддержание технологической и информационной зависимости. Как доказательство к этому можно вспомнить «Концепцию информационной войны», которая была сформулирована министерством обороны США в конце XX века и на реализацию которой выделяются миллиарды долларов ассигнований из бюджета [2]. В целом, в качестве информационного оружия могут применяться компьютерные вирусы (способны размножаться, внедряться в программы, передаваться по линиям связи и сетям передачи данных, выводить из строя целые системы), программные закладные устройства (часто заранее внедряются в информационные продукты и по сигналу или в установленное время приводятся в действие), средства фальсификации информации, разнообразные ошибки (те, которые сознательно вводятся в ПО). Такое информационное оружие сейчас широко применяется хакерами-любителями, однако, по оценкам специалистов, сегодня в мире насчитывается свыше 50 государств, осуществляющих компьютерные диверсии и шпионаж, поддерживаемые на государственном уровне посредством использования возможностей различных IT-ресурсов. Последствия таких акций могут приравниваться к результатам применения оружия массового поражения (вспомним хотя бы атаку хакеров в 2002 году на глобальную сеть «Интернет», когда были выведены из строя 8 из 13 серверов, что поставило ее на грань полного разрушения) [3].

Одним из наиболее уязвимых мест в применении информационного оружия становятся программные обеспечения. Политика информатизации при всей своей открытости и ориентации на соблюдение законных прав граждан на информацию и интеллектуальную собственность, должна защищать от проникновения скрытых элементов информационного оружия. Это особенно важно, учитывая массовое использование иностранного софта IT-технологий, в том числе, органами государственного и местного самоуправления. Особо остро в России сейчас встает проблема защиты собственных информационных ресурсов, учитывая все реальные позиции технологического отставания от информационных технологий западного мира.

Вообще, можно говорить и о технических закладных устройствах, которые могут быть использованы производителями микросхем и комплектующих для вычислительной техники в своих целях. Так в ходе операции «Буря в пустыне» французы кодовым сигналом отключили бортовые компьютеры иракской армии, что превратило самолеты в летающие мишени. А после эксперты пришли к выводу, что автоматизированная система ПВО Ирака была парализована именно из-за инициализации программных и аппаратных закладок в компьютерной технике западного производства

Тем не менее, важнейшим элементом, определяющим устойчивость работы информационной системы и ее защищенность, является используемое ПО и ОС, обеспечивающие взаимосвязь между компонентами информационной сети.

Безусловно, мировым лидером по популярности, в том числе и в нашей стране, является операционная система корпорации Microsoft. А между тем, Windows недоступна в исходных кодах, что не может не насторожить, когда речь идет о безопасности государства - ведь там могут содержаться программные закладки, которые в любой момент могут быть приведены в действие по сигналу на разработчика. Даже на просьбы пользователей открыть исходные коды США отказали, мотивируя это тем, что система Windows является национальным достоянием. Здесь мне кажется вполне логичным отказ Германии от использования ПО Microsoft сразу же после заявления немецких экспертов о наличии специальных кластеров, встроенных в операционную систему для доступа американских спецслужб к пользователям, а Бундесвер вообще отказался от использования на стратегически важных ПК всех американских IT-продуктов [4].

Кроме того, большинство вирусных программ разрабатываются именно под Windows, как наиболее используемую в мире, а спрос на продукты Microsoft также диктует свои правила и, в следствии, некоторые обновления корпарации выходят «недоработанными». Например, в 2014 году вышел очередной пакет обновлений Windows 7, которые привели к отказу тысяч компьютеров по всему миру, т.к. в нем имелись критические ошибки. Такая же ситуация повторилась с Windows RT, Windows 8, Windows 8.1 [5]. А ситуация с Windows 10 вообще обескураживает своей непосредственностью. В этой ОС все создаваемые пользователем файлы по умолчанию копируются на американские сервера сетевого хранилища (OneDrive). По своим свойствам же эта версия больше напоминает вирус: Microsoft настойчиво предлагает пользователям прежней версии установить новую, обещая уникальные возможности. Как правило, линейный пользователь уступает надоевшим просьбам, а в результате - его ПК выдает изрядный список ошибок. Попытка же вернуть старую версию может обернуться полным провалом. Практически, Windows 10 весьма ненавязчиво сообщает о том, что собирает информацию и даже, не нарушая действующего законодательства, спрашивает согласия. У пользователя, разрешившего установку обновленной версии, выбора особого нет, и он вновь соглашается. Стоит ли говорить, что использование такой ОС в госучреждениях абсолютно недопустимо, т.к. может сказаться не только на качестве предоставляемых услуг населению, но и привести к фатальным результатам общегосударственной системы.

Стоит отметить, что при наличии должной воли сверху Россия способна сделать качественный технологический рывок, отказавшись от зарубежного ПО. О необходимости форсированного развития отечественного рынка ПО, обеспечивающих максимальную независимость от иностранных разработок в сфере высоких технологий и сохранении информационного суверенитета России впервые на высшем уровне заговорили в 2014 году, когда санкции ЕС и США резко повысили риски, связанные с зарубежным софтом в государственных органах. Именно тогда в Минсвязе РФ всерьёз озадачились решением этого стратегически значимого вопроса. Были приняты обширные меры по поддержке отечественных разработчиков (преференции в сфере госзакупок отечественных IT-компаний, всевозможные конкурсы и государственные гранты), стимулированию спроса на национальный продукт. В краткие сроки на законодательном уровне были наложены ограничения на использование иностранного ПО, а уже в 2015 году премьер-министр Д. Медведев подписал Постановление[1], согласно которому с 01.01.2016 госорганы были обязаны закупать софт из специального реестра отечественного ПО. Приобрести же иностранную продукцию они могут только при отсутствии российских аналогов, причем должны предоставить обоснования для закупки западного продукта.

Но невозможно не сказать о «пробелах» в нормативно-правовой базе: согласно действующему законодательству российским ПО признается софт, принадлежащий компании с долей иностранного капитала менее 50%. Никаких ограничений на сотрудничество с иностранцами, по сути, не накладывается. Очень много инициатив по-прежнему остается на бумаге, хотя простор для работы российских IT-компаний колоссальный. Председатель комитета по информационной политике Л. Левин уверен, что отечественный софт может занять до 75% рынка госзакупок вместо нынешних 25%. Однако, как отметил парламентарий, «часто отечественные поставщики не информируются о конкурсах под надуманными предлогами». Так, по данным РБК, с ссылкой на Е. Василенко (исполнительного директора АРПП «Отечественный софт»), госорганы сами иногда нарушают закон о приоритетных закупках отечественного софта [6].

Специалист по информационной безопасности Российского института стратегических исследований (РИСИ) И. Моньков констатировал, что практически весь госсектор РФ, включая министерства, продолжает пользоваться Windows, многочисленным иностранным ПО и мессенджерами. В лучшем случае ведомства и госкомпании отказались от почты Google, перейдя на «Яндекс», Mail или закрытую систему обмена сообщениями и документооборота. А пресс-секретарь Президента РФ Д. Песков в конце 2016 года еще говорил о невозможности перехода госорганов на российские ОС, пока отечественный софт не будет соответствовать зарубежным аналогам [7].

Но вот сегодня уже можно говорить о конкурентоспособном отечественном ПО. За последние годы были выпущены такие продукты, как: РОСА (Разработчик: ООО «НТЦ ИТ РОСА», сайт продукта: rosalinux.ru), Ось (Разработчик: Национальный центр информатизации - входит в госкорпорацию «Ростех», сайт продукта: os-rt.ru), была презентована на конференции в 2017 году), Альт Линукс (Разработчик: компания «Базальт СПО», сайт продукта: basealt.ru), Calculate Linux (Разработчик: компания «Калкулэйт», сайт продукта: calculate-linux.ru), Astra Linux (Разработчик: НПО «Русские базовые информационные технологии», сайт продукта: astra-linux.ru), Ульяновск.BSD (Разработчик: Сергей Волков, сайт продукта: ulbsd.ru), Заря (разработана специально для вооруженных сил ФГУПом «Центральный научно-исследовательский институт экономики, информатики и систем управления», сайт

продукта: cniieisu.ru), ГосЛинукс (разработана специально для нужд государственных органов власти) и Колибри[2] (которая, кстати, на столько легковесна, что вмещается на обычный флеш-носитель) и др.

Хоть большинство из них и использует дистрибутив Linux, они все являются самостоятельным ПО, не зависящим от ядра Microsoft, как было до этого: так называемые отечественные ПО были всего лишь до неузнаваемости переработанной Windows на платформе иностранного софта (например, СПЕКТРУМ, БедОС 2, ТАНЯ). Однако, российские ПО были доработаны, в них были устранены ранее возникающие ошибки и сейчас можно говорить не только о конкурентоспособности с западными ПО, но и ряде преимуществ.

Если обобщить, то можно отметить удобный для пользователя, привыкшего работать с тем же Windows, интерфейс, простоту установки, возможность бесплатного скачивания и поддержку производителя от 4 лет. Кроме того, в этих ПО предусмотрены пакеты для домашнего, корпоративного или серверного использования и вместе с тем не требуют высокотехнологичной оснастки ПК. Также они отличаются достаточно большой функциональностью и объемным пакетом приложений, уже встроенных и, соответственно, не требующих дополнительных материальных ресурсов на их приобретение. Тем не менее, эти отечественные ПО совместимы со всеми программами, поддерживаемые Windows. За счет простоты конфигурации им удается загружаться и выключаться быстрее продукциям редмондской корпорации. А проблема вирусов будет беспокоить только тех, кто их целенаправленно устанавливает в систему. «Внезапно» на компьютере они не могут появиться.

Ещё одним преимуществом российских ОС, хоть они и адаптированы на несколько языков, является активное и доступное русскоязычное сообщество в соцсетях и на форумах, где разработчики гораздо ближе к пользователям и способны помочь новичкам освоиться.

Иными словами жаловаться на отсутствие отечественных операционных систем нам не приходится. Кроме того, свои работы в данном направлении ведут ООО «Р-Платформа», Раменское приборостроительное конструкторское бюро (входит в концерн «КРЭТ» Ростеха) и другие компании. Именно по этой причине мы приглашаем читателей 3DNews принять участие в обсуждении материала и поделиться ссылками на достойные внимание проекты в этой области.

К сожалению, информатизация сферы ГМУ в России происходит в целом весьма хаотично и со значительным отставанием от требований времени. Проблема информационной безопасности в системе государственного и муниципального управления останется открытой ещё на долгие годы. В эпоху информационного общества необходимо адаптироваться ко всем инновациям в сфере информационных технологий. И походу создания новейших технологий разрабатывать средства защиты от организаций, представляющих угрозу информационной безопасности.

Список литературы / References

1. *Голобородько Ю.А.* Государственная культурная политика в системе обеспечения национальной безопасности современной России // Государственное и муниципальное управление: Ученые записки СКАГС, 2012. № 3. С. 128-133.
2. *Аверчинков В.И., Рытов М.Ю., Кондрашин Г.В., Рудановский М.В.* Системы защиты информации в ведущих зарубежных странах // Учебное пособие: Брянск, Издательство БГТУ, 2007. С. 38-54.
3. *Воробьева А.А., Пантюхин И.С.* История развития программно–аппаратных средств защиты информации // Учебное пособие: Санкт–Петербург, 2017. С. 44-47.
4. Правительство Германии предостерегает ведомства страны от использования Windows 8 [Электронный ресурс], 2013. Режим доступа: https://habrahabr.ru/ (дата обращения: 21.04.2018).
5. Новое обновление Windows: опять проблемы. [Электронный ресурс], 2014. Режим доступа: https://xakep.ru/ (дата обращения: 21.04.2018).
6. Ограничение госзакупок иностранного ПО: надежды и сомнения. [Электронный ресурс], 2015. Режим доступа: http://tass.ru/ (дата обращения: 21.04.2018).
7. Песков признал невозможность перехода госорганов на российский аналог Windows [Электронный ресурс], 2016. Режим доступа: https://m.lenta.ru/ (дата обращения: 21.04.2018).