Информационная безопасность.
Опасность зарубежного программного обеспечения, сервисов и услуг.
Некоторые мероприятия Российской Федерации по импортозамещению.

ВВЕДЕНИЕ

В настоящее время в борьбе за сферы экономического и политического влияния акцент с открытого, в том числе военного, противостояния все заметнее смещается в сторону использования различных форм контроля и управления информационными ресурсами государств. Для достижения этих целей применяются высокоэффективное скрытое проникновение в информационные, телекоммуникационные и управляющие системы, а также активно навязываемая всеми доступными средствами привязка к информационным технологиям зарубежного происхождения. В результате информационная инфраструктура государства становится технологически зависимой даже от отдельной фирмы-производителя программного обеспечения.

1. ИНФОРМАЦИОННОЕ ВОЗДЕЙСТВИЕ КАК НОВЫЙ ВИД ОРУЖИЯ

Ни одна организация-разработчик не гарантирует абсолютной надежности создаваемого программного продукта, фактически снимая с себя ответственность за последствия, к которым могут привести дефекты в программах.

Информационное воздействие может рассматриваться как новый вид оружия, которое в определенной степени более эффективно, чем традиционные виды вооружения и военной техники.

Россия обладает значительным военным потенциалом и представляет серьезное препятствие для проводимой странами Запада, прежде всего США, политики экономической, культурной и военной экспансии. Поэтому она является объектом наиболее пристального внимания спецслужб иностранных государств, занимающихся вопросами информационного противоборства.

Современное программное обеспечение – очень сложный продукт. При его создании используются специальные программные средства разработки и системное программное обеспечение, объем и сложность которого могут на порядок превышать аналогичные характеристики прикладного программного обеспечения. В связи с этим верификация программного обеспечения представляет практически неразрешимую задачу. Именно поэтому ни одна организация-разработчик не гарантирует абсолютной надежности создаваемого

программного продукта, фактически снимая с себя ответственность за последствия, к которым могут привести дефекты в программах.

Особую сложность представляет обнаружение дефектов, которые могут преднамеренно вноситься на этапе создания программных продуктов. Имевшая место в России тенденция импорта зарубежных программных средств и информационных технологий очевидно привела к увеличению возможного импорта программных дефектов. При этом достаточно высока вероятность поражения важнейших информационных систем России информационным оружием уже на этапе их разработки.

Недостатки и отставание в создании информационных технологий, в разработке нормативно-методической базы контроля безопасности программного обеспечения многократно обостряют проблему информационной безопасности России. Поэтому основой безопасных информационных технологий должны стать отечественные системные и инструментальные программные средства (операционные системы, компиляторы, отладчики, кроссассемблеры и т.д.), обеспечивающие эффективную разработку прикладного программного обеспечения.

2. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРОГРАММНЫХ СРЕДСТВ И СЕРВИСОВ

Проблема информационной безопасности имеет два аспекта: технологический и эксплуатационный

Технологическая безопасность подразумевает отсутствие в программном обеспечении злоумышленных программных дефектов диверсионного типа.

Эксплуатационная безопасность характеризует защищенность информации от несанкционированного доступа и несанкционированных действий с ней.

При этом очевидно, что одними только мероприятиями по защите информации и информационных систем от несанкционированного доступа нельзя обеспечить ее безопасность. При всей их эффективности они не исключают ситуации, когда защищенные информационные системы содержат в своем составе программное обеспечение, имеющее программные закладки, то есть специально внесенные дефекты либо блоки, реализующие так называемые недекларированные возможности. Эти блоки могут быть направлены на решение задач, выходящих за рамки данного программного средства (например, сбор персональной информации, данных о выполняемых прикладных программах и т.п.). Более того, программные средства защиты также могут содержать программные закладки.

Например

Elcomsoft, российская компания, специализирующаяся на разработке средств криминалистического анализа данных, хранящихся, в частности, на мобильных устройствах и в облачных сервисах, сообщала, что Apple вопреки официальным заявлениям фиксирует в iCloud – с неопределенной целью – историю звонков, совершаемых пользователем не только в сотовой сети, но и с помощью сервисов Skype, WhatsApp, Viber и FaceTime.

«Начинаю верить в теории заговора и постоянно вспоминаю Сноудена. Теперь мы уже не так уверены, что Apple не хранит и сообщения (iMessage) тоже, хотя, конечно же, они это гневно отрицают», — такую оценку обнаруженной недокументированной возможности дал гендиректор Elcomsoft Владимир Каталов в переписке с корреспондентом D-Russia.ru.

Как это происходит

Специалисты Elcomsoft в данном случае (как и в предыдущей истории, когда им удалось обнаружить, что фотографии, сделанные iOS-устройством и удалённые пользователем, на самом деле не уничтожаются, а неопределённо долгое время остаются доступны) извлекали информацию не из мобильных устройств, а из облачного хранилища iCloud, где регистрируются и сохраняются данные пользователя. Предметом исследования был протокол передачи данных между серверами Apple и мобильным устройством, и результаты исследования позволили обнаружить, какие сведения о поведении пользователей в действительности хранит Apple.

Легально, то есть в соответствии с тем, что заявляет Apple, в iCloud по желанию пользователя хранятся контакты и календари, резервные копии системы, фотографии. Но синхронизация с iCloud истории звонков – это недокументированная функция, работающая без ведома пользователя.

Какие данные о звонках собирает Apple

В iCloud сохраняются все звонки за последние четыре месяца. Для устройств, работающих под управлением iOS 10, в облаке фиксируются пропущенные («missed») звонки, совершённые через WhatsApp, Viber или Skype. Звонки, совершённые по FaceTime (сервис видеозвонков от Apple, встроенный в iOS), сохраняются полностью.

Для каждого звонка фиксируются следующие метаданные:

- номер абонента;
- точные дата, время и продолжительность звонка;
- статус звонка (входящий или исходящий, поддерживалась ли при соединении передача видео, а также атрибуты «not answered» (без ответа) и «missed» (пропущенный);
- данные, назначение которых в Elcomsoft пока не выяснили.

Если к аккаунту Apple привязано несколько устройств, нельзя определить, с какого именно из устройств (или на какое из них) был сделан звонок.

Подозрения, что Apple фиксирует историю звонков, возникли у Elcomsoft из-за того, что пользователи, чьи iPhone «привязаны» к одной и той же учётной записи Apple ID (обычная практика для, например, супругов – это облегчает совместное использование покупок, сделанных в App Store или iTunes), обнаружили в истории звонков на своём устройстве сведения о звонках, которые совершались с другого устройства, использующего тот же Apple ID. Очевидное предположение о том, что такая синхронизация происходит через iCloud, подтвердилось.

Единственное правдоподобное объяснение: Apple делает это ради ФБР

В Elcomsoft самым вероятным объяснением массовой слежки Apple за звонками пользователей считают сотрудничество с американскими спецслужбами: компания оставила им лазейку. Сами устройства защищены достаточно надёжно, и Apple на радость своим поклонникам демонстративно отказывается их вскрывать по запросу ФБР и даже по решению суда.

Но, как теперь оказывается, взламывать iPhone террориста нет нужды – всё необходимое есть в iCloud.

Такое предположение многое подтверждает. Даже если пользователь отключает в настройках устройства опцию «Allow Calls on Other Devices» («Разрешить звонки с других устройств», то есть устройств, использующих тот же Apple ID), данные о звонках все равно попадают в iCloud. История звонков сохраняется постоянно, не в реальном времени, но близком к реальному.

А главное, чего ради Apple рисковать репутацией. Однако рискует. В Legal Process Guidelines («Основные принципы юридической практики») Apple заявляет, что хранит в iCloud данные только тех приложений, которые выбрал для хранения сам пользователь («iCloud only stores content for the services that the subscriber has elected to maintain in the account while the subscriber's account remains active»), что действительности не соответствует. Даже хранение в iCloud истории звонков FaceTime, о чём пользователя честно предупреждают, и то делается жульнически – вместо обещанных до 30 дней, и не более, история хранится четыре месяца, а может, и дольше.

Есть ли защита

От американских спецслужб здесь защиты нет и быть не может, они доступ к истории звонков интересующего их человека получат беспрепятственно и без того, чтоб Apple потеряла лицо. Никаких судов, никакого взлома айфонов – просто доступ к серверу.

Данные, хранящиеся в iCloud, зашифрованы – Apple не упускает случая с гордостью сообщить об этом, и это же зафиксировано в официальной документации. Однако Apple нигде не сообщает, что хранит ключи шифрования вместе с данными. Всякий, у кого есть доступ к облаку (а есть он, прежде всего, у Apple), может не только взять данные, но и расшифровать их. «Мы это установили ещё четыре года назад», — говорит Владимир Каталов.

Пользователь при этом лишен возможности как-либо влиять на метод защиты своих данных в iCloud. Если, например, для локальной копии документов и фотографий он может решать, прибегать ли к криптозащите с помощью пароля или нет, то в облаке выбор отсутствует, все решения принимает Apple. Иными словами, для облачных резервных копий пользовательский пароль (или какое-то иное шифрование, задаваемое пользователем) не применим в принципе.

Такой доступ к серверу могут получить не только спецслужбы, но и хакеры. Та же Elcomsoft не ограничивается исследовательской работой и предлагает программный продукт для легального – через логин и пароль учётной записи Apple ID – «выкачивания» истории звонков из iCloud. Чтобы завладеть учётной записью, хакеру придётся прибегнуть к обычному шпионажу или социальной инженерии, как это уже было в случае с кражей фото знаменитостей в 2014 году.

Elcomsoft ограничивается рекомендацией обязательно активировать предлагаемую Apple двухфакторную авторизацию доступа к учётной записи – в этом случае у хакера на все про все будет 30 секунд, в течение которых активен временный код доступа. Для социально-инженерной операции, скорее всего, не хватит.

Заметим, что устройства, работающие на операционных системах Android и Windows, ничуть не безопаснее устройств на iOS. Функция сохранения истории звонков в облаке присутствует в Android 6.0 начиная с апреля 2016 года. Есть она и в Windows 10 Mobile. В отличие от Apple, Google и Microsoft официально предупреждают об этом своих пользователей.

Анализ вероятных последствий применения программных закладок показывает, что в случае систем управления военного назначения речь может идти о блокировании возможности применения системы оружия определенного класса или информационной системы оборонного характера. В других случаях – о блокировании передачи, утечке или модификации (вплоть до уничтожения) информации в информационно-телекоммуникационных системах государственного управления, утечке или модификации (уничтожении) финансовой или банковской информации, нарушении функционирования экологически опасных производств, в первую очередь связанных с атомной энергетикой. Фактически это означает, что Россия, обладающая мощным оружием сдерживания потенциального агрессора, может оказаться безоружной.

Например.

Самым ярким примером действия программной закладки является военный конфликт в Персидском заливе. Тогда при проведении операции «Буря в пустыне» система ПВО Ирака оказалась заблокированной по неизвестной причине. Несмотря на отсутствие исчерпывающей информации, высказывалось предположение, что ЭВМ, входящие в состав комплекса технических средств системы ПВО, закупленные Ираком у Франции, содержали специальные управляемые электронные закладки, блокировавшие работу вычислительной системы.

Периодически эксперты обнаруживают недокументированные возможности в ПО аппаратных комплексов. Например, в информационном бюллетене Computer Emergency Response Team объявлено о существовании программной закладки (backdoor) в операционной системе AOS (Alcatel Operating System) версии 5.1.1, применяемой для управления коммутаторами Alcatel OmniSwitch 7700/7800. Эта закладка запускает telnet-сервис, что позволяет удаленному злоумышленнику неавторизованно управлять коммутатором.

Нередки случаи, когда уволенный программист похитил данные через оставленный собой же «черный ход» (backdoor) в программе.

8 октября 2012 года РИА Новости со ссылкой на Ассошиэйтед Пресс сообщало, что комитет по разведке при Палате представителей США рекомендует частным американским компаниям воздержаться от любых деловых контактов с Huawei и ZTE, а властям США – отказаться от использования продукции этих производителей.

А агентство Bloomberg сообщало о намерении властей США проверить деятельность Huawei и ZTE на наличие в продукции, поставляемой ими на территорию Соединенных Штатов, инструментов для шпионажа в пользу Китая.

Обеспечение безопасности информационных и автоматизированных систем, от расчетного функционирования которых зависит безопасность России,

требует, в первую очередь, создания и внедрения перспективных автоматизированных систем обработки информации. При этом повышение требований к средствам управления в критических сферах, постоянное расширение круга решаемых ими задач приводят к возрастанию удельного веса программного обеспечения в автоматизированных системах управления. Это, в свою очередь, повышает требования к безопасности программного обеспечения, а, следовательно, и к безопасности используемых при его разработке и эксплуатации информационных технологий.

Недостатки и отставание в создании информационных технологий, в разработке нормативно-методической базы контроля безопасности программного обеспечения многократно обостряют проблему информационной безопасности России.

Таким образом, ключевым элементом безопасного функционирования критической инфраструктуры является безопасность информационных технологий, используемых при разработке программного обеспечения.

Под безопасностью информационных технологий понимается их способность к парированию (нейтрализации) или недопущению воздействий внешних и внутренних угроз безопасности информации, таких как:

- внедрение злоумышленных программных закладок, нарушающих расчетное функционирование систем;
- несанкционированный доступ к информации с целью ее модификации или уничтожения либо получения лицом, для которого данная информация не предназначена, с помощью специальных программных закладок, которые позволяют нейтрализовать механизмы защиты информации и информационных систем.

С учетом изложенного можно утверждать, что злоумышленные программные дефекты – самая опасная разновидность информационного оружия, а проблема обеспечения безопасности систем критической инфраструктуры является наиболее актуальной.

3. ПРИНЦИПЫ СОЗДАНИЯ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В основу реализации политики в области создания информационных технологий для систем критических приложений должны быть положены следующие принципы:

- государственное бюджетное финансирование фундаментально-поисковых, научно-исследовательских и опытно-конструкторских работ по созданию и внедрению безопасных информационных технологий и их элементов на предприятиях-разработчиках программных средств с сохранением государственной собственности на разработанные технологии;
- долевое финансирование за счет средств государственного бюджета, коммерческих и банковских структур, а также важнейших государственных корпораций научно-исследовательских и опытно-конструкторских работ по созданию и внедрению безопасных информационных технологий в кредитно-финансовую и банковскую сферы, на критически важных объектах промышленной и энергетической инфраструктуры государства;
- выделение и государственная поддержка научных организаций и наукоемких промышленных предприятий, способных разработать промежуточный вариант безопасных информационных технологий и их элементов, с возможным оформлением их в качестве «ноу-хау» и коммерческим распространением как в России, так и за рубежом;
- создание и государственная поддержка системы независимых центров контроля безопасности программных средств, не исключающая их коммерческой деятельности.

Итак, использование зарубежного программного обеспечения может представлять серьезную угрозу информационной безопасности России, особенно в случае его применения для систем критических приложений. Существующая система аттестации и сертификации импортных программных продуктов не может дать стопроцентной гарантии отсутствия в них программных закладок.

4. ИМПОРТОЗАМЕЩЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

С 1 января 2016 года все государственные и муниципальные органы, государственные корпорации «Росатом» и «Роскосмос», органы управления государственными внебюджетными фондами, а также казенные и бюджетные учреждения, осуществляющие закупки в соответствии с требованиями Федерального закона от 5 апреля 2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», обязаны соблюдать запрет на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд.

Запрет введен постановлением Правительства Российской Федерации от 16 ноября 2015 года № 1236 «Об установлении запрета на допуск программного

обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

При закупке программного обеспечения вышеперечисленные заказчики должны прямо указывать на запрет приобретать импортное ПО в извещении об осуществлении закупки.

Запрет распространяется на закупки программ для электронных вычислительных машин и баз данных, реализуемых независимо от вида договора на материальном носителе и (или) в электронном виде по каналам связи, а также исключительных прав на такое программное обеспечение и прав использования такого программного обеспечения.

Есть несколько исключений, когда закупка импортного ПО заказчикам разрешена:

- закупки программного обеспечения и (или) прав на него дипломатическими представительствами и консульскими учреждениями Российской Федерации, торговыми представительствами Российской Федерации при международных организациях для обеспечения своей деятельности на территории иностранного государства;
- закупки программного обеспечения и (или) прав на него, сведения о котором и (или) о закупке которого составляют государственную тайну;
- сведения о программном обеспечении, соответствующем требуемому к закупке, отсутствует в реестре отечественного программного обеспечения;
- характеристики требуемого программного обеспечения, отличаются от характеристик программного обеспечения того же класса и представленное в реестре.

Во всех остальных случаях от заказчика перед осуществлением закупки программного обеспечения потребуется работа с единым реестром российских программ для электронных вычислительных машин и баз данных и классификатором программ для электронных вычислительных машин и баз данных.

По итогам конференции Russian Interactive Week представители Минкомсвязи России обнародовали новые тезисы закона о импортозамещении в ИТ. Основные из них:

- создание реестра российских ИТ-продуктов. Главные критерии внесения в него – исключительное право на ПО должно принадлежать Российской Федерации, российскому региону, муниципальному образованию или коммерческой организации;

- суммарная доля прямого или косвенного участия такого субъекта должна составлять более 50%;
- общая сумма лицензионных отчислений его в пользу иностранных организаций не может превышать 30% от общей суммы выручки.

5. ПЛАН ИМПОРТОЗАМЕЩЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДО 2025 ГОДА

Приказ Министерства связи и массовых коммуникаций Российской Федерации об утверждении плана по импортозамещению программного обеспечения от 01 февраля 2015 года № 96.

Цель: установить конкретные задачи по поэтапному сокращению доли импортного программного обеспечения в российских государственных и коммерческих предприятиях.

МИНИСТЕРСТВО СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНКОМСВЯЗЬ РОССИИ)

ПРИКАЗ

01.04.2015 № 96

Москва

Об утверждении плана импортозамещения программного обеспечения

В целях реализации пункта 41 плана первоочередных мероприятий по обеспечению устойчивого развития экономики и социальной стабильности в 2015 г., утвержденного распоряжением Правительства Российской Федерации от 27 января 2015 г. № 98-р (Собрание законодательства Российской Федерации, 2015, № 5, ст. 866), формирования благоприятных условий для развития разработки отечественного конкурентоспособного программного обеспечения, учитывая предложения заинтересованных российских организаций отрасли информационных технологий и их объединений (ассоциаций),

ПРИКАЗЫВАЮ:

Все продукты либо их прототипы, импортозамещение которых признается необходимым, разделены в документе на три сегмента, к каждому из которых подобран индивидуальный подход со стороны государства:

- сегмент рынка корпоративного программного обеспечения, в котором уже имеется задел конкурентоспособности отечественных разработок. Например: антивирусное ПО, браузеры, бизнес-приложения типа CRM, сервисы обмена мгновенным сообщениями. Подход государства: предоставление преференций при осуществлении госзакупок;
- сегмент рынка корпоративного ПО, по которому отсутствует задел отечественных конкурентноспособных аналогов. Примеры: мобильные операционные системы, средства управления «облачной» инфраструктурой, системы управления базами данных. Подход государства: помощь в коллективной разработке данного программного обеспечения;
- сегмент программного обеспечения, связанного с отраслевой спецификой. Подобные системы призваны обеспечить развитие: здравоохранения, ТЭК, финансового сектора, транспорта и т.д. Подход государства: совместное взаимодействие с ответственными министерствами и ведомствами.

Присутствие продукта в государственном реестре программного обеспечения означает допуск к госзакупкам программного обеспечения, импорт которого ограничен постановлением Правительства Российской Федерации от 16 ноября 2015 года № 1236.

Заявки на включение в реестр рассматривает экспертный совет при Минкомсвязи России. Совет принимает решения голосованием, при котором для допуска в реестр необходимо набрать простое большинство голосов. Среди участников органа – представители различных ассоциаций разработчиков, сотрудники федеральных органов власти и государственных институтов развития.

Общий объем госзаказа программного обеспечения в 2016 году составляет около 160 млрд. рублей. При этом, импортное ПО занимает в нем долю от 75% до 95%. Наибольшей популярностью у госструктур пользуются SAP, Microsoft, Oracle, Cisco и IBM.

6. КРАТКИЙ АНАЛИЗ ГОСЗАКУПОК ОСЕНЬЮ 2016 ГОДА

Осень 2016 года отличается тем, что относительно крупные закупки западного софта совершались, как правило, либо вместе с оборудованием, либо вместе с отечественным ПО. Вот некоторые значительные лоты этой осени, без ранжирования.

Одним из крупнейших закупщиков стала ФНС, которая объявила конкурс на проведение четвертой (финальной) очереди работ по созданию центров обработки данных. Стоимость услуг — 2,21 миллиарда рублей. В документах имеется обоснование невозможности закупки отечественного ПО: несколько подробных таблиц, в которых отмечены недостатки каждого из программных продуктов нужного класса, включенных в реестр российского софта. «По совокупности функциональных, технических и (или) эксплуатационных характеристик программное обеспечение, сведения о котором включены в реестр, не соответствует установленным государственным заказчиком требованиям к программному обеспечению, являющемуся объектом закупки», резюмируют авторы технического задания.

Департамент города Москвы по конкурентной политике (функциональный заказчик, получатель — Центр организации дорожного движения правительства Москвы) объявил конкурс на оказание услуг по обеспечению бесперебойного функционирования информационных систем интеллектуальной транспортной системы, включая аппаратно-программные средства защиты информации общей стоимостью 196,6 миллиона рублей. Согласно ТЗ, заказчику необходимы, помимо прочего, программные продукты Citilog (VisioPad) (частная компания со штаб-квартирой в Париже), и американские системы видеонаблюдения производства Cisco, а также Microsoft Windows Server.

Обоснования, почему невозможно купить отечественный аналог, обнаружить не удалось. Закупка проходит по категории «Техническое обслуживание и ремонт вычислительной техники».

Департамент информационных технологий Москвы разместил крупный лот на поставку технических и программных средств комплексного обеспечения рабочих процессов Центра автоматического мониторинга содержания объектов городского хозяйства на базе Государственного казенного учреждения «Московский центр «Открытое правительство», с максимальной начальной ценой контракта 187 миллионов рублей. Закупка включает как отечественное ПО (ABBYY FineReader – 125 тысяч рублей, «1С» — 13 тысяч рублей), так и более значительную по стоимости закупку западного ПО: Microsoft Office Standard 2016 на 1,4 миллиона рублей, Adobe Creative Cloud на 302 тысячи, Microsoft Project на 229 тысяч и др. Согласно обоснованию, программные продукты из реестра отечественного ПО не удовлетворяют требованиям заказчика.

Этот же заказчик – ДИТ Москвы – объявил еще один конкурс – на поставку программного обеспечения для поддержки функционирования общегородских информационных систем, обеспечивающих предоставление государственных услуг в электронном виде, стоимостью 154 миллиона рублей. Согласно ТЗ, ведомству необходимо закупить IBM FileNet Content Manager. Обоснование невозможности заменить эту поставку отечественным аналогом приложено. В документации приводится подробная таблица с требованиями заказчика и данными, какими функциями не обладает ПО из того же класса («серверное и связующее ПО»), включенное в реестр.

Пенсионный фонд России объявил лот на поставку оборудования и лицензионного программного обеспечения компонента «Ведомственная телефонная связь» подсистемы «Инфраструктурное обеспечение» АИС ПФР-2 для территориальных органов ПФР на 130 миллионов рублей. ПФР необходимо закупить в числе прочего и программное обеспечение Unify OpenScape Voice V8 («серверное и связующее программное обеспечение») и ПО того же класса Unify OpenScape UC Application V7. Компания Unify входит в группу компаний Atos (штаб-квартира расположена во Франции). В обосновании ведомство приводит список технических требований, и делает вывод, что отечественный аналог не подходит по функциональным характеристикам.

Минобороны закупает ноутбуки трех видов на 102,3 миллиона рублей. Более всего (430) требуется ноутбуков на операционной системе Windows 7 Professional или последующей версии в комплекте с дистрибутивом операционной системы (поставка эквивалента не допускается в соответствии со ст. 33 ФЗ 44-ФЗ в связи с необходимостью обеспечения совместимости с оборудованием и ПО, эксплуатируемым заказчиком) и пакетом программ Microsoft Office Professional plus 2010 или последующей версии (поставка эквивалента не допускается в соответствии со ст. 33 ФЗ 44-ФЗ в связи

с необходимостью обеспечения совместимости с оборудованием и ПО, эксплуатируемым заказчиком). Также закупаются 100 ноутбуков на операционной системе Astra Linux Special Edition с пакетом офисных программ LibreOffice.

Государственное казенное учреждение Новосибирской области «Управление контрактной системы» объявило о конкурсе на 90 миллионов рублей на осуществление услуг по расширению программно-аппаратных комплексов центров обработки данных правительства Новосибирской области в целях размещения информационных систем области.

В обосновании невозможности покупки российского ПО указано, что встроенное программное обеспечение должно быть совместимо с имеющимся у заказчика телекоммуникационным оборудованием сети ТИС НСО, построенным на базе коммутаторов и сетевых экранов Juniper.

Центральное информационно-техническое таможенное управление объявило конкурс на поставку неисключительных прав на использование программного обеспечения Microsoft SharePoint и Microsoft SQL Server Standard на 24 миллиона рублей. Продукты, входящие в реестр, не удовлетворяют ведомство по техническим характеристикам.

Чувашский госуниверситет им И.Н. Ульянова разместил лот на закупку разного вида ПО на 17,2 миллиона рублей. При этом университет не нашел подходящих российских аналогов в таких классах, как «система сбора, хранения, обработки, анализа, моделирования и визуализации массивов данных», «системы управления базами данных», «офисные приложения», «средства обеспечения облачных и распределенных вычислений средства виртуализации и системы хранения данных», «серверное и связующее программное обеспечение», «средства подготовки исполнимого кода» и др.

7. ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ИНОСТРАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Минэкономразвития России совместно с Минкомсвязи России, Минпромторгом России и Институтом развития интернета разработали проект изменений в законодательство о мерах административной ответственности чиновников за несанкционированное использование зарубежного программного обеспечения и телекоммуникационного оборудования. Причиной разработки послужили неоднократные нарушения введенных с начала года ограничительных мер.

Список соответствующих предложений закреплен в проекте доклада, который будет представлен Президенту Российской Федерации В.Путину. По словам представителя Минэкономики Е.Лашкиной, ответственность должностных лиц будет соизмерима с другими подобными нарушениями. Однако, поправки в Кодекс об административных правонарушениях пока не

разработаны. По ее словам, сейчас для правительства более важно обеспечить мониторинг закупок программного обеспечения и оборудования для обнаружения необоснованных покупок.

Некоторые юристы полагают, что наиболее вероятным наказанием будет уже действующая норма КоАП (нарушение порядка осуществления закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд). По ней штраф ограничивается 1% от начальной цены контракта, но не менее 5 тыс. руб. и не более 30 тыс. руб.

Торгово-промышленная палата России уже поддержала идею введения штрафов. По словам главы комитета по развитию системы закупок А.Емельянова, госзаказ является одним из главных инструментов развития российского ИТ-бизнеса. И в данный момент, когда рынок российского ПО находится на подъеме, такая мера вполне оправдана.

Запрет на закупки иностранного ПО вступил в силу 1 января 2016 года. Его действие распространяется на все госорганы. В мае от Минэкономразвития России поступило предложение о расширении списка на компании с государственным участием. Кроме того, было предложено полностью отказаться от иностранного софта в документообороте и делопроизводстве.

Общий объем госзаказа программного обеспечения в 2015 году составил 93,3 млрд. рублей. Доля импортного ПО составила 77%. Наибольшей популярностью у госструктур пользуются компании SAP, Microsoft, Oracle, Cisco и IBM.

8. К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИЮ МЕСЕНЖЕРОВ ДЛЯ РАБОЧЕЙ ПЕРЕПИСКИ

В Минэкономразвития России предлагают законодательно запретить военным и госслужащим пользоваться мобильными приложениями WhatsApp, Viber и Telegram в служебных целях.

Для обмена информацией их обяжут использовать российские мессенджеры для госорганов, возможность разработки которых в конце апреля обсуждалась на совещании у советника президента по интернету Германа Клименко. Минэкономразвития России предлагает установить законодательный запрет на использование госслужащими и военными в служебных целях иностранного софта, в том числе мобильных

приложений, таких как WhatsApp, Viber и Telegram. Также предложено запретить вести рабочую переписку с почтовых ящиков на Gmail.com.

Как сообщила представитель министерства Е.Лашкина, для служебных целей планируется использование только российских мессенджеров. По ее словам, данная позиция согласована с Минкомсвязи России, Минпромторгом России, а также с Институтом развития интернета.

Также в докладе Минэкономразвития России Президенту содержатся предложения по расширению ограничений на закупку иностранного ПО для органов государственной власти.

Вопрос об использовании иностранного ПО для рабочей переписки встал особенно остро после многочисленных утечек конфиденциальной информации, организованных группой хакеров Shaltay Boltay.

В июле 2014 года Shaltay Boltay взломали почтовый ящик на Gmail.com вице-премьера Аркадия Дворковича и опубликовали его переписку. Ее подлинность газете «Ведомости» подтвердили два человека, чьи письма были опубликованы.

В августе 2014 года хакеры опубликовали переписку с нескольких аккаунтов на Gmail.com и Yandex.ru, якобы принадлежащих премьер-министру Дмитрию Медведеву. В письмах говорилось о неудачной попытке покупки часов Casio G-Shock через интернет-магазин Amazon.com. В тот же день был взломан аккаунт премьера в Twitter, где появилось сообщение: «Ухожу в отставку. Стыдно за действия правительства. Простите».

В августе 2015 года секретарь Совета безопасности Российской Федерации Николай Патрушев потребовал от губернаторов принять меры в отношении чиновников, которые используют иностранные сервисы Google, Yahoo и WhatsApp. Патрушев подчеркнул, что использование чиновниками для решения служебных вопросов ресурсов, расположенных за рубежом, представляет серьезную опасность.

28 марта 2016 года стало известно, что московским полицейским запретили передавать служебные сведения через мессенджеры и социальные сети. Приказ об ограничении общения в мессенджерах мог быть связан с тем, что ранее стало известно о подразделении полицейских, которые обменивались информацией через WhatsApp и Viber. Через мессенджеры они получали от начальников графики дежурств и информацию о том, кто и какие посты должен занимать.

В феврале 2016 года на «Радио Свобода» был опубликован материал, в котором содержалась переписка, которую якобы вели московские следователи в приложениях WhatsApp и Viber. В ней обсуждалась фабрикация уголовного дела об угоне автомобиля. В статье отмечалось, что переписка попала в руки журналистов после потери следователем телефона.

Где еще запрещают популярные мессенджеры?

В Казахстане также посредством мессенджера WhatsApp распространялась служебная записка в отношении введения запрета в зданиях всех госорганов на использование мобильных устройств (смартфоны, планшеты, смарт-часы) сотрудниками и посетителями органа власти. Сообщается, что эту меру ввели в связи с активным использованием госслужащими мобильных устройств для служебных целей и участившимися фактами утечки служебной информации через приложение WhatsApp. Вместе с тем, разрешается использование мобильных устройств с функциями «звонок/ответ/sms», но не оснащенными интернет-модулями, фото-, видеокамерами.

Viber в Саудовской Аравии уже запретили, на очереди WhatsApp и Skype. Власти этой страны потребовали от сервисов предоставить возможность отслеживать видеозвонки и сообщения пользователей, на что сервисы ответили отказом. Причем требования эти, судя по сообщениям в СМИ, полностью соответствовали законодательству Саудовской Аравии.

Однако, несмотря на запрет, госслужащие различных уровней продолжают пользоваться зарубежными сервисами. Особенную популярность у них имеет WhatsApp, который установлен на мобильных устройствах у губернаторов, депутатов Госдумы, сенаторов, региональных и муниципальных служащих. Чтобы найти их в сети, достаточно пройти регистрацию и знать номер их телефона. Например, в WhatsApp встречаются аккаунты губернаторов Калужской области Анатолия Артамонова, Тульской области Владимира Груздева, Орловской области Вадима Потомского и других чиновников.

В Беларуси 17 марта этого года опубликовали указ президента «О совершенствовании порядка передачи сообщений электросвязи». Он вступил в силу 18 сентября. Позже появился еще и приказ Оперативно-аналитического центра при президенте Беларуси. Он называется «О системе противодействия нарушениям порядка пропуска трафика на сетях электросвязи». Он тоже вступил в силу 18 сентября. И в нем тоже идет речь о контроле IP-трафика и блокировках, если речь идет о нарушениях.

В Китае за пользование WhatsApp и Instagram начали отключать телефоны. Правительство Китая отключило мобильную связь многим жителям провинции Синьцзян, где проживает крупнейшее сообщество мусульман КНР, за использование интернет-фильтров, позволяющий обойти запрет на использование ряда западных веб-ресурсов и приложений.