НАШИ ИНТЕРВЬЮ

Современные технологические и геополитические изменения обуславливают повышение внимания к проблемам безопасности во всех сферах деятельности, в том числе к технической защите информации. Одним из крупнейших специалистов в названной области является доктор физико-математических наук, профессор ***Баранов Александр Павлович.***

Александр Павлович вырос в Москве, в 1973 г. окончил Высшую школу КГБ СССР, факультет засекреченных систем связи по специальности «прикладная математика» и как инженер-математик в звании лейтенанта был направлен в 8 Главное управление КГБ СССР, в котором занимался разработкой отечественных криптографических систем. В звании генерал-лейтенанта в 2011 г. демобилизован.

Является одним из ведущих специалистов по защите информации, разработал и реализовал ряд сегментов современной концепции обеспечения компьютерной безопасности в России, за что был удостоен в 1976 Премии Ленинского комсомола, а в 1998 и 2008 годах Премий Правительства России в области науки и техники. В 1983 г. защитил диссертацию кандидата физико-математических наук, в 2006 г. — доктора физико-математических наук, действительный член (академик) Академии Криптографии Российской Федерации.

В настоящее время является заведующим кафедры информационной безопасности НИУ ВШЭ, заместителем Генерального директора по информационной безопасности Федеральной налоговой службы России.

Александр Павлович любезно согласился ответить на наши вопросы.

Александр Павлович, в чем, на Ваш взгляд, состоят на сегодняшний день наиболее актуальные проблемы в сфере обеспечения информационной безопасности программного обеспечения?

В сложившихся современных условиях автоматизация деятельности бюрократическо-управленческого аппарата является насущной необходимостью каждого развивающегося общества. Ожидания положительного эффекта от автоматизации известны. Однако, при выработке алгоритмического описания деятельности организации техническим специалистам (алгоритмистам) приходится переводить, так сказать, гуманитарные представления и действия в последовательность с конечным числом операций. Затем эта последовательность программируется для исполнения в ЭВМ, и тем самым фиксируется деятельность административного органа в соответствии с утвержденным для него регламентом функционирования. Сложность заключается в том, что специалисты с гуманитарным образованием с большим трудом могут соотнести регламент действий с предложенной им последовательностью операций, имеющей, как правило, разветвления и циклы. Собственно, эту проблему можно назвать валидацией алгоритмического описания регламента. Весьма часто для получения адекватного алгоритмического описания приходится трансформировать регламент, а иногда и саму деятельность органа. Ясно, что если алгоритм противоречит регламенту, то и предназначение органа меняется.

Но ведь проблемы могут возникать и на этапе разработки программного обеспечения?

Да, безусловно. Следующим этапом преобразования алгоритма непосредственно в программное обеспечение (ПО) является применение средств «быстрого « создания исполняемого кода на основе применения так называемых «кейс-технологий» типа SAP, Oracle Business Suite и др. Эти технологии многократно ускоряют процесс выработки эффективного программного обеспечения и упрощают отладку исполняемого кода. Сертификация кейс-технологий по вопросам отсутствия в блоках-кейсах НДВ, а также в способах их стыковки является важной задачей, без которой ускоренная автоматизация управленческой деятельности в массовом масштабе невозможна. Сложность сертификации заключается в наличии большого числа самих блоков (от ста тысяч до не-

скольких миллионов для разных систем), а также в целесообразности проверки длинных (более чем три) цепочек стыковки. Тем не менее, подобная работа уже ведется, например, по SAP, и очевидно будет носить поэтапный характер.

Это основная трудность, связанная с верификацией программного обеспечения?

Не только. Основной проблемой верификации ПО на современном этапе является его объемность. Автоматизация работы ведомства или, точнее, ее компьютеризация, в сочетании с внедрением автоматизированных процедур (не путать с автоматическим, то есть без участия человека, выполнением процедур) приводит к созданию и дальнейшей эксплуатации ПО объемами 1 Гбайт и более. «Ручная» верификация таких объемов ПО невозможна и, в свою очередь, конечно, требует автоматизации. Автоматизированной проверке по определенным критериям может быть подвергнуто как ПО в исходных (высокоуровневых) текстах, так и в виде исполняемого кода.

Но ведь существуют средства автоматизации таких проверок?

Да, разработано несколько систем автоматизации проверки на определенные типы НДВ. Было бы целесообразно как-то сертифицировать эти системы проверок, а возможно и санкционировать только их применение, например, для невысоких уровней сертификации и применения ПО. Ясно, что от целенаправленной разработки и внедрения НДВ такой метод не защитит, но непреднамеренные недоработки, тупиковые ветви, переполнения регистров, забытые отладочные люки и т.д. могут выявляться и затем весьма эффективно исправляться.

То есть эффективность применения таких средств, на Ваш взгляд, невысока?

В целом, приходится с прискорбием констатировать, что теории верификации ПО до настоящего времени не создано, равно как отсутствует и научно обоснованная методология гарантированного обеспечения информационной безопасности (ИБ) ПО. Разрабатываемые и предлагаемые в ряде работ модели расчетов надежности верификации ПО сами не прошли реальную верификацию, как и модели получения количественных оценок ИБ ПО.

Видимо, в этой области знания происходит процесс накопления экспериментальных данных, не перешедший еще даже в стадию научной классификации.

В чем, по Вашему мнению, состоит специфика защиты от несанкционированного доступа к информации для облачных технологий?

Без опасения можно сказать, что современные «облачные» технологии построены на принципах виртуализации. Эти принципы были известны и разработаны еще в прошлом столетии, причем, даже не в конце его. Однако, в современных программно-аппаратных реализациях они приобрели новые свойства и новые масштабы, которые порождают новые вопросы, не имевшие существенного значения или легко решавшиеся ранее в малых системах.

ПЕРВАЯ проблема заключается в сложности и нередко громоздкости собственно самой программной платформы виртуализации и системы управления ею в масштабе тысяч серверов реализуемых в кластере при эмуляции десятков серверов на каждом «лезвии». Задачу сертификации можно начинать решать исследованием архитектурных принципов построения компонент виртуализации основных платформ и выделением критических для обеспечения ИБ узлов. Множества и содержание узлов могут быть различны в зависимости от сертификации устойчивости к тому или иному классу атак. Выигрыш заключается, во-первых, в возможности поэтапной сертификации, а во-вторых, в сокращении объемов исследуемого ПО. Изучать надо только то ПО, которое обеспечивает надлежащее функционирование критических узлов. По опыту исследования крупных программных платформ можно констатировать, что объем тестируемого ПО может оставлять 5-10% от общего массива.

ВТОРОЙ, нерешенной, проблемой обеспечения ИБ «облачных» технологий является отсутствие сертификации эффективных систем управления базами данных (СУБД) и, соответственно, аттестованных сверхвысокоемких хранилищ данных, основанных на Oracle, ECM и т.д. Производители этих СУБД отказывают в предоставлении детальных архитектурных описаний СУБД и исходных текстов пакетов ПО, необходимых для проведения сертификационных исследований на отсутствие НДВ. Исключение составляет только Microsoft Server, эффективность которого для больших кластеров еще недостаточно подтверждена. Продолжение разработок

защищенных хранилищ данных, сравнимых по эффективности с Exadata или Teradata, является общенациональной задачей, без решения которой применение перспективных «облачных» вычислений в критических технологиях проблематично.

ТРЕТЬЕЙ, решаемой в настоящее время, проблемой является создание защищенных мобильных офисов, использующих различные виды телекоммуникаций в совокупности, то есть на одном рабочем месте могут быть использованы в зависимости от условия расположения различные виды связи по технологиям LTE, GSM, Wi-Fi и пр.

Как на сегодняшний день обстоят дела со стандартизацией и взаимной совместимостью криптографических решений разных производителей?

Повышению общего уровня ИБ современных технологий способствовала бы дальнейшая стандартизация криптографических примитивов и принципов реализации шифрованной связи. Удалось достигнуть состояния возможности взаимопроверки квалифицированной ЭП разных производителей. Однако, шифрованный IP - пакет одного производителя криптопровайдера не может быть расшифрован криптопровайдером другого. Поэтому в автоматизированных системах, ориентированных на массового пользователя, приходится поддерживать в актуальном состоянии целый ряд криптопровайдеров. Ситуация осложняется еще и тем, что при модернизации или даже «патчировании» (установки новых патчей) необходима либо доработка каждого криптопровайдера, либо их замена. Эксплуатация подобных систем увеличивает издержки и приводит к применению несертифицированных средств криптографической защиты. Очевидно, что наличие нескольких криптопровайдеров «на борту» персонального компьютера пользователя можно обнаружить только у энтузиастов либо у профессионалов ИБ. Причины такой ситуации известны и заключаются в «глубоком», а также самостоятельном и нестандартном встраивании криптоуслуг в работу операционной системы (ОС). Выход может содержаться в стандартизации интерфейсов и функций криптопровайдеров. В целом, институт стандартизации криптосистем, ориентированных на массового пользователя, нуждается в развитии не только по алгоритмам и параметрам криптосхем, но и по функционалу применения как услуги.

Возможно, положительную роль здесь могла бы сыграть сертификация соответствующего программного обеспечения?

Общеизвестно требование регулятора о необходимости сертификации ПО при использовании криптографических функций. Оно проистекает из возможности неправильного применения сертифицированных криптопримитивов. Проверка корректности встраивания, то есть выполнения условий применения сертифицированных криптофункций, возложена на специальные лаборатории, имеющие специальные лицензии.

Насколько сложна эта процедура для заказчика?

Для небольшого прикладного ПО, объемом, скажем, высокоуровневого кода до 100000 строк, эта проблема может быть решена за 1 - 2 месяца. Однако, если производится модернизация ПО, проверка корректности встраивания должна повторяться. Для большого ПО (в несколько миллионов строк) трудоемкость этой задачи может возрастать пропорционально, например, в 10 раз. Тогда для такого ПО, к тому же еще и изменяемого хотя бы один раз в год, задача проверки корректности встраивания не имеет решения, либо требует привлечения весьма и весьма больших ресурсов экспертов. Отмеченная проблема усугубляется многократным применением ЭП различными блоками ПО в процессе его функционирования.

Другим осложнением является отсутствие исходных текстов для некоторых блоков ПО, что еще более затрудняет анализ корректности встраивания. Некоторые производители из-за опасений потери авторства отказываются предоставлять полные высокоуровневые тексты ПО, чем провоцируют отказ от применения криптосредств, в частности, электронной подписи как эффективного средства идентификации пользователя или процесса.

Как Вам видится решение этой проблемы?

Представляется, что для решения перечисленных проблем надо либо отказаться от экспертизы корректности встраивания, возложив ее на производителя ПО без специального лицензирования, либо предложить методы изготовления прикладного ПО, гарантирующие сразу же только правильное использование криптопримитивов. В последнем случае проверяется только применение метода, да и то самим производителем ПО.

Сложность этого подхода заключается в большом разнообразии методов реализации алгоритмов в виде ПО.

Александр Павлович, как именно на сегодняшний день осуществляется оценка надежности защиты информации при реализации криптографических функций?

При построении криптографических средств защиты информации (КСЗИ) одним из требований регулятора - ФСБ России - является проверка корректности встраивания уже сертифицированных и реализованных в виде ПО криптографических примитивов (КП) или криптобиблиотек. Это делается для повышения надежности работы системы в целом как совокупности прикладного ПО и КП. В большинстве случаев при обработке информации, не содержащей государственной тайны, модель угроз ИБ для системы исходит из того, что пользователь не пытается извлечь и скопировать ключи шифрсистем, а также целенаправленно не модифицирует прикладное ПО для «обхода» или компрометации КП. Однако, в ряде «контрольных» систем, таких как учет алкогольной продукции, транспортной нагрузки на грузовой автомобиль или контрольно-кассовой техники, пользователь этой техники должен рассматриваться в качестве одной из реальных угроз для корректной работы криптопримитивов, а также утечки или подделки передаваемой информации.

Как именно владелец или пользователь техники может реализовать такую угрозу?

С целью компрометации КСЗИ владелец средства может предпринимать различные действия, включая передачу КСЗИ для исследования весьма квалифицированному инженерно-исследовательскому персоналу. В таких условиях актуальными становятся задачи определения защиты информации, сформулированные в требованиях для категорий КВ 1, 2 и КА 1, которые предполагают исследования побочных сигналов от работающих криптосредств и обеспечения определенной надежности штатного функционирования КП в условиях стимуляции сбойных ситуаций различной природы.

Модель приема побочных излучений формулируется как процедура распознавания опасного информативного сигнала на фоне помех. Наличие конфиденциальной информации в побочном излучении составляет угрозу безопасности защищаемой системы. Поэтому углубление исследований в области приема и обработки сигналов от функционирующей техники, обрабатывающей конфиденциальные сведения, является актуальной задачей. Особое значение этому направлению придает удешевление средств приема и обработки электромагнитных излучений. Ранее доступные только узкому кругу специалистов комплексы «прием и оцифровка сигналов в сопряжении с ЭВМ» сейчас достаточно дешевы и обеспечивают высокие значения параметров чувствительности антенн, а также обработки больших массивов информации. Возможность реализации сложных процедур обработки оцифрованных данных ставит вопрос об оценке эффективности оптимального приема сигналов в различных моделях зашумления. К таким моделям относится многоканальный прием и совместная адаптивная обработка коррелированных наблюдений.

Александр Павлович, спасибо за содержательное интервью по животрепещущим вопросам информационной безопасности. В завершении нашей беседы разрешите задать наш традиционный вопрос – что бы Вы хотели пожелать читателям нашего журнала?

Лично читателям настоятельно рекомендую использование криптографических средств защиты хранимой и передаваемой информации!