ЗАЩИТА ИНФОРМАЦИИ

Безопасность информации в государственных информационно-телекоммуникационных системах в опасности!

А.А. Гусаров

генеральный директор ЗАО "Телрос"

Современный этап развития нашего государства характеризуется тем, что наряду с расширением созидательных устремлений личности и общества интенсивное развитие информационно-телекоммуникационных систем создает предпосылки для реализации угроз национальной безопасности, связанных с осуществлением враждебных и других преступных действий по нарушению установленных режимов их функционирования на основе использования возможностей современных информационных технологий [1].

Оснований для такого утверждения более чем достаточно. Прежде всего, следует отметить происшедшее в последнее время возвышение в политическом руководстве США выходцев из разведслужб. Так главой Национального директората разведки США назначен отставной адмирал Джон Майкл "Майк" Макконел, который ранее был директором Агенства национальной безопасности (АНБ) США (1992–1996), пост директора ЦРУ занял генерал Майкл Хейден, до этого 6 лет возглавлявший АНБ (1999–2005). Указанные назначения недвусмысленно свидетельствуют о явном усилении позиций разведслужб в американской госадминистрации и, что особенно характерно – инфотехнологического направления.

Стремительное и динамичное развитие информационно-телекоммуникационных технологий ставит перед разведывательными службами промышленно развитых государств в качестве одной из приоритетных задач установление контроля за "чужими" государственными информационными системами, в первую очередь, за той информацией, которая в них циркулирует, а также за программным обеспечением (ПО) их технических средств.

Подтверждением указанного предположения является сообщение о том, что официальные лица США открыто признали факт тесного сотрудничества в сфере безопасности разрабатываемого ПО между АНБ и главной софтверной компанией. В частности, речь идет о совместной работе Microsoft и Агентства национальной безопасности США над ОС Windows Vista [2].

Тот факт, что корпорация Microsoft на протяжении многих лет сотрудничает с АНБ США, секретом не является. Еще в конце 1990-х годов в Интернете появилась история о том, как один въедливый программист, изучая код подпрограмм в операционной системе Windows NT, обнаружил переменную с выразительным именем _NSAKEY ("ключ АНБ"). Какого-либо серьезного скандала из этой истории не получилось, поскольку для присутствия такой переменной нашли более или менее невинные объяснения, а название ради всеобщего спокойствия сменили на нейтральное _KEY2. Кроме того, именно АНБ, когда этого требовали американские законы, всегда способствовало снижению криптографической стойкости программных продуктов, предназначенных для экспортных продаж, что подтверждает наличие многолетних, но не афишируемых контактов Microsoft с Агентством национальной безопасности США.

Активное вмешательство разведывательных служб в использование телекоммуникационных сетей хорошо иллюстрирует крупный шпионско-политический скандал (2006) вокруг греческой сети сотовой связи Vodafone Greece, в котором были замешены АНБ США и его главный партнер в американской ИТ-индустрии - компания SAIC. В составе дирекции последней регулярно фигурируют бывшие высокие чины из разведслужб и Министерства обороны. Эта история в свое время подробно освещалась в прессе, здесь же подчеркнем, что тайная программная закладка, обеспечившая перехват и прослушивание мобильной связи всей военно-политической элиты Греции, была встроена в аппаратуру Vodafone Greece в процессе модернизации при подготовке к Олимпиаде-2004 в Афинах. Главным подрядчиком, строившим системы безопасности для афинской Олимпиады, была американская фирма SAIC. Когда независимая греческая пресса раскрыла эту шпионскую историю и опубликовала имена сотни лиц, "стоявших на прослушке", то в списке помимо высшего политического руководства Греции фигурировали также греческие партнеры SAIC по афинским контрактам и военные чины, ведающие закупками вооружений для греческой армии. После публикации списка этим военным стали совершенно понятны причины поразительной удачливости их американских партнеров по переговорам, каждый раз добивавшихся максимально выгодных для себя условий сделок.

Другой пример связан со скандалом швейцарской компании Crypto AG, в ходе которого вскрылось внедрение в программное обеспечение закладки, снижавшей криптостойкость средств, поставляемых в ряд стран.

Приведенные факты свидетельствуют о том, что в современных условиях под различными, в том числе и такими, как борьба с терроризмом, предлогами разведывательными службами промышленно развитых государств и, в первую очередь США, предпринимаются серьезные усилия для установления тотального контроля над информационно-телекоммуникационными системами других стран.

К сожалению, в настоящее время в России для реализации указанных планов складывается весьма благоприятная обстановка. В течение последних десятилетий нашей стране целенаправленно навязывалась западная политика в области создания и внедрения средств телекоммуникации. Для этого были созданы соответствующие условия по приватизации и передаче в иностранные руки подавляющей части пакетов операторских компаний. В интересах иностранных компаний перераспределены частотные ресурсы, созданы условия для ввоза иностранной техники связи и вложения денежных средств. На фоне повсеместного внедрения мобильной связи ведущих мировых операторов в значительной мере были свернуты собственные научные исследования в области телекоммуникаций, а научные центры по их разработке переориентированы в центры сертификации иностранного оборудования.

Среди множества проблем, связанных с использованием информационно - телекоммуникационных систем, особо следует выделить критическую зависимость отечественной информационной инфраструктуры от поставок образцов зарубежной информационно-телекоммуникационной техники, а также несоответствие темпов разработки и внедрения средств и способов защиты информации динамике изменения спектра угроз безопасности информации и росту интенсивности их применения.

В этих условиях чрезвычайно важной представляется практическая реализация таких положений "Доктрины информационной безопасности Российской Федерации", как развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, а также защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем как уже развернутых, так и создаваемых на территории РФ [3].

Альтернативы указанным выше направлениям деятельности нет. Только при условии государственного подхода к решению проблемы обеспечение безопасности информации в информационно-телекоммуникационных системах в РФ могут быть созданы условия для адекватного противодействия возросшим угрозам в информационной сфере.

Одним из значимых шагов в реализации приведенных положений Доктрины следует рассматривать принятие Госдумой Федерального закона от 09.02.2007 №14-ФЗ, основные положения которого направлены на обеспечение целостности, устойчивости функционирования и безопасности сети связи общего пользования посредством регистрации сетей связи и оценки соответствия установленным требованиям проектной документации путем проведения экспертизы [4].

Заслуживает внимания также инициатива депутата Госдумы РФ Ю.Г. Медведева по внесению на рассмотрение проекта закона "О безопасности информации критически важных объектов информационной и телекоммуникационной инфраструктуры Российской Федерации". В этом документе предлагается реализацию мер по обеспечению безопасности информации указанных объектов, включая функционирующие в их составе ключевые информационно-телекоммуникационные системы, возложить на субъекты информационной и телекоммуникационной инфраструктуры. Осуществлять эти меры следует как самостоятельно с обязательным привлечением специализированных организаций, имеющих лицензии на соответствующие виды деятельности, так и с участием федеральных

органов исполнительной власти, уполномоченных в областях обеспечения безопасности информации в ключевых системах информационной инфраструктуры, внутренних дел, по контролю и надзору в системах связи, обеспечения безопасности и обороны государства.

Наряду с государственным подходом на суд общественности, в отдельных случаях, выносятся и другие суждения. В частности, по заявлению директора по информационной безопасности кабинета Президента Microsoft в России и СНГ Мамыкина обращение группы ученых и политиков к российской верховной власти с предложением поддержать поправку в законодательство о недопустимости использования зарубежных программ и технических средств в стратегических отраслях и особо важных объектах Российской Федерации. Свою позицию г-н Мамыкин обосновывает тем, что в нашей стране якобы отсутствуют отечественные операционные системы, базы данных, технологии для изготовления современных компьютеров, а также тем, что наша страна не производит современные цифровые автоматические телефонные станции [5]. Таким образом, по мнению указанного специалиста от Microsoft, для использования в России исключительно зарубежных технических средств альтернативы нет.

Позиция таких специалистов как г-н Мамыкин понятна. Они представляют интересы зарубежных фирм и, естественно, отстаивают их интересы.

Реальное состояние дел не столь пессимистично. Многие государственные предприятия и коммерческие структуры активно занимаются разработкой IT технологий и телекоммутационного оборудования. Кроме того, серьезные основания для воплощения в жизнь основных положений "Доктрины информационной безопасности Российской Федерации" в части разработки отечественного программного обеспечения и современных средств информатизации, телекоммуникации и связи дает, в частности, внимание первых лиц государства к этой проблеме. Так, во время посещения Зеленограда в октябре 2006 года Президент Российской Федерации В.В. Путин вновь обратил внимание специалистов на необходимость активного развития рынка информационных технологий. Активизировать рост инновационной экономики Путин предложил за счет создания центров научной информации.

Что касается проблемы обеспечения безопасности информации, то, прежде всего, следует особо подчеркнуть, что в нашей стране сформирована государственная системы защиты информации [6]. В организационном плане государство создало нормативно-правовую базу в области защиты информации, определило предмет защиты, правила категорирования информации по уровню доступа. При этом информационные ресурсы, являющиеся собственностью государства, находятся в ведении органов государственной власти и организаций и в соответствии с их компетенцией подлежат учету и защите, а режим защиты информации конфиденциального характера устанавливается собственником информационных ресурсов или уполномоченным лицом в соответствии с действующим законодательством.

При всей масштабности работы по защите информации, проведенной в последние годы с привлечением ученых и ведущих специалистов, основное внимание в ней уделялось обеспечению безопасности информации в автоматизированных системах на основе средств вычислительной техники и сетях передачи данных. Вопросам же защиты информации, циркулирующей в телекоммуникационных сетях и, в особенности, в учрежденческих АТС (УАТС) внимания уделялось недостаточно.

Главной угрозой для пользователей УАТС импортного производства, как и другого аналогичного оборудования, является возможность несанкционированного доступа к его программным портам со стороны сетей общего пользования (так называемый "полицейский режим").

При этом, такой доступ может быть инициирован из различных центров, в том числе и расположенных на значительном удалении (зарубежных центров) от объектов наблюдения, в частности, по открытому каналу сервисного обслуживания. Наличие недекларированных возможностей в программном обеспечении ("программных закладок") импортных УАТС обеспечивает успешную реализацию акций нарушителей.

Возможность скрытного доступа к УАТС превращает ее в мощное средство перехвата статистической и другой информации (включая прослушивание разговоров, совещаний и др.), управляемое дистанционно. По командам, скрытно передаваемым на фоне другой информации в каналах связи, УАТС переключается в режим сбора, накопления и замаскированной передачи информации на заданные номера телефонов, становясь, таким образом, эффективным техническим средством разведки.

Программные и аппаратные закладки, реализующие упомянутые функции, весьма сложно выявить, особенно с учетом того, что ни один иностранный производитель не передает для анализа ни принципиальных схем, ни исходных текстов программного обеспечения. В таких условиях трудоемкость поиска закладок становится соизмеримой с разработкой нового аналогичного оборудования, а зачастую и превышает ее. Кроме того, дистанционная "перезаливка" программного обеспечения фирмой-разработчиком по каналам связи, ставшая практической нормой эксплуатации, не позволяет определить, какие модули ПО в текущий момент исполняются в оборудовании. В этих условиях органы государственной власти, предприятия ОПК, другие предприятия и учреждения, использующие УАТС иностранного производства,

рискуют стать легкодоступным источником информации для иностранных технических разведок.

Решение проблемы защиты информации в УАТС дополнительно осложняется еще и тем, что нормативная база, разработанная применительно к обеспечению безопасности информации УАТС, явно недостаточна. Федеральные органы исполнительной власти для сертификации УАТС используют руководящие документы, разработанные либо для средств вычислительной техники, либо для автоматизированных систем управления. Ни один из используемых документов не отражает в полной мере особенностей УАТС как источника угроз утечки информации. В связи с этим периодически появляющиеся в средствах массовой информации сообщения о сертификации того или иного иностранного оборудования, ко всему еще проведенной в условиях ограниченного доступа к исходным текстам программного обеспечения, в какой-то мере позволяют сделать вывод о снижении риска утечки информации, но не могут служить гарантией ее полной безопасности.

Кардинальным решением проблемы утечки информации по каналам телефонной связи могло бы стать введение ограничений на применение техники связи импортного производства на предприятиях и в учреждениях, деятельность которых представляет интерес для спецслужб других стран. Однако такой подход трудно реализуем.

Более продуктивным следует рассматривать разработку новых и совершенствование существующих нормативно-правовых актов и документов по обеспечению безопасности информации УАТС, а также активизацию работ по созданию технических средств защиты информации в телекоммуникационных сетях.

Воспрепятствованию добывания спецслужбами иностранных государств информации путем НСД к УАТС может способствовать реализация мероприятий, перечисленных ниже, в частности:

– руководствуясь требованиями ст. 43.1 Федерального закона от 09.02.2007 года №14-ФЗ, целесообразно разработать и ввести в действие “Положение об обязательной сертификации по требованиям безопасности импортного телекоммуникационного оборудования, планируемого к установке на критически важных объектах информационной и телекоммуникационной инфраструктуры”;

– комплект специальных нормативных документов по технической защите информации ФСТЭК России необходимо дополнить “РД. Безопасность информации в телекоммуникационных сетях. Положение об учрежденческих АТС в защищенном исполнении”;

– необходимо спланировать проведение ряда НИОКР, направленных на разработку технических решений по ограничению доступа из общих сетей связи к УАТС критически важных объектов в виде интеллектуальных телекоммуникационных экранов, на разграничение прав пользователей, сбор, обработку и анализ трафика.

Практическая реализация перечисленных выше, как равно и других мер, направленных на повышение уровня безопасности информации в УАТС, при координирующей роли соответствующих федеральных органов исполнительной власти будет способствовать обеспечению сохранности не только государственных и производственных секретов, но и интеллектуальной собственности государства, общества и личности.

Литература

1. Информационная безопасность систем организационного управления: Теоретические основы/ Под ред. Н.А. Кузнецова и В.В. Кульбы. – М.: Наука, 2006. – т. 1, 2.
2. Берд К., Секретное оружие АСБ. //Компьютеры.–2007.–№1.
3. Доктрина информационной безопасности Российской Федерации, 2000.
4. Федеральный закон от 09.02.2007 года №14-ФЗ “О внесении изменений в Федеральный закон “О связи”, 2007.
5. “Information Security//Информационная безопасность”