**Интернет под колпаком спецслужб**

В последнее время ходят упорные слухи, что российские спецслужбы якобы собираются использовать компьютерную сеть для тотальной слежки за гражданами. Дескать, будет установлена спецаппаратура для контроля за перепиской по каналам Интернета, а программа по считыванию информации уже несколько месяцев разрабатывается контрразведчиками совместно с сотрудниками телекоммуникационных компаний. Прокомментировать ситуацию согласился один из руководителей Федерального агентства правительственной связи и информации при президенте РФ (ФАПСИ), пожелавший, однако, сохранить инкогнито.

**Самое массовое оружие XXI века**

На наших глазах создается единое мировое информационное пространство, центром которого становится глобальная компьютерная сеть Интернет. Ее пользователи - частные лица, организации и целые государства. Наряду с положительными такой процесс несет в себе и отрицательные моменты. Во-первых, за счет лидерства в этой области отдельные страны осуществляют глобальный информационный контроль над мировым сообществом и фактически навязывают свои правила жизни. Многие государства вынуждены даже принимать специальные меры, чтобы защитить национальную культуру, традиции и духовные ценности. Во-вторых, анализ мирового опыта показывает, что в связи с интенсивным продвижением технологий резко усилилась опасность несанкционированного вмешательства в работу информационных систем. Наиболее развитые страны, банки, фирмы и предприятия стали в определенном смысле заложниками своих информационных систем. Специалисты едины во мнении, что разрушение и дезорганизация информационной инфраструктуры государства по силе воздействия соизмеримы с последствиями применения оружия массового поражения. Отсюда и берет начало понятие "информационное оружие", опасность использования которого особенно возрастает в XXI веке. Этим термином эксперт из ФАПСИ называет проникновение в информационно-телекоммуникационные системы страны иностранных спецслужб с целью хищения, искажения или уничтожения информации. В США, к примеру, на подготовку и проведение подобных мероприятий ежегодно выделяется около 2 млрд. долларов. Всего же расходы на реализацию концепции информационной войны до 2005 года составят свыше 18 миллиардов. В России переход к рыночным экономическим отношениям, построение нового правового поля вызвали необходимость срочного совершенствования информатизации всех аспектов государственной и экономической деятельности. В условиях технологического отставания отечественной промышленности это привело к массовому ввозу в страну современных средств коммуникации и переходу от хорошо защищенных, но обладавших низкими сервисными качествами систем шифрованной связи к вновь создаваемым информационным системам. А они хоть и предоставляют пользователю более широкий спектр услуг, но менее защищены и более подвержены воздействию информационного оружия. Таким образом, могут возникнуть большие проблемы. Хорошей иллюстрацией нашего не столь далекого будущего служат данные, полученные по ту сторону Атлантики. По сообщениям Конгресса США, уже пресечено около 250 тыс. попыток хакеров прорваться через Интернет в компьютеры Пентагона. Масштабы этого явления оцениваются в Вашингтоне как непосредственная угроза национальной безопасности.

**Закон не дышло**

Итак, как же обстоят дела в нашем Отечестве? В соответствии с российским законодательством задача комплексной защиты информационно-телекоммуникационных систем, технических средств, информационно-аналитических сетей и баз данных органов государственной власти России возложена на ФАПСИ. Эта служба располагает данными о скрытых функциональных возможностях различных средств и методах перехвата данных, а также о деструктивных функциях, которые могут быть заложены в телекоммуникационные системы. Ведь попытки продвижения на российский рынок средств защиты информации, разработанных за границей, уже предпринимаются, однако практически все они учитывают интересы иностранных спецслужб. Кроме того, резкое обострение криминогенной обстановки в России привело к регулярному проникновению хакеров в компьютерные сети государственных органов. Все чаще перехватываются конфиденциальные сообщения, передаваемые средствами документальной электросвязи. Выкрадывается и уничтожается банковская информация и программное обеспечение систем электронных платежей. Отправляются фальшивые авизо, используются коды подтверждения достоверности межбанковских операций и возможности локальных сетей коммерческих банков. Активность, квалификация и вооруженность хакеров постоянно растут. Поэтому применение нестойких к дешифрованию средств криптографической защиты может привести к губительным последствиям для экономики страны. По оценке американских специалистов, снятие элементов защиты информации с компьютерных систем приведет к разорению 20 проц. средних компаний и 33 проц. банков в течение считанных часов, а 48 проц. более крупных фирм и 50 проц. банков потерпят крах через несколько дней. Необходима правовая база, которая регламентировала бы функционирование электронной связи и квалифицировала различного рода преступления информационного характера. Кстати, в сенатском подкомитете Конгресса США давно проводится регулярная работа по совершенствованию законодательной защиты информационных и телекоммуникационных систем страны от преступного воздействия. В частности, один из законопроектов в этой сфере предусматривает в качестве наказания для хакеров, сумевших добыть конфиденциальную коммерческую, экономическую или финансовую информацию, тюремное заключение сроком на 25 лет или штраф до 1 млн. долларов. Всего в США действуют не менее шести федеральных законов, направленных на борьбу с информационной преступностью. В Великобритании подобных законов пять, в Германии - четыре. В КНР введены специальные полицейские подразделения, осуществляющие контроль за работой соотечественников в Интернете. В России же до сих пор отсутствуют законодательные акты, которые могли бы гарантировать надежную защиту личности, общества и государства в области электронной информации. По словам нашего собеседника из ФАПСИ, организационно-правовая база обеспечения информационной безопасности ограничивается в нашей стране пока только Указом президента РФ "О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации". Этот документ, в частности, определяет меры, препятствующие распространению в стране криптографических средств, не обеспечивающих надежную защиту информации. Впрочем, и в таких условиях ФАПСИ провела объемную работу по лицензированию предприятий, организаций и фирм на право деятельности по защите информации. К настоящему времени выдано 46 лицензий. Сертифицированы различные типы шифрованных средств, предназначенных для защиты конфиденциальной информации и коммерческой тайны. Всего выдан 161 сертификат на эти средства.

**Еще одна компьютерная "страшилка"**

Летом этого года непреднамеренно, а вполне вероятно, что и сознательно, в Интернете произошла утечка двух документов. Это "Порядок внедрения системы оперативно- розыскных мероприятий в сетях документальной электросвязи" и "Технические требования к системе технических средств по обеспечению функций оперативно- розыскных мероприятий на сетях документальной электросвязи". ФСБ и Госкомсвязи даже не пытались скрыть свою причастность к этим проектам. Более того, представители указанных ведомств подтвердили, что в целях укрепления информационной безопасности государства они давно работают над возможностью доступа к потокам сетевых данных. Анализируя распространенные по Интернету документы, некоторые специалисты выразили опасение, что описываемые в них меры представляют угрозу свободе компьютерного общения, а по большому счету являются элементами тотальной слежки за гражданами. В частности, в ставших объектом интернетовской гласности материалах содержится пункт, который позволяет силовым ведомствам тайно снимать информацию с электронного оборудования провайдера. Эта техническая операция якобы станет возможной при помощи "черных ящиков", которые должны быть установлены на аппаратах пользователей для передачи необходимой информации прямо на компьютеры ФСБ. Появились также сообщения, что за установку "черных ящиков" для контроля за электронной перепиской придется заплатить самим провайдерам. По их оценкам, такая приставка обойдется примерно в 15-20 тыс. долларов. Если же возникнет необходимость "спонсирования" прокладки для ФСБ так называемого толстого канала, то сумма затрат достигнет сотен тысяч долларов. В целом вывод некоторых экспертов таков: в случае реализации системы оперативно- розыскных мероприятий в Интернете ФСБ получит мощный инструмент слежки за гражданами, а провайдеры и их клиенты будут оплачивать эту слежку из своего же кармана. Комментируя ситуацию, наш собеседник заявил, что говорить об установлении контроля за перепиской по электронной сети как о свершившемся факте преждевременно. По его словам, идет лишь процесс поиска приемлемых форм и способов усиления защиты телекоммуникационных систем и информационной безопасности. Попавшие в Интернет документы - это рабочие проекты, в которых содержится обсуждение технической стороны вопроса. О возможных расходах на осуществление такой программы речь и вовсе не шла. В то же время опыт показывает: нельзя руководствоваться принципом абсолютной свободы в Интернете. В этом контексте уместно процитировать недавнее высказывание директора ФСБ Владимира Путина: "Конечно, ФСБ не собирается брать Интернет под контроль, но мы имеем в виду, что современные средства телекоммуникации могут быть использованы во вред безопасности страны. Мы должны строить свою работу так, чтобы потенциальный противник не мог спокойно получать закрытую информацию через Интернет". Подключение к глобальной сети само по себе не создает никаких принципиально новых проблем в области информации. Основными опасностями при пользовании Интернетом являются следующие: ? несанкционированный доступ внешних пользователей к какому- либо виду сервисного обслуживания; - доступ к информации и базам данных российских организаций без идентификации внешнего пользователя, включая проникновение к ресурсам абонентов с целью съема информации, ее разрушения или искажения; - перенос (импорт) в системы и сети российских организаций разрушающего программного обеспечения; нарушение конфиденциальности информационного обмена по каналам связи абонентов систем и сетей.

**"Колпак": сделано в сша**

Не секрет, что спецслужбы США охотятся за сведениями об информационно- телекоммуникационных комплексах других стран. Активно участвуя в развитии мировой информационной инфраструктуры, они проводят привлекательную ценовую политику, создают удобные для пользователей информационные технологии, разрабатывают американские стандарты, которые становятся впоследствии международными. Уже сейчас США закладывают маршруты информационных потоков, которые могли бы контролировать американские спецслужбы. Кроме того, получены данные, что там начали реализовывать программу контроля точек входа в Интернет, фиксируя корреспондентов, обращающихся через эту систему к американским информационным базам. Основной мерой противодействия этой опасности при подключении российских организаций к Интернету, по нашему мнению, должна стать защита информационного управления государством. Эту задачу по поручению президента и решает ФАПСИ, создавая и развивая информационно-телекоммуникационную систему специального назначения (ИТКС). Ее принципиальное отличие от других подобных систем - обеспечение надежной защиты циркулирующего сетевого потока информации. ИТКС основана на применении в сетях и абонентских пунктах пользователей стойких криптографических средств, которые в сочетании с применяемыми организационно- режимными, программно-техническими и специальными мерами позволяют обеспечить комплексную защиту информации. Принято также решение о создании в ФАПСИ узла международной ассоциации компьютерных сетей Интернета. В данном узле должны быть реализованы функции защитного шлюза между компьютерными сетями России и международными информационными системами. Насколько эффективны разрабатываемые сейчас меры информационной защиты, покажет время.

**Список литературы**

Миронов Виктор. Интернет под колпаком спецслужб