От электронного рабства пора избавляться

КАК БОРОТЬСЯ С ЦИФРОВЫМИ УГРОЗАМИ

«Информационная безопасность органов государственного и военного управления, правоохранительных органов, предприятий и организаций военно-промышленного комплекса» — тема межрегиональной конференции, которую 24 февраля организует представительство Комитета Государственной думы по обороне в СЗФО. Законодательные инициативы и конкретные рекомендации, выработанные на конференции, будут полезны как специалистам в области защиты информации, так и всем интернет-пользователям.

ВКЛЮЧАЯ компьютер или даже смартфон, путешествуя по Интернету, вряд ли кто задумывается, что всю переписку, все данные, которыми мы оперируем, без особого труда могут прочитать… не ФСБ и другие российские спецслужбы, а создатели используемой нами цифровой техники и программного обеспечения, прочно связанные с западными разведками. Недаром эффект разорвавшейся бомбы во всем мире вызвали разоблачения Сноудена, раскрывшего глобальную сеть электронного шпионажа со стороны США. А информация, которой обмениваются российские власти, конструкторские бюро и предприятия оборонно-промышленного комплекса, — вожделенная и, увы, легкая добыча для охотников за нашими секретами.

Константин Лысов.

Как показывает практика, охотнее всего (85% случаев) воруют персональные данные и клиентские базы — их можно без труда продать. Далее, по числу утечек (их количество год от года растет), следуют коммерческие и государственные тайны.

Наталья Касперская.

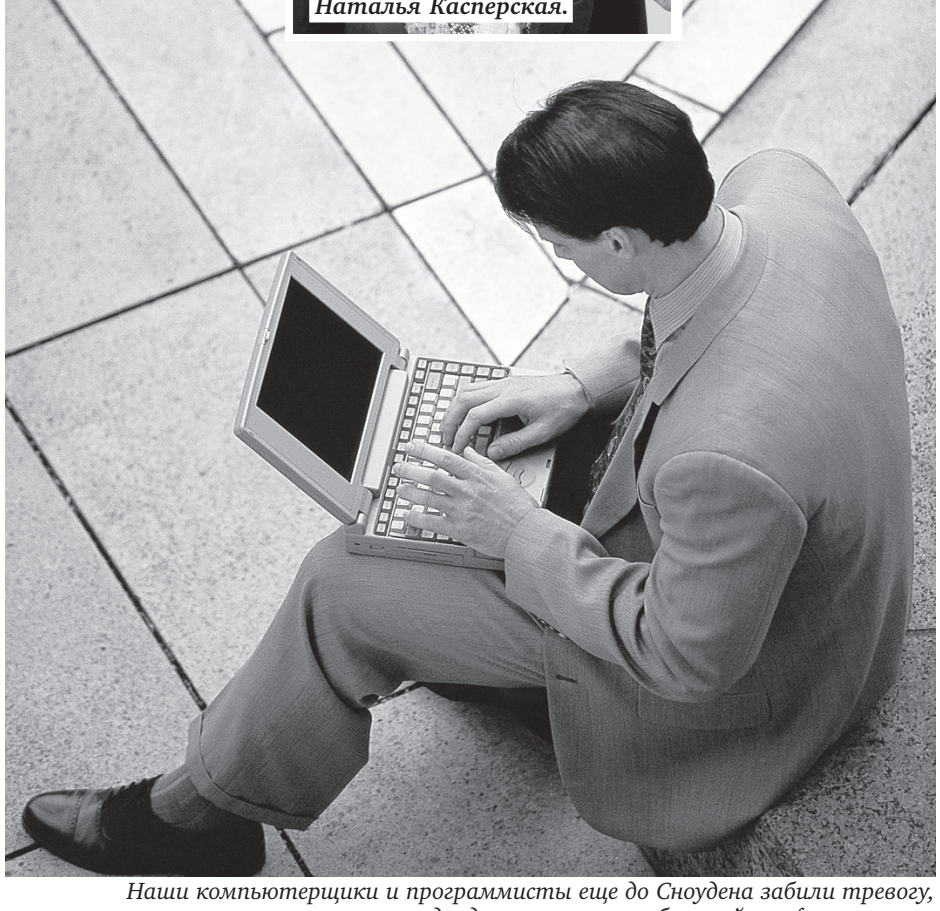
Пока Россия безропотно кормила Европу нефтью и газом, нас гладили по головке, при этом окольцовывая натовскими военными базами. Но как только мы заявили о своих национальных интересах, на нас тут же обрушили море санкций, в первую очередь застопорив поставки наукоемкой техники и технологий.

Между прочим, наши компьютерщики и программисты еще до Сноудена забили тревогу, предвидя опасности глобальной «цифровизации». Их долго не слышали, им не хотели верить. Но они продолжали работать, за свой счет создавая системы защиты от электронного рабства. В частности, с новейшими и эффективными разработками в сфере информационной безопасности участников конференции познакомит генеральный директор группы компаний «Info Watch» Наталья Касперская. Этот холдинг, объединяющий создателей отечественного программного продукта, наряду с партнерами из компетентных госструктур постоянно отслеживает развитие мировой компьютеризации с точки зрения реальных угроз национальной безопасности России.

Сегодня специалисты фиксируют нарастание опасных тенденций. Среди них — участившиеся утечки информации и кибершпионаж, резкое увеличение целевых атак на конкретные предприятия и очаговое распространение вредоносного программного обеспечения, недостаточная защищенность «облачных хранилищ» информации и смартфонные вирусы, информационные войны через социальные сети и сбор информации о гражданах России в пользу других стран. А еще существуют проблемы, связанные с защитой АСУ ТП, наличием в программах недекларированных возможностей, так называемых «закладок», и так далее…

Если в 2006 году было выявлено 200 случаев утечки информации, то в 2013-м уже 1500. Это только то, что просочилось в открытую печать на русском и английском языках.

Новая угроза — целевые вирусные атаки, которые во много раз опаснее рядовых вирусов. Вирус поражает пользователей наудачу. Это своего рода стрельба из пушки по воробьям: массовые «обстрелы» территорий — куда-нибудь да попадет. Что делать с ними, пока неясно: антивирусники на данном этапе не справляются.



Наши компьютерщики и программисты еще до Сноудена забили тревогу, предвидя опасности глобальной «цифровизации».

Целевые вирусные атаки «официально» стартовали в 2010 году. Над первым вредоносным продуктом несколько лет трудился могучий коллектив американских и израильских спецслужб. И хотя пилотная атака была направлена против ядерных объектов Ирана, киберэпидемия расползлась и по компьютерам обычных пользователей 12 стран. Любопытная деталь: вирус был обнаружен в 2010 году, но оставался незамеченным в сетях целых три года. Такого провала антивирусные компании еще не знали. С тех пор география атак неизменно расширяется, а их сложность становится более «убийственной». Притом что никуда не делась и проблема вирусов как таковых, и списывать антивирусы в утиль еще рано.

Лаборатория Касперского утверждает, что за последний год заблокировала 6 млрд. вирусных программ, «Panda Security» говорит о ежедневном обнаружении 160 000 вредоносных программ, «Symantec» подсчитал, что на вирусные атаки приходится уже одно из 431 электронного письма, «McAfee» считает, что за первый квартал 2014 года число программных «сюрпризов» превысило 200 миллионов.

Все оценки свидетельствуют: число вредоносных программ исчисляется миллиардами. Вручную никакими силами столько не напишешь. Созданы автоматические генерации вирусов, которые эти продукты производят и выпускают в свет. 99,9% отбрасывается антивирусными программами, но достаточно и той доли процента, которая проникает, поскольку это все равно огромное число.

Пугает и вредоносное программное обеспечение для мобильных устройств (сотовые телефоны, планшеты и прочие девайсы). Между основными платформами вирусы распределяются в следующей пропорции: 18% — айфон, 70% — андроид. Андроид — открытая платформа, под нее уже написано несколько десятков миллионов приложений, среди которых есть и вредоносные. По данным Лаборатории Касперского, за 10 месяцев 2014 года обнаружено 259 тысяч мобильных вирусов.

В настоящий момент примерно 32% трудоспособного населения России пользуются импортными смартфонами. Это значит, что заокеанским корпорациям в каждый момент времени известно местоположение 30 млн. российских граждан с точностью до 50 метров, их маршруты, все персональные данные, включая ФИО, возраст, профессию, номера счетов, круг общения, родственников, переписку, фото и прочее.

Конечно, многое потеряно, тем не менее надо выбираться из мышеловки, пока она не захлопнулась.

Первое — обеспечить цифровой суверенитет страны. Безусловно, необходим мониторинг Всемирной паутины на государственном уровне, что сейчас не проводится.

Второе — сетевая безопасность, импортозамещение и поддержка отечественных разработчиков. Где есть российские аналоги — применять их, где нет — создавать.

К сожалению, наши пользователи не спешат переходить на отечественные технологии. В прошлом году на закупку российских информационных разработок было израсходовано лишь 20% от всего объема госзакупок в сфере программного обеспечения.

Программа цифрового суверенитета должна быть принята на государственном уровне с соответствующей поддержкой, в том числе финансовой.

Госпрограмму нужно подкрепить законодательной и нормативной базой. Доктрина информационной безопасности России принята еще в 2000 году, а документов для ее реализации не хватает.

Важно определить первоочередные стратегические объекты и обеспечить их безопасность несколькими контурами защиты. Параллельно организовать переподготовку персонала — как местных айтишников, так и пользователей-секретоносителей.

В нынешней ситуации исключительно полезными и востребованными станут региональные центры реагирования на угрозы (их необходимость и эффективность подтверждает опыт стран, дорожащих своим суверенитетом). Подобные структуры, оперативно анализируя информацию о возникающих вирусных атаках, смогут своевременно вырабатывать противоядие и защищать от киберопасностей.

Главные условия информационной безопасности страны — технические средства и программное обеспечение — должны быть созданы в России и российскими разработчиками.

Константин ЛЫСОВ, руководитель Северо-Западного представительства Комитета Госдумы по обороне