Раздел I. Общие вопросы информационной безопасности

УДК 004.239. 056

Ф.Г. Хисамов

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УСТОЙЧИВОСТИ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СООБЩЕСТВ

В ноябре 2008 г. создан Совет при Президенте РФ по развитию информационного общества в РФ из ведущих ученых РАН, членов Правительства и Администрации Президента, силовых министров, а также некоторых Глав субъектов РФ, Москвы и Санкт-Петербурга. В данной работе на основе анализа отечественных и зарубежных источников прослеживается влияние криптографических методов защиты информации на обеспечение устойчивости общественных формаций к информационным атакам со стороны криминальных и террористических группировок с момента изобретения телеграфа до построения современного информационного общества с глобальной информатизацией всех сторон жизнедеятельности граждан.

Информационная безопасность; информационная атака; кибертерроризм; криптографическая защита; криптографическая транзакция; электронная цифровая подпись; биометрия; электронный документооборот.

F.G. Khisamov

PROBLEMS OF INFORMATION SECURITY AND STABILITY OF MODERN INFORMATION COMMUNITIES

In November 2008, the Presidential Council on Information Society Development in Russia of the leading scientists of the RAS, members of the Government and Presidential Administration, the power ministers, as well as some heads of Russian regions, Moscow and St. Petersburg has been established. In this paper, based on an analysis of domestic and foreign sources, the influence of cryptographic protection of information on the sustainability of social systems to information attacks by criminal and terrorist groups since the invention of the telegraph to a modern information society, with global computerization of all aspects of citizen's life is shown.

Information security; information attack; cyberterrorism; cryptographic protection; cryptographic transaction; digital signature; biometrics; Electronic Document Management.

Современное общество ускоренными темпами движется к информационному обществу, что многократно обостряет зависимость социально-политической стабильности государств от степени защищенности информационной сферы от злоумышленных посягательств криминальных структур. В ноябре 2008 г. при Президенте РФ создан Совет по развитию информационного общества в Российской Федерации. В него вошли члены Администрации Президента, силовые Министры, члены Общественной палаты РФ, Президент и ведущие ученые РАН, мэры Москвы и Санкт-Петербурга, министры и члены Правительства, а также некоторые губернаторы и главы республик РФ. Такая представительность состава «Совета» свидетельствует о том, что руководство страны понимает важность защиты обще-

ства от глобальных последствий широкого, повсеместного использования информационных технологий, которые, к большому сожаленью, еще не всегда осознаются некоторыми руководителями хозяйственных субъектов. Ежегодно все промышленно развитые страны сталкиваются с последствиями от мощных информационных атак на государственные и банковские электронные сети со стороны кибертеррористов, что приводит к огромным финансовым ущербам и надолго парализует деловую активность государственных структур. По мнению экспертов Международной конференции E-Grime, ежегодно проводимой в Лондоне, в будущем информационном обществе придется столкнуться с угрозами совершенно нового рода – огромной армией киберпреступников, опирающихся на поддержку специализированных «сервисных служб» [1]. Поэтому появляется возможность террористам-одиночкам реально разрушать государственные структуры, убирать отдельных людей, наносить реальные потери войскам, инициировать реальные катастрофы и кризисы. Используя, на первый взгляд совершенно, безобидные производства например, городской Холодильник, террорист одиночка может, проникнув в сеть автоматического управления, снять ограничения на давление отравляющей жидкости в системе и взорвать холодильные установки, заразив целые кварталы города, или проникновением в сеть автоматического управления объектами энергетики, водозабора и др. систем жизнеобеспечения города или региона создать техногенные аварийные ситуации надолго парализующих нормальное развитие соответствующих народохозяйственных комплексов.

Современные информационные атаки давно классифицируются как ведение информационной войны. Не следует недооценивать эффективности таких войн. По мнению западных и российских аналитиков ущерб от действий сетевых террористов уже в ближайшее время будет сопоставим с потерями от военных действий, особенно эффективными эти действия будут в современных информационных сообществах, построение которых стремительно набирает обороты во всех промышленно развитых странах, в том числе и в России.

Проблема информационной устойчивости напрямую связана с проблемой защиты информационных ресурсов государства, т.е. криптографией. Криптография очень древняя наука. Она появилась с появлением письменности. Уже на ранних стадиях развития человеческих формаций неизбежно возникала потребность в защите информации, т.е. в системе массовой криптографии, которая на первых порах легко заменялась государственными гарантиями, например, неприкосновенностью почты. Однако с развитием новых телекоммуникационных средств, таких как телеграф, телефон, радио и Интернет государственных гарантий становится далеко недостаточным. Появление новых информационных технологий приводит, с одной стороны, к широкой доступности информации и как следствие к возможности несанкционированного доступа (НСД), а с другой – связано с ослаблением степени учетности источников и приемников информации. Поэтому новые информационные технологии неизбежно порождают необходимость внедрения технологии обеспечения учетности информации через ее криптографическую защиту. Это хорошо видно на историческом развитии криптографических услуг так называемых криптотранзакций [2, 7]. Например, на момент появления телеграфа 1844 г. – на одного гражданина приходилось как минимум 10^{-7} криптографических транзакций. Подобный поток крайне мал и не осознавался гражданами как обыденная реальность, хотя он практически существовал и вполне поддавался статистическим оценкам.

В 1943 г. на момент появления ЭВМ каждый час на одного человека приходилось 10^{-5} криптографических транзакций. Это уже реально осязаемый процесс, если перевести на военный язык, для обработки такого потока криптотранзакций требу-

ется, чтобы в каждой дивизии (это примерно 10^4 человек) должна была существовать своя криптографическая служба, в среднем шифрующая/расшифровывающая порядка двух сообщений каждые сутки.

С появлением цифровой связи потока оцифрованной информации (данных), увеличиваются новые приложения криптографических транзакций. Так, необходимость защиты от неограниченного копирования музыки и изображений в Интернете привела к появлению технологии нанесения цифровых водяных знаков для цифровой музыки и цифровых изображений так называемой стеганографии. То есть расширяются функции по созданию эффективных механизмов обеспечения учетности информации. Поэтому начиная с 70-х гг. прошлого столетия, поток криптотранзакций начинает монотонно возрастать. Этому способствует появление персональных ЭВМ, кредитных карт и GSM-связи и т.д.

Если считать, что каждый десятый человек, связанный с ПЭВМ, хотя бы раз в сутки запускает его по паролю, то мы получим поток на уровне $2{,}5 \cdot 10^{-3}$ криптотранзакций в час, приходящихся на одного человека. Использование кредитных карт увеличивает этот поток примерно в 2 раза, т.е. имеем $7{,}5 \cdot 10^{-3}$ транзакций. С учетом Internet эта цифра достигает порядка 10^{-2} криптотранзакций в час на одного среднестатистического человека. Достаточно ощутимый прирост массовости использования криптографических операций дает мобильная телефонная связь. Этот вид коммерческих услуг полностью опирается на криптографические процедуры аутентификации. Средний пользователь мобильной связи звонит по своему телефону не менее трех раз в сутки – этот поток звонков приводит к эквивалентному потоку криптотранзакций на уровне 10^{-1} в час.

Таким образом, за предыдущее столетие востребованность криптографии поднялась на 5 порядков. Поток криптотранзакций 10^{-1} уже реально ощутим, среднему человеку каждые десять часов его жизни приходится сталкиваться с необходимостью осуществления хотя бы одной криптографической операции. Криптографические услуги начинают становиться действительно массовыми.

Одним из главных характеристик информационного общества является биометрия, обеспечивающая политику учетности граждан. Машиночитаемые биометрические приложения к обычному паспорту придется оформлять в виде электронного документа, подписанного электронной цифровой подписью органа внутренних дел, выдавшего это электронное биометрическое приложение. Тогда, с одной стороны, мы все оказываемся надежно «учтены» через биометрию и легко идентифицируемы государственными службами, а с другой – электронные паспорта могут оказаться очень удобными в бытовом плане (покупки в магазинах, автоматическая аутентификация при входе в дом, на работу, в метро и т. д.). По крайней мере, если в электронный паспорт гражданина России будет внесен его открытый ключ, то проверка его электронной цифровой подписи существенно упростится для других граждан. В принципе это все может оказаться очень эффективным решением удобного юридического оформления значимых в правовом отношении электронных процедур.

Как бы мы сегодня ни относились к этому, мы не в силах остановить процесс глобальной информатизации учетно-паспортных государственных систем России и других стран [8]. По сути дела, эпоха электронных паспортов – это эпоха глобального распространения криптографии, когда ВСЕ люди вынуждены будут пользоваться криптографическими механизмами. Даже те, кто никогда не пользуется электронными деньгами, паролями, мобильными телефонами, компьютерами будут все равно вынуждены иметь электронный машиночитаемый паспорт. Скорее всего, это приведет к существенному росту потока криптографических операций по проверке подлинности ЭЦП-паспорта и ЭЦП-владельца паспорта в различных электронных документах.

Однако заметим, что обеспечение достоверности открытого ключа ЭЦП-пользователя – это только половина проблем будущей массовой криптографии. Вторая половина проблем связана с тем, как обеспечить пользователей надежными механизмами хранения их личных ключей. На данный момент этой проблемой активно занимаются во всех ведущих странах мира. Пока просматриваются два пути решения проблемы. В России прорабатывается путь использования больших обученных нейронных сетей по преобразованию тайного биометрического образа пользователя в его личный ключ [3, 4]. А в США идут иным направлением, разрабатывая технологию использования нечетких экстракторов для преобразования нечетких, неоднозначных биометрических параметров в сильный криптографический ключ [5]. Таким образом, можно однозначно утверждать, что в ближайшей перспективе проблема однозначной связи биометрии с личным ключом пользователя будет решена и криптография станет удобной для обычных пользователей. Это должно привести к существенному росту потока криптографических транзакций.

Кроме того, на базе биометрии будет решена еще одна проблема информационного общества, а именно внедрение электронных денег. По существу будущие электронные деньги (электронные монеты) будут являться гибридом биометрии и криптографии. Фактически это будут расписки (чеки) на определенную сумму, первоначально выданные некоторым банком с указанием конкретного владельца. Далее эти расписки (чеки) будут кочевать от одного владельца к другому (при этом каждая операция передачи электронного документа будет записываться в него и охватываться ЭЦП, участвующих в сделке лиц). В целом должна появиться удобная система мировых электронных денег для безопасных платежей, эквивалентная использованию обычных бумажных наличных денег. Проверка подлинности такой электронной монеты (купюры) фактически будет сводиться к проверке подлинностей всей цепочки электронных цифровых подписей всех лиц, промежуточно владевших конкретной электронной монетой от момента ее создания банком-эмитентом до момента ее приема банком-приемником. Здесь важно подчеркнуть, что в этой технологии криптографические механизмы разных людей и разных банков оказываются многократно и надежно сцепленными. Криптотранзакции будут размножаться лавинообразно, цепляясь друг за друга и, соответственно, их поток будет существенно увеличиваться. Получается, что наблюдаемое сегодня линейное увеличение потока криптографических операций может смениться на некоторую степенную функцию.

Однако здесь возникает еще одна проблема защиты не только личных ключей пользователя, но большинство личных приложений граждан. Одним из мощных инструментов решения этой проблемы послужило принятие Федерального закона «О персональных данных» №152-ФЗ от 27 июля 2006 г. и Постановления Правительства от 17 ноября 2007 г. №781 “Об утверждении Положения, об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных” [6]. В будущем информационном обществе появятся электронные секретари, способные узнавать ваш голос или почерк. Фактически вы получаете своего электронного двойника, распознающего ваши биометрические параметры. Ценность такого электронного секретаря, способного узнавать ваш почерк для вас, несомненно, велика. Однако эта ценность велика и для ваших недоброжелателей. Имея такого двойника можно легко приспособить его для решения обратной задачи, например, для взлома вашей биометрико-нейросетевой защиты. Выход из этого положения только один: в будущем информационном обществе необходимо будет надежно защищать не только ваш электронный кошелек, но и вашего персонального секретаря, способного понимать ваш почерк или ваш голос. Получается, что всякий раз, обращаясь к вашему личному приложению, вы будете вынуждены иметь дело с некоторыми механизмами криптографической

защиты, что может очень и очень сильно поднять поток криптотранзакций. Практически защита личных секретарей и иных личных приложений дает поток в 10^3 криптотранзакций в час. По сравнению с сегодняшней ситуацией (10^{-1}) ожидается рост на 4 порядка, что является очень серьезным скачком.

Сегодня в личных компьютерах, используются общественные программы, изготовленные под массового пользователя и потому обезличенные. В недалеком информационном обществе мы будем иметь не только личные компьютеры, но и личное программное обеспечение. Личные электронные секретари будут хорошо понимать только своего хозяина и выполнять только его поручения. Появятся личные электронные адвокаты, для правовой поддержки конкретного человека и обеспечивающие надежное хранение его личных тайн и документов. Личные надежные электронные бухгалтеры, отслеживающие интересы своего хозяина, помнящие все его расходы и доходы. Вместо историй болезней, медицинских карт у каждого человека появится свой персональный электронный врач, помнящий все о своем хозяине, обладающий общими медицинскими знаниями и допускающий очередного реального медика только к той информации, которую разрешит хозяин. Пока мы доверяем такую информацию сторонним людям, но это явление временное, которое навсегда исчезнет в построенном информационном обществе.

Из вышесказанного можно сделать вывод: по мере продвижения к информационному будущему проблемы обеспечения устойчивости государства будут только расти. Решение этих проблем можно осуществить только через повсеместное, тотальное использование специальных криптографических механизмов обеспечения конфиденциальности, анонимности, аутентификации, целостности, учетности, доступности. Криптография из закрытой элитарной сферы деятельности вынужденно станет массовой и будет обслуживать всех граждан как работающих, так и домохозяек, пенсионеров, детей, во много раз увеличив объемы своих услуг.

То есть реализация проблемы обеспечения устойчивости работы государственных институтов при переводе их на электронный документооборот будет напрямую зависеть от внедрения средств криптографической защиты. По данным Совета безопасности РФ сумма ежегодного ущерба от компьютерных преступлений в стране составляет более 34 млрд руб. Только за последние три года количество преступлений, связанных с неправомерным доступом к компьютерной информации возросло в 30 раз, а с созданием и распространением вредоносных программ – в 140 раз. Преступные и террористические сообщества обладают мощной финансово-экономической базой, действуют в рамках информационно и технически сверхоснащенных сетевых структур.

Применяемые сегодня в России меры обеспечения информационной безопасности не всегда эффективны, часто неадекватны или носят стихийный и бессистемный характер. Общая тенденция к введению электронного документооборота, в государственных, ведомственных, коммерческих и других структурах в ходе реализации Федеральной целевой программы «Электронная Россия», может стать почвой для увеличения преступлений в информационной сфере, если не будет обеспечена надежная защита электронных документов криптографическими методами.

Организационной мерой, направленной на решение проблемы информационной безопасности электронного документооборота могут стать региональные ситуационные центры информационной безопасности (РСЦИБ), которые целесообразно ввести в структуры аппарата глав субъектов РФ в федеральных округах. Основная задача РСЦИБ – формирование региональной системы информационной безопасности (РСИБ). Технической основой решения данной проблемы является использование новейших отечественных разработок, созданных на основе программно-аппаратных средств защиты информации «Криптон», выпускающих ОАО «Анкад» г. Зеленоград.

В настоящее время проект создания «Региональной системы информационной безопасности» разработан применительно к Южному федеральному округу, включающего 13 субъектов Российской федерации. Этапы выполнения проекта подробно обоснованы с научной, технической и финансовой стороны. Однако основные принципы и технологии реализации проекта универсальны и применимы к любому Федеральному округу Российской федерации, в том числе и к Республике Татарстан. Создание региональной системы информационной безопасности в масштабах Республики Татарстан может быть завершено, согласно проведенным нами расчетам в течение 1 – 1,5 года.

Инициатором проекта выступает Кубанский институт информзащиты, г. Краснодар. Руководителем проекта является ректор Кубанского института информзащиты академик РАЕН, профессор, доктор технических наук Ф.Г. Хисамов.

Институт обладает интеллектуальной собственностью в области информационной безопасности, содержит в штате научные кадры высшей квалификации и имеет партнерские отношения с ведущими отечественными производителями криптографических средств защиты информации (КСЗИ), продукция которых сертифицирована и широко используется в МВД, Министерстве Обороны, Центральном Банке РФ, Сбербанке России, Министерстве по налогам и сборам РФ, Федеральном казначействе РФ, коммерческих банках, финансовых и страховых компаниях страны. Мы открыты к сотрудничеству для обеспечения надежной защиты электронного документооборота Республики Татарстан и других субъектов РФ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Вехов В.Б.* Преступления, связанные с неправомерным использованием баз данных и содержащейся в них компьютерной информации // Защита информации. – 2008. – № 2. – С. 78.
2. *Гезенко И.И., Иванов А.И.* Обеспечение устойчивости будущего информационного общества: массовая, гражданская криптография // Защита информации. – 2005. – № 1. – С. 71.
3. *Michel.* The Security Features in the GSM-System // 6-th World Telecommunication Forum Proceedings. – Geneva, 1991. – Part 2. – P. 385-389.
4. *Иванов А.И.* Биометрическая идентификация личности по динамике подсознательных движений // Монография. – Пенза: Изд-во ПГУ, 2000. – 188 с.
5. *Yevgeni Dodis, Leonid Reyzin, Adam Smith.* Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data // April 13, 2004. www.cs.bu.edu/~reyzin/fuzzy.html.
6. Что делать с персональными данными // Защита информации. – 2008. – № 3. – С. 39.
7. *Гольев Ю.И., Ларин Д.А., Шанкин Г.П.* Криптографическая деятельность революционеров в России. Полиция против революционеров // Защита информации. – 2008. – № 2. – С. 86.
8. *Костромитин А.А.* Возможные перспективы развития системы электронных паспортов в РФ // Защита информации. – 2005. – № 3. – С. 16.

Статью рекомендовал к опубликованию д.т.н., профессор О.А. Финько.

Хисамов Франгиз Гильфанетдинович
Краснодарское высшее военное училище.
E-mail: Frangiz_khisamov@rambler.ru.
350035, г. Краснодар, ул. Красина, 4.
Тел.: 88612681456.
Зав. кафедрой математики и физики.

Khisamov Frangiz Gilfanetdinovich
Krasnodar Higher Military School.
E-mail: Frangiz_khisamov@rambler.ru.
4, Krasin Street, Krasnodar, 350035, Russia.
Phone: +78612681456.
Head of the Department Mathematics and Physics.