XXX Юбилейная Неделя науки СПбГТУ. Материалы межвузовской научной конференции. Ч. VII: С.46, 2002.
УДК 681.324

Ю.А. Торшенко (1 курс, ИТМО каф. БИТ), А.В. Птицын, к.т.н., доц.

КРИПТОГРАФИЯ В ИСТОРИИ РОССИИ

С древних времён в России и зарубежных странах использовались различные приёмы для скрытия от посторонних глаз конфиденциальной информации. Формирование государственной системы защиты информации в России началось во второй половине XVI века во времена правления Ивана IV Грозного. Это обусловлено увеличением сферы влияния России на внешнеполитической арене и расширением государства российского. В те времена криптография (или тайнопись) использовалась для шифрования военной, дипломатической, торгово-финансовой и прочей переписки. Тогда же появляются первые специалисты-тайнописцы, находящиеся на государственной службе, а также первая структура управления охраной государственных секретов – Посольский приказ. Использовавшиеся способы зашифровки: литорея (“тарабарская грамота”) и “полусловица” являлись достаточно примитивными, но в своё время выполняли необходимые функции.

Учреждение постоянной почтовой связи России с Европой дало новый толчок к совершенствованию государственной системы защиты информации вообще и криптографических методов преобразования в частности. Первым российским государем, осознавшим особую значимость защиты информации, был Пётр Великий. В Посольской канцелярии образовывается “цифирное отделение”, ведавшее всей деятельностью в области криптографии. В то время в России использовались однобуквенные, двухбуквенные, цифровые, буквенно-слоговые шифры замены. Шифры начинают снабжаться “пустышками” (шифрообозначения, которым не соответствует никакой знак открытого текста) и “суплементом” (небольшой словарь, включавший наиболее употребительные термины). 30-е г.г. XVIII в. ознаменованы появлением совершенно новых систем тайнописи – алфавитных и неалфавитных кодов. Для обеспечения государственной безопасности в 40-50 г.г. XVIII в. создаются “чёрные кабинеты” (служба перлюстрации). Россия достигает первых успехов в дешифровке иностранных шифров.

В первой половине XIX века вся криптографическая деятельность сосредотачивается в канцелярии Министерства иностранных дел (МИД), где было образовано три секретные экспедиции: шифрования, дешифрования и служба перлюстрации. Шифры постоянно усложняются, разрабатываются новые системы шифрования, криптография обретает статус науки. Крупнейший криптограф XIX века П.Л. Шиллинг изобретает шифр биграммного типа.

Во второй половине XIX века криптографическая служба создаётся ещё в двух ведомствах: военном и внутренних дел. Шифры МИД, Военного министерства и Министерства внутренних дел (МВД) разделялись на секретные, несекретные и специального назначения. Несекретные ключи использовали в случаях, когда содержание сообщения не являлось секретным, но в то же время желательно было избегать преждевременной огласки передаваемых сообщений в печати и т.п. Ключи специального назначения использовались для связи с различными правительственными учреждениями и частными учреждениями и лицами. В МИД применяли следующие виды шифров: французские и русские биграммные шифры, биклавные шифры, шифровальные коды, перешифровальные ключи. Наиболее распространённым типом шифров, используемым в военном министерстве, был словарный ключ (объёмом до 1000 словарных величин). Шифры МВД и других ведомств включали шифры Цезаря, книжные шифры и шифры перестановок.

Во все времена в России к криптографии подходили как к делу государственной значимости. Богатый практический и теоретический опыт, накопленный российскими криптографами всегда достойно служил защите государственных интересов нашей страны.