Д.А. Ларин

ПЕРВОПРОХОДЕЦ В ЭЛЕКТРОСВЯЗИ
К 230-летию со дня рождения изобретателя электрического телеграфа П.Л. Шиллинга фон Канштадта

230-лет назад родился П.Л. Шиллинг фон Канштадт, выдающийся ученый и изобретатель, криптограф. Главным его изобретением стал электрический телеграф, сделавший революцию в связи, стала возможной практически мгновенная передача информации; также П.Л. Шиллинг возглавлял криптографическую службу и разработал несколько шифрсистем.

Ключевые слова: П.Л. Шиллинг фон Канштадт, электрический телеграф, связь, криптография.

Люди всегда хотели иметь возможность передачи важных срочных сведений на значительные расстояния. Самым надежным средством связи долгое время оставались гонцы. Однако изобретались и другие способы передачи информации. При желании можно историю современных телекоммуникационных технологий вывести от первобытного тамтама (Африка), дымовых сигналов, огней костров и т. д. Для передачи сообщений с древних времен использовались почтовые голуби. Однако решающую роль в появлении систем передачи информации на большие расстояния сыграло открытие электричества. В XVIII и начале XIX в. в разных странах проводились опыты по использованию электрического тока для передачи информации. Первый практически пригодный электромагнитный телеграф был создан нашим соотечественником бароном Павлом Львовичем Шиллингом фон Канштадтом, выдающимся ученым и изобретателем. Рассмотрим его деятельность в области отечественной криптографии подробнее.

Павел Львович был уникальным человеком, своей разнообразной и плодотворной деятельностью он прочно вошел в историю российской науки и культуры. П.Л. Шиллинг фон Канштадт родился 5 апреля (ст. ст.) 1786 г. в г. Ревеле (ныне г. Таллин, Эстония), в семье командира Низовского мушкетерского полка.

По примеру отца П.Л. Шиллинг выбрал военную карьеру. После окончания обучения в 1802 г. в Первом кадетском корпусе в Санкт-Петербурге он в чине подпоручика начал военную службу в Генеральном штабе российской армии. Через год по семейным обстоятельствам Павел Львович вынужден был оставить военную службу. Он поступил на службу в Министерство иностранных дел, где стал работать переводчиком русской миссии в столице Баварии (тогда это было независимое государство) г. Мюнхене. В результате обострения отношений России с наполеоновской Францией наши дипломаты в 1812 г. были спешно отозваны на Родину. В период войны 1812–1814 гг. проявляется одна из замечательных черт личности Павла Львовича – высокий патриотизм, безграничная любовь и преданность Отечеству. Два раза П.Л. Шиллинг подавал рапорт о возвращении на военную службу, вторая попытка оказалась успешной, Шиллинг получил назначение в 3-й Сумской драгунский полк в чине штабс-ротмистра и отправился в действующую армию. За храбрость, проявленную в боях, в 1814 г. П.Л. Шиллинг был награжден первым боевым орденом, а затем одной из самых почетных наград – саблей с надписью «За храбрость». В том же году, находясь в составе русских войск в Германии, Павел Львович заинтересовался изобретенным еще в 1796 г. А. Зенефельдером литографированием. Поясним здесь, что литография – это способ плоской печати, при котором печатной формой служит поверхность камня (обычно известняка). Изображение на литографический камень наносят жирной тушью или специальным литографическим карандашом. После окончания войны с Наполеоном П.Л. Шиллинг подал прошение о возвращении с военной службы в Министерство иностранных дел. Главнокомандующий Барклай де Толли эту просьбу удовлетворил. Вернувшись в МИД, Шиллинг обратил внимание тогдашнего статс-секретаря министерства графа К.В. Нессельроде на только что входивший тогда в употребление в Европе литографический способ печати. Руководство МИД тут же отправило Шиллинга в командировку в Баварию – родину изобретения литографии (кстати, там добывалась порода камня, наиболее пригодная для литографирования). Ознакомившись там с технологией, Павел Львович в 1817 г. организовал первую в России литографию, которая стала одним из подразделений МИД. 12 июня 1818 г. барон Шиллинг фон Канштадт был назначен управляющим литографией. Одновременно он выступил инициатором использования этого метода печати для размножения топографических карт и других военных документов, в том числе и ключевой документации к российским шифрам, а впоследствии – результатов дешифрования перехваченных и перлюстрированных писем

для доклада руководству. С этого же времени Павел Львович становится заведующим цифирной частью МИД (шифровальной службой Российской империи), которая в 1832 г. преобразуется в экспедицию.

Шиллинг был разносторонним ученым, например, в кругах научной и культурной общественности завоевал всеобщее признание литографированием китайских рукописей. Вот что об этом пишет российский историк Т.А. Соболева: «Ревностный пропагандист китайской литературы», по выражению синолога академика Клапрота, Шиллинг добился такого уровня воспроизведения китайских рукописей, который был равен «по тщательности и изяществу самым совершенным образцам китайской печати». Клапрот отмечал, что русское издание китайского текста «оставляет далеко позади все, что было издано до сих пор в Европе». Шиллинг был страстным любителем и знатоком восточной культуры. Во время своей поездки по Южной Сибири он собрал ценнейшие коллекции китайских, маньчжурских, монгольских, тибетских, японских и индийских рукописей. Богатейшие собрания этих манускриптов были переданы ученым в Азиатский музей Академии наук в Петербурге. Он собрал также интересные коллекции по этнографии Средней Азии[1].

Разносторонняя и одаренная личность, полковник российской армии, ученый-востоковед, член-корреспондент Российской академии наук, П.Л. Шиллинг был другом А.С. Пушкина, К.Н. Батюшкова, А. Мицкевича, А.И. Тургенева.

Вновь обратимся к книге Т.А. Соболевой: «Исследователи жизни и творчества А.С. Пушкина при изучении людей пушкинского круга обращают особое внимание на П.Л. Шиллинга, приводят свидетельства многочисленных встреч великого поэта с Шиллингом и даже некоторые даты. Так, например, 19 ноября 1818 г. А.С. Пушкин и П.Л. Шиллинг в компании с Н.И. Гнедичем, В.А. Жуковским, М.С. Луниным, А.И. Тургеневым и др. выезжали в Царское Село для проводов уезжавшего в Италию Батюшкова. 25 мая 1827 г. возвратившийся из ссылки в Санкт-Петербург Пушкин вместе с Шиллингом, П.А. Вяземским и А.А. Олениным принимал участие в прогулке в Кронштадт, а 6 июня Пушкин и Шиллинг были у Карамзиных. В ноябре – декабре 1829 года Шиллинг готовился к экспедиции в Восточную Сибирь и Китай в сопровождении И.Я. Бичурина, и Пушкин, по словам Н.В. Путяты, собирался ехать с ними, но не получил разрешения Бенкендорфа. К этому времени относится карандашный портрет Шиллинга, выполненный Пушкиным в альбоме Ек.Н. Ушаковой. О встречах Пушкина и Шиллинга в 30-х годах писал позднее М.П. Погодин»[2].

П.Л. Шиллинг, по отзывам современников, был не только серьезным ученым, но и веселым и компанейским человеком, правда они отмечали его чрезмерный вес: «необычайно толстый человек». Павел Львович отлично играл в шахматы, он мог играть «две партии одновременно, не глядя на шахматные доски, и побеждать обоих противников в один момент»[3]. Прежде всего, это был выдающийся ученый. Как востоковед, П.Л. Шиллинг в 1827 г. становится членом-корреспондентом Академии наук (по отделению языкознания и словесности). Также П.Л. Шиллинг занимался исследованиями и опытами в области электротехники и внес существенный вклад в ее развитие в России. Например, в 1812 г. он впервые демонстрировал в Санкт-Петербурге взрыв изобретенной им электрической мины, затем повторно опыты были проведены в 1815, 1822 и 1827 гг. По окончании Русско-турецкой войны 1828–1829 гг. «электрическая мина Шиллинга была подвергнута полевым испытаниям, а с 1833 года осваивалась в специальном саперном подразделении»[4].

Создание электрического телеграфа стало венцом изобретательской деятельности Павла Львовича. Этот аппарат он публично продемонстрировал 21 октября 1832 г. в своей квартире на Царицыном лугу в Санкт-Петербурге (Марсово поле, д. 7). На этом доме сохранилась установленная Русским техническим обществом в 1886 г. в связи со 100-летием со дня рождения выдающегося ученого мемориальная доска со следующей надписью: «Здесь жил и умер русский изобретатель электромагнитного телеграфа Павел Львович Шиллинг»[5].

В основе действия этого аппарата находился эффект отклонения магнитной стрелки в результате воздействия электромагнитного поля от электрических проводов. Передающий и приемный аппараты соединялись кабелем, состоящим из восьми проводов. Каждый провод при передаче включался своей клавишей. При этом приходилось для передачи одной буквы нажимать по три-четыре клавиши одновременно. На приеме каждый проводник подсоединялся к своему электромагниту с висящей над ним магнитной стрелкой. Если по проводу проходил ток, то стрелка поворачивалась. По набору состояний стрелок восстанавливалась переданная буква. Таким образом, каждая буква кодировалась своим набором нажимаемых клавиш.

В 1828 г. прообраз будущего электромагнитного телеграфа был готов и испытан. Он представлял собой двухпроводный однострелочный телеграф. Аппарат содержал все основные узлы, необходимые для телеграфирования: источник питания – вольтов столб (или столбец, как его называл сам Шиллинг); передатчик, подключавший

к каждому из двух линейных проводов то один, то другой полюс батареи; двухпроводную линию; коммутатор, производящий переключение с приема на ожидание передачи; и, наконец, приемник.

Основной частью приемника являлась так называемая астатическая пара стрелок, предложенная французским физиком А.М. Ампером в 1821 г. для устранения влияния земного магнетизма. Две магнитные стрелки укреплялись на общей медной оси и располагались параллельно одна другой. Полюса были обращены в противоположные стороны. Спаренные стрелки подвешивались так, что могли вращаться в горизонтальной плоскости, причем одна располагалась внутри катушки, состоящей из нескольких сот витков изолированного провода, а другая – вне ее. К шелковой нити, на которой подвешивались стрелки, был прикреплен небольшой диск диаметром около 40 мм. Одна его сторона окрашивалась в черную краску, другая – в белую. В зависимости от направления тока в катушке магнитная стрелка поворачивалась в ту или иную сторону (правую П и левую Л), и телеграфист, принимающий депешу, видел либо черный, либо белый диск. Если ток в катушку не поступал, то диск был виден ребром. Внизу располагался сосуд с ртутью, гасящий колебания астатических стрелок и приводящий их в первоначальное положение по окончании действия электрического тока.

Для передачи латинского алфавита и цифр Шиллингом был разработан специальный код из комбинаций разного числа (от одного до пяти) последовательных сигналов, посылаемых током разного направления. Однако подобный код оказался чересчур неудобным: для распознавания каждой буквы требовалось запоминание всей комбинации обозначающих ее последовательных сигналов. Например: для буквы А – П, Л; для буквы М – Л, П, Л; для цифры 5 – Л, П, П, Л, Л и т. д. Процесс телеграфирования происходил очень медленно.

Решение проблемы принес шестистрелочный телеграф в сочетании с более рациональным кодом. Передача всех букв русского алфавита обеспечивалась отклонением в разные стороны одной или двух стрелок из шести. Цифры обозначались отклонением трех стрелок из шести. Были разработаны единый передатчик с восемью парами белых и черных клавишей (одна пара служила для посылки вызова и одна пара являлась общей) и единый приемник с семью стрелками, смонтированными на общей раме (одна стрелка обозначала наличие вызова). Линейная часть устройства состояла из восьми проводов, включая вызывной и общий обратный. Для передачи латинского алфавита достаточно было пяти стрелок и пятизначного кода.

Первая публичная демонстрация телеграфа Шиллинга происходила 9(21) октября 1832 г. Для демонстрации работы созданного аппарата Павел Львович снял на время у владельцев дома, в котором жил, весь этаж. Передатчик был установлен на одном конце этажа, а приемник – на другом, в рабочем кабинете Шиллинга, на расстоянии немногим более 100 м. Первая телеграмма, состоящая из десяти слов, на глазах у присутствующих была принята по электромагнитному телеграфу лично П.Л. Шиллингом моментально и верно. Это произвело на присутствующих огромное впечатление. Интерес к изобретению в самых разных кругах русского общества был настолько велик, что демонстрация работы электромагнитного телеграфного аппарата не прекращалась почти до самых рождественских праздников. Выдающийся русский военный инженер того времени К.А. Шильдер, ознакомившись с изобретением П.Л. Шиллинга, после демонстрации аппарата писал своему другу об электромагнитном телеграфе: «В скором времени сообщу тебе еще одно интересное дело. Оно касается проекта телеграфа на неопределенное расстояние, основанного на гальванизме, с помощью которого возможно будет во всякое время телеграфировать с быстротой мысли. Я надеюсь, что он будет когда-нибудь испытан до Москвы, если только опыты в малом виде сделают очевидным то, что в техническом отношении не подлежит малейшему сомнению...»[6].

Несмотря на большой интерес общественности к новому изобретению, правительство не торопилось с его внедрением. Только в 1836 г. в России был наконец образован под председательством морского министра «Комитет для рассмотрения электромагнетического телеграфа», предложивший Шиллингу установить телеграф в здании Главного Адмиралтейства в Санкт-Петербурге с целью длительных испытаний его в условиях, близких к эксплуатационным. Аппараты располагались в противоположных концах длинного здания, провода были проложены частично под землей, частично под водой. Эта линия действовала более года. В том же году Шиллинг предложил подвешивать линейные провода между телеграфными станциями на деревянные опоры. В мае 1837 г. комитет предписал Шиллингу устроить телеграфное сообщение между Петергофом и Кронштадтом, для чего составить проект и смету. Выполнить задачу ученый не успел, так как 25 июля 1837 г. П.Л. Шиллинг скончался. Труды Павла Львовича можно рассматривать как один из этапов работ по созданию и распространению проволочного телеграфа, они оказали большое влияние на развитие этой области науки и техники в других странах.

Помимо изобретения собственно телеграфного аппарата, начиная с 1811 г. и до конца своей жизни Шиллинг занимался еще

одним важнейшим вопросом – созданием линии, практически пригодной для передачи электрических сигналов по изолированному проводу (кабелю). При монтаже телеграфного аппарата медные провода изолировались шелком или просмоленной пенькой. Так, обмотка мультипликаторов была выполнена медным проводом, покрытым одним слоем шелковой пряжи, а соединения между мультипликаторами – медным проводом, покрытым одним слоем пеньки, густо пропитанной озокеритом. Для прокладки телеграфной линии между станциями в земле П.Л. Шиллинг применял такие же провода, как для изобретенных им же еще в 1812 г. электрических мин. Так как передающая и принимающая станции соединялись восьмипроводной линией, то все восемь проводов заключались в общую пеньковую изоляцию, а затем просмаливались. Провода же, предназначавшиеся для прокладки в воде, изолировались несколькими слоями шелка или пеньки, причем провода, изолированные шелком, в таких случаях покрывались лаком.

Научные заслуги Павла Львовича Шиллинга фон Канштадта хорошо известны, его имя с одинаковым уважением произносится как учеными-гуманитариями, так и естествоиспытателями. Но вся эта деятельность осуществлялась им в свободное от основной работы время. Главным делом жизни Павла Львовича являлись работа и руководство отечественной шифровальной службой, которому он посвятил почти 20 лет своей жизни. Окружению П.Л. Шиллинга было известно, что он состоит на службе в Министерстве иностранных дел в качестве некого ответственного чиновника. Упоминание об этом в различных изданиях сейчас естественным образом воспринимается как деятельность Павла Львовича на дипломатическом поприще, тем более что он предпринимал заграничные поездки, участвовал в научных заграничных экспедициях.

На самом же деле Павел Львович Шиллинг фон Каншатдт был одним из выдающихся российских криптографов XIX в. В историю криптографии он вошел прежде всего как изобретатель так называемого биграммного шифра. По сути, его шифр являлся комбинацией шифра перестановки с шифром многозначной замены на биграммах (двухбуквенных сочетаниях). Соответственно шифрвеличинами были не буквы, а биграммы. Шифробозначениями являлись числа, по два на каждую биграмму. Важно при этом заметить, что шифровались не две рядом стоящие в открытом тексте буквы, а пара букв, разделенных некоторым заранее оговоренным расстоянием T друг от друга.

Открытый текст сначала переписывался в биграммы букв, находящихся на расстоянии T. Если длина открытого сообщения была не кратна T, то она дополнялось произвольными знаками алфавита.

Таким образом, сообщение a_1, a_2, ..., a_i, ... преобразовывалась к следующему виду: a_1 a_{T+1}, a_2 a_{T+2}, ..., a_i, a_{T+i}... По сути это было предварительное шифрование – перестановка букв исходного сообщения.

Табличное задание правила шифрования биграмм напоминает биграммный шифр итальянца Д. Порты (автора одного из первых фундаментальных трудов по криптографии)[7], однако вместо замысловатых знаков для замены биграмм использовались числа. При этом вводились и «пустышки». Предусматривалось шифрование отдельных знаков, дополнение открытого текста хаотическим набором знаков и т. д. Для реализации такого способа шифрования Шиллинг предложил механическое устройство – наборно-разборную таблицу, наклеенную на коленкор. Срок действия шифра был определен в шесть лет (позднее снижен до трех лет). С современных позиций этот шифр нельзя признать стойким[8].

Этот шифр Шиллинг изобрел, работая в цифирном отделении МИД, среди документальных подтверждений данного факта следует отметить распоряжение К.В. Нессельроде цифирному комитету от 22 марта 1823 г.: «рассмотреть шифр, предложенный П.Л. Шиллингом»[9], а также рапорт Нессельроде от членов цифирного комитета по этому поводу, датированный 14 июня того же года. В российских архивах сохранились некоторые ключи к шифру П.Л. Шиллинга. Вновь обратимся к книге Т.А. Соболевой: «О них есть сведения в “Описи цифирям”, составленной Трефуртом, где наряду с данными о других цифирях, составленных со времени образования цифирного комитета, указывается, что “13 августа 1823 г. от члена оного Комитета Господина Статского Советника Барона Шиллинга фон Канштадта получены его сочинения биграммный ключ № 1 и № 2, № 3 на французском языке, а также пакет с бумагами, относящимися к составлению этих цифирей”»[10].

В феврале 1824 г. экземпляр № 1 биграммного шифра Шиллинга был направлен цесаревичу Константину Павловичу; в январе 1826 г. тот же ключ, а также ключ № 2 переданы князю Меншикову при отправлении его в Персию; в 1828 г. граф К.В. Нессельроде получил третий экземпляр этого шифра при поездке в Америку.

В 1826 г. Шиллинг составил цифирь для адмирала Синявина. В 1827 г. этот экземпляр шифра был передан К.В. Нессельроде, а еще три экземпляра этого шифра направлены в миссию в Вашингтон.

В том же году П. Л. Шиллинг составил генеральную цифирь под № 16, партикулярные цифири № 4, 5, 6, 8, 9 и 10, а также «“военный шифр” № 28 на русском языке»[11].

В литографии, которую Шиллинг организовал и которой заведовал все годы работы в министерстве, проводились работы по

размножению и копированию различных государственных документов. Со времен деятельности Павла Львовича в практику МИД вошел обычай каждый день предоставлять на просмотр министру литографированные копии с перлюстрированных документов и писем, большинство из которых в дешифрованном виде также направлялось для ознакомления государю. Материалы перлюстрации и дешифрования переписки были обычной темой обсуждения на заседаниях цифирного комитета.

Постоянное увеличение числа корреспондентов, сетей и линий шифрованной связи, рост объема шифропереписки повлекли за собой настоятельную необходимость в поисках способа быстрого размножения шифродокументов, и здесь литография Шиллинга играла очень важную роль. П.Л. Шиллинг весьма заботливо относился к своим сотрудникам, учитывая важность их работы. Вот одна из его докладных вице-канцлеру Нессельроде, текст которой гласит: «Литографские ученики Ефимов, Пальцев и Григорьев при хорошем поведении усердным исправлением своей должности, а первый из них сверх того и оказанным искусством в печатании противу своих товарищей, заслуживают внимания начальства, почему долгом поставляю себе испрашивать у Вашего сиятельства в награждение им, первому звание унтер-офицера и 75 рублей, а двум последним по 50 рублей, равно и переплетчику Пазову, занимавшемуся наклейкою цифирных таблиц, 100 рублей»[12].

Успехи зарубежной криптографии требовали от наших специалистов постоянного совершенствования методов работы по созданию шифров. И ранее, и в дальнейшем, в первой половине XIX в., руководители государства осознавали необходимость криптографической деятельности и всемерно ее поощряли. Как и в какой форме осуществлялось поощрение, можно узнать, например, из письма графа К.В. Нессельроде П.Л. Шиллингу от 23 марта 1830 г.:

Барону Шиллингу фон Канштадту
от графа Нессельроде.
Секретно
Милостивый Государь мой!

Государь император в награду особенных на пользу службы трудов Вашего Превосходительства при составлении и изготовлении новых цифирей всемилостивейше пожаловать Вам соизволил 1000 червонных голландских, высочайше повелел выдать Вам сию сумму без всякого вычета из государственного казначейства.

Принимавшим под руководством Вашим участие в сем деле коллежскому советнику Нестеровичу и VII класса Иванову пожаловано каждому на том же основании по 2000 рублей ассигнациями;

надворный советник Геслер удостоен знаков ордена Св. Анны 2-й степени, императорскою короною украшенных; титулярные советники Гасс и Быков получили следующие чины, а титулярному советнику Рахонину пожалован бриллиантовый перстень в 1000 руб.

Я поставляю себе за особенное удовольствие уведомить Вас, Милостивый Государь мой, о таковом монаршем внимании к отмеченным заслугам Вашим и к усердной службе находящихся при Вас чиновников, покорнейше прошу, Ваше Превосходительство, объявить им о пожалованных им наградах[13].

Шифры П.Л. Шиллинга использовались вплоть до начала XX в. В основном они были ориентированы на французский язык. В нарушение существовавших правил эти шифры в неизменном виде использовались на протяжении около 20 лет, что, естественно, не могло не сказаться на их стойкости. Предлагались усовершенствования этого шифра. Так, в частности, рекомендовалось уменьшить число букв латинского алфавита, используемых при написании секретного текста, а также знаков препинания (без потери его смысла при их пропуске или замене на оставшиеся буквы). В этом случае появлялась возможность заменять числовые шифробозначения на буквы и биграммы латинского алфавита (биграммы образовывались за счет наличия исключенных – «запретных» букв в шифрованном тексте). Аналогичным изменениям подвергался и русский биграммный шифр. Нередко в качестве его усложнения использовались дополнительно вариации шифра перестановки.

В заключение расскажем о влиянии появления телеграфа на развитие криптографии. В 1838 г. американский инженер и художник Сэмюэль Ф.Б. Морзе (1791–1872) получил свой первый патент на работоспособный электрический телеграф; ему принадлежат идеи применения ручного ключа для прерывания тока и передачи сообщений по проводам посредством последовательной кодовой системы, использующей в роли элементарных символов короткие и длительные посылки тока. В 1843 г. был предложен эффективный последовательный код переменной длины Вейла–Морзе, в котором ускорение передачи обеспечивалось согласованием длины кодовых слов с частотой появления соответствующих букв в английском языке, т. е. самые короткие кодовые символы присваиваются наиболее часто используемым буквам (например, наиболее частой букве «E» соответствует символ «точка», букве «T» – «тире», букве «A» – «точка-тире», букве «I» – «точка-точка», а редким буквам «X» и «Z» «тире-точка-точка-тире» и «тире-тире-точка-точка» соответственно. Математическая теория связи, разработанная спустя

100 лет, установила, что код Морзе не более чем на 15 % отличается от теоретически достижимого предела.

В 1844 г. С. Морзе передал первую телеграмму по проводному телеграфу своей конструкции: «Вот что сотворил Бог!». При этом Морзе использовал специальную азбуку для кодирования букв, получившую название «азбуки Морзе». Многие «старые» шифры стали непригодными для использования на телеграфных линиях связи. Так, например, экзотические замены букв на замысловатые знаки (например, пляшущих человечков из знаменитого рассказа А. Конан-Дойля) оказались принципиально неприемлемыми.

Уже в 1845 г. Ф. Смит, юрист С. Морзе, опубликовал коммерческий код под названием «Словарь для тайной корреспонденции; приспособлен для применения на электромагнитном телеграфе Морзе». Для обеспечения безопасности предлагалось применять код с перешифровкой, легко реализуемый на телеграфных линиях связи. В последующем развитие шифровального дела и создание механических шифровальных устройств шло с учетом использования их в телеграфной связи.

Хотя П.Л. Шиллинг опередил Морзе в создании телеграфа на 12 лет, электромагнитный телеграф Морзе оказался более удобным в практической реализации и именно он получил широкое распространение.

Увеличение количества линий связи приводило к необходимости разрабатывать новые шифры и коды, удобные для закрытия секретной информации, передаваемой с помощью телеграфа.

В 1850 г. российский инженер Б.С. Якоби изобрел буквопечатающий телеграф. Однако, как и в случае с телеграфом Шиллинга, всемирное распространение получил другой аппарат – буквопечатающий телеграф англичанина Д.З. Юза, созданный им в 1855 г. В 1875 г. появился телеграфный аппарат Бодо с использованием пятизначного кода фиксированной длины. Операторы работают на передатчике с пятью клавишами, комбинация которых нажимается после получения синхронизирующего акустического сигнала от аппарата.

Примерно с 1848 г. телеграфия становится большим бизнесом и занимает центральное положение в технике электрической связи. Поскольку телеграфные передачи стоили недешево и эта стоимость определялась количеством букв передаваемого сообщения, то сразу же были предложены эффективные методы «сжатия» информации – несекретные телеграфные коды, в которых буквы, слова, фразы «сжимались» до коротких буквенно-цифровых единиц передаваемого текста. Однако при передаче секретных

сообщений, помимо такого несекретного кодирования, по необходимости должны были использоваться шифры (шифрование кодированного сообщения). Особенно остро вопросы стоимости телеграфного послания встали в 1866 г., после прокладки трансатлантического кабеля (США–Европа).

Телеграфная передача сопряжена с неизбежными искажениями сообщения в линии связи. Поэтому появилось новое направление в кодировании – помехоустойчивое кодирование. За счет избыточности, вводимой в передаваемое сообщение, на приемном конце появлялась возможность устранить эти искажения. Одновременно увеличилось внимание к такому свойству шифров, как помехоустойчивость. Одной из самых неприятных ситуаций, связанных с искажениями, является такая, при которой на приемной стороне воспринимается текст иного содержания. Приведем исторические примеры, связанные с использованием «азбуки Морзе».

Выпадение одной точки в сообщении, соответствующей букве «E» (E=.) превращает французский глагол citerons («мы укажем») в слово citrons («лимоны»). Увеличенный пробел в букве M (M= - -) превращается в биграмму TT (T= -). При таких искажениях получаются слова, по смыслу далекие от оригинала. Например, слово baneful («губительный»), имеющее в азбуке Морзе вид: -.-... .--. ...-. ..-.-.. может превратиться в слово dutiful («обязательный»): -.. ..--.. ..-. ..-.-.. Такие искажения приводили к дезинформации приемной стороны и порождали серьезные негативные последствия. Так, в 1887 г. один торговец шерстью в США направил своему агенту телеграмму с указанием продать большой объем шерсти и затем ждать дальнейших указаний. Обмен посланиями был защищен разработанным торговцем собственным секретным кодом, в котором шифробозначения букв также имели вид азбуки Морзе. В процессе обмена сведениями в результате искажения слово «продай» превратилось в слово «купи»; такое указание получил агент и выполнил его. В результате торговец потерял несколько десятков тысяч долларов. Он подал в суд на телеграфную компанию. Его иск был удовлетворен своеобразным образом: компанию обязали выплатить торговцу стоимость искаженной телеграммы (чуть больше одного доллара).

Такого рода искажения приводили к необходимости принимать меры защиты. Наиболее важные места сообщений дублировались, что приводило к увеличению расходов на связь. Использовали так называемый «двухбуквенный дифференциал»: ключевые слова должны были отличаться друг от друга не менее чем двумя буквами. Это приводило к появлению большого числа неологизмов – слов, не являвшихся общепринятыми в данном языке (т. е. выра-

батывался телеграфно-кодовый язык, имевший вид жаргонных кодов). Наконец, начали применяться помехоустойчивые коды, позволявшие обнаруживать и устранять искажения. Но это опять привело к удорожанию связи.

Учитывая повышенные требования к точности передачи шифрованных телеграмм, телеграфные компании повысили цену за их передачу. Телеграфисты утверждали, что они вынуждены тщательно и побуквенно передавать нечитаемые тексты, что существенно снижало эффективность их работы по сравнению с передачей обычных «осмысленных» сообщений. В ответ пользователи шифров попытались придать шифрованному (кодированному) сообщению «осмысленный вид» (хотя бы на уровне имеющихся в шифртексте «слов»). Поэтому в 1889 г. в Лондоне была проведена специальная конференция, посвященная толкованию понятия «шифрованная телеграмма». Наконец, в 1890 г. конференция в Париже ввела в обращение официальный словарь кодового языка, содержавший лишь «читаемые слова». Этот словарь вызвал бурю протестов, поскольку, по существу, запрещал передачу секретных (шифрованных) сообщений. Участники конференции в Лондоне в 1903 г. отказались от единого словаря. Было разрешено применять искусственные слова, но при условии, что они будут состоять из «читаемых и произносимых слов» и их длина не будет превышать 10 букв. И все же в 1932 г. на конференции в Мадриде все ограничения по кодированию и шифрованию были сняты.

В 1904 г. в Англии появился словарь Уайтло для кодобозначений; по утверждению автора, он содержал 400 млн произносимых слов. Слова имели вид FREAN, LUFFA, LOZOI, FORAB и т. д., т. е. все слова были пятибуквенными. Уайтло допускал соединение слов для обозначения нового словообразования. Идею Уайтло уже в 1905 г. поддержал и развил Э. Бентли, создавший универсальный пятибуквенный код для телеграфных сообщений. Разбиение шифртекстов на пятибуквенные сочетания дошло до наших дней. Также «нормированные» по длине коды вытеснили коды, полностью основанные на использовании словарных величин.

Почти каждая промышленная или коммерческая компания разрабатывала секретные коды для собственных нужд. Появились коды торговцев автомобилями, коды банкиров, биржевых маклеров и т. д., что вызвало создание специальных профессиональных «криптографических групп», которые «по заказу» составляли секретные коды для пользователей с учетом их профессионального языка. Такие коды стоили достаточно дорого, они стали обычным рыночным товаром. Составляемые ими кодовые книги по объему были сравнимы со словарем английского языка. Появился рынок

торговли кодами. При этом возникли и разноязычные коды, т. е. коды, предназначенные для корреспондентов, говорящих на разных языках. Были созданы и многоязычные кодовые книги. Эти коды дошли до наших дней. Сигнал «SOS» (Спасите наши души) во всех странах сегодня воспринимается как просьба о помощи. Современные коды «сжимают» информацию более чем в 10 раз (этот эффект зависит, естественно, от богатства лексики открытого языка). Сжатие передаваемой по техническим каналам связи информации и в наши дни является актуальной задачей. При этом имеются в виду не только экономические аспекты передачи, но и скорость (оперативность) обмена сообщениями. Проблемы наиболее эффективного «сжатия» информации породили новое научное направление в теории связи – математическую теорию кодирования. Сегодня это научное направление исследований занимает одно из первых мест в теории связи.

Вернемся к проблемам, порожденным в криптографии появлением телеграфа. Сопряжение аппаратуры шифрования с техникой, передающей телеграфные сообщения, существенно повысило требования к быстродействию процесса шифрования. Шифрование при непосредственной передаче сообщения должно производиться в том темпе, который диктует телеграфный аппарат[14].

Телеграфная связь значительно увеличила объем передаваемых сообщений (в том числе, и секретных). Потребовалась разработка новых шифров с легкой сменой ключей. Это также стимулировало развитие криптографии. Одновременно телеграфная связь существенно затруднила перехват сообщений. Оказалось, что перехватить сообщение стало гораздо сложнее (в техническом смысле), чем перехватить гонца с документами или получить документы через почтамты. Конечно, можно было завербовать телеграфиста, но этот путь получения посланий оказался недостаточно эффективным. Поэтому начала создаваться техника тайного съема информации с телеграфных линий связи. Одновременно возникла проблема обнаружения такого тайного съема. Однако именно телеграф стал эффективным методом обеспечения оперативной связи между удаленными друг от друга абонентами в XIX в. Скорее всего, впервые электрический проводной телеграф для шифрованной связи в ходе боевых действий был применен русскими войсками во время Крымской войны 1853–1856 гг., а первые факты перехвата и дешифрования телеграфной информации имели место в 1861 г. во время гражданской войны в США 1861–1865 гг.[15]

В XIX в. применялось в основном так называемое предварительное шифрование сообщений. В этом случае отправитель зашифровывал передаваемое сообщение (в котором шифртекст

удовлетворял требованиям телеграфной передачи), а после этого относил шифрованное сообщение на телеграф. В XX в. такое замедление в передаче сообщений часто оказывалось неприемлемым. Потребовалось разработать методы, так называемой линейной передачи шифрованных сообщений; здесь аппарат шифрования (шифратор) встраивался непосредственно в аппаратуру передачи сообщений, так что передача шифрованного сообщения в принципе (в техническом смысле) не отличалась от передачи несекретного сообщения. В целом прав американский историк Дэвид Кан, утверждая, что «свой современный вид шифровальное дело получило благодаря телеграфу»[16].

Примечания

[1] *Соболева Т.А.* История шифровального дела в России. М.: ОЛМА-ПРЕСС-Образование, 2002. С. 197.

[2] Там же. С. 197–198.

[3] Там же. С. 198.

[4] Там же.

[5] Там же. С. 199.

[6] Там же. С. 201.

[7] Следует отметить, что Порта внес значительный вклад в развитие криптографии. Он является автором первого шифра биграммной замены (каждая пара букв открытого текста заменялась определенным знаком). Также Порта развил идею шифра многоалфавитной замены. Главным вкладом Порты в мировую криптографию является трактат «De Furtivis Literarum Novi» (1563), обобщивший достижения того времени в этой области.

[8] *Бабаш А.В., Гольев Ю.И., Ларин Д.А., Шанкин Г.П.* Криптографические идеи XIX века. Русская криптография // Защита информации. Конфидент. 2004. № 3. С. 90–96.

[9] *Соболева Т.А.* Указ. соч. С. 203.

[10] Там же. С. 204.

[11] Там же. С. 205.

[12] Там же. С. 207.

[13] Там же.

[14] *Бабаш А.В., Гольев Ю.И., Ларин Д.А., Шанкин Г.П.* О развитии криптографии в XIX веке // Защита информации. Конфидент. 2003. № 5. С. 90–96.

[15] *Гольев Ю.И., Ларин Д.А., Тришин А.Е., Шанкин Г.П.* Криптографическая деятельность в США XVIII–XIX веков // Там же. 2004. № 6. С. 68–74.

[16] *Kahn D.* The codebreakers. N. Y.: Macmillan Publ. Co., 1967. C. 111.