МЕЖДУНАРОДНАЯ СТАНДАРТИЗАЦИЯ и информационная безопасность

Н.Борисова, заместитель директора по науке и технике ЦМС им. А.С.Попова

DOI: 10.22184/2070-8963.2017.64.3.46.51

Как свидетельствует история, в телекоммуникациях международная стандартизация и информационная безопасность – две стороны одной медали, диаметрально противоположные проявления одной сущности, неразрывно связанные и неотделимые друг от друга.

История вопроса

Проблемы информационной безопасности имеют давнюю историю, начало которой можно отнести к тем временам, когда люди обменивались посланиями с помощью гонцов. Послание можно было изъять, прочитать, заменить и т.п., денежное отправление – выкрасть. Трудности при этом, безусловно, были, и злоумышленникам приходилось их преодолевать самыми разными способами. Но представьте себе, насколько бы облегчилась их задача, если бы заранее были известны: личность гонца (со всеми достоинствами и недостатками); маршрут следования и места остановок; вид оружия, имеющегося у гонца, и сведения о сопровождающей охране; способ упаковки послания, примененная при написании письма кодировка и т.п. Значимость информации, приведенной в данном примере, сродни той, которой обладают хакеры, фрики и прочие "научные хулиганы", взламывающие компьютерные, телекоммуникационные устройства и сети, построенные по единым стандартизированным принципам.

Прежде чем привести ряд примеров из истории электросвязи, свидетельствующих о том, какую неоднозначную роль играет международная стандартизация в борьбе за информационную безопасность, обратимся к историческим истокам некоторых терминов.

Известный в области радиотехники и электротехники английский ученый Джон Амброз Флеминг "научным хулиганством" (от англ. scientific hooliganism) и "поруганием традиций Королевского института" охарактеризовал на страницах "Таймс" несанкционированный доступ в радиосистему Маркони, совершенный в процессе публичной демонстрации возможностей нового вида связи. Произошло это летом 1903 года в Лондоне в знаменитом лекционном театре Королевского института. Беспроводная передача сигналов еще не получила широкого распространения и представляла большой научный интерес. План презентации возможностей новой аппаратуры предполагал, что Маркони, находясь в Корнуолле (300 км от Лондона), отправит радиосообщение, а его коллега Джон Амброз Флеминг, работавший консультантом Marconi Wireless Telegraph Company, примет этот сигнал. В анонсе показательной демонстрации было указано, что новый вид связи является "сверхконфиденциальным", и послание никто не сможет перехватить. В начале демонстрации, за несколько минут до того, как Флеминг должен был получить сообщение из Корнуолла, тишину нарушили сигналы морзянки. Сначала несколько раз было передано слово rats (от англ. rat – крыса, шпион),

а затем поступил короткий стих, обвиняющий Маркони в "надувательстве общественности". К счастью, постороннее вмешательство быстро прекратилось, и полностью сорвать основную презентацию не удалось, но доверие научной общественности к беспроводной связи как надежному средству передачи секретной информации было безвозвратно утрачено. Осуществивший "научное хулиганство" известный британский иллюзионист и изобретатель Джон Невил Маскелайн примерно за год до этого был нанят конкурентами Маркони – фирмой The Eastern Telegraph Company, занимавшейся прокладкой подводных кабелей между странами и континентами и опасавшейся, что беспроводная связь их разорит [1].

Маскелайн в совершенстве знал азбуку Морзе и, будучи иллюзионистом, использовал ее в трюках для связи с помощниками, невидимыми зрителям; он экспериментировал с электромагнитными волнами и искровым передатчиком, поражая зрителей тем, что поджигал порох, не прикасаясь к нему. В его лице The Eastern Telegraph Company нашла идеального хакера – человека, который стремился разобраться в принципах работы новой техники и выявить ее недочеты (действуя иногда весьма нестандартно). Именно такой смысл имел термин "хакер" (от англ. hack – подрубать, подрезать) на начальном этапе его применения; в наши дни его первоначальный смысл утрачен, и понятие "хакер" ассоциируется прежде всего с компьютерным злоумышленником.

С целью проверки заявленной "сверхконфиденциальности" системы Маркони Маскелайн на деньги фирмы The Eastern Telegraph Company построил 50-метровую радиомачту недалеко от Порткерно (графство Корнуолл) и убедился в простоте перехвата радиосигналов, которыми обменивались береговые службы и суда. Достаточно было иметь приемник, настроенный на ту же частоту, что и передатчик Маркони. Несанкционированное вторжение в демонстрацию, запланированную в Королевском институте, Маскелайну организовать было несложно. Он разместился в здании, расположенном неподалеку, имея простейший передатчик и телеграфный ключ; рассчитал время, когда сигнал должен был поступить из Корнуолла в Лондон, настроил передатчик на частоту, используемую Маркони, и без труда передал упомянутые выше телеграфные сообщения [1].

Еще до описанной выше демонстрации тем, кто имел отношение к практическому применению радиосвязи (эксплуатировал судовые радиостанции), уже было ясно, что передача телеграфных

Рис.1. Шифратор Чарльза Уитстона (сер. 1850-х гг.). Экспонат ЦМС им. А.С.Попова

депеш беспроводным способом требует не меньшей криптографической защиты, чем при использовании проводной телеграфной связи. Криптография – одна из старейших наук, ее история насчитывает несколько тысяч лет. Появление в 19 веке телеграфной связи способствовало развитию криптографии (рис.1). В проводных телеграфных сетях данные могли быть перехвачены только в том случае, если злоумышленник получал физический доступ к среде передачи, а в беспроводных сетях распространявшиеся в эфире с помощью электромагнитного излучения информационные сигналы мог перехватить любой приемник, находившийся в зоне действия радиостанции. Это обстоятельство незамедлительно было использовано на флоте, где радиосвязь нашла первое практическое применение. Так, во время Русско-японской войны, в марте 1904 года, командующий Тихоокеанской эскадрой вице-адмирал С.О.Макаров отдал приказ корабельным связистам в обязательном порядке записывать неприятельские депеши, определять направление на работающую радиостанцию, устанавливать организацию радиосвязи противника [2]. Таким образом, на заре радиосвязи появился новый способ доступа к секретной информации противника – радиоразведка. К началу Первой мировой войны с целью обнаружения работающих радиостанций противника стали использовать радиопеленгаторы (рис.2).

О международных правилах радиообмена и регламентации радиосвязи начали задумываться в самом начале ее применения, и с этой целью в 1903 году в Берлине была организована

Рис.2. Приемник детекторный пеленгационный Радиотелеграфного депо Морского ведомства (1912–1914 гг.). Экспонат ЦМС им. А.С.Попова

Предварительная международная конференция по радиосвязи. Первый свод международных правил (Международная радиотелеграфная конвенция) был принят на следующей Берлинской конференции в 1906 году. В приложении к Конвенции содержался первый регламент, регулирующий беспроводную телеграфную связь. Этот регламент за прошедшие 110 лет неоднократно дополнялся и пересматривался на многочисленных Всемирных конференциях, в настоящее время он носит название "Регламент радиосвязи".

Фрикинг и стандартизация

С одной стороны, Регламент радиосвязи и многие другие документы Международного союза электросвязи (МСЭ), направленные на оптимизацию радиообмена и унификацию разнообразного связного оборудования, сыграли важную координирующую роль в создании мировой инфраструктуры. С другой – документы МСЭ и других органов стандартизации, а также техническая документация стандартного оборудования общедоступны, и ими пользуются как те, кто разрабатывает и эксплуатирует технику связи, так и те, кто ее взламывает.

Прекрасной иллюстрацией к тому, как это происходило, служат известные истории с фриками. Фрикинг (от англ. phreaking) – сленговое выражение, образованное слиянием слов phone (телефон) и freak (выходка, шалость); обозначает мошенничество, основанное на нелегальном использовании телефонных сетей. Например, это может быть блокирование тарификационных систем, осуществление телефонных разговоров за чужой счет, незаконное подслушивание разговоров, кража паролей (PIN-кодов) и др. Человека, совершающего такие противоправные действия, называют фриком (от англ. phreak). Иногда используется термин "фрикер", созвучный с термином "хакер".

Появление фрикинга связано с использованием в телефонных сетях системы сигнализации. Телефонная сеть включает в себя ряд взаимосвязанных телефонных станций. Когда абонент набирает номер того, с кем хочет говорить, должно быть установлено соединение его телефонной станции со станцией вызываемого абонента. На заре телефонии функция установления соединения осуществлялась вручную, после появления автоматических телефонных станций (АТС) – с помощью системы сигнализации, которая по мере развития сетей совершенствовалась.

Впервые осуществлять сигнализацию посредством мультичастотных сигналов тональной частоты стали в США. В 1954 году компания Bell Telephone System, в то время крупнейший монополист в сфере предоставления телефонных услуг, перешла на новый стандарт телефонной сети. В 1955 году в журнале Bell System Technical Journal вышла статья под названием "О диапазонах частотных сигналов", где описывался процесс, с помощью которого посредством сигнальной системы того времени телефонные звонки переводились через транковые линии. В этой статье не были указаны номиналы мультичастотных тоновых импульсов, которые использовались при наборе номеров. Но в 1964 году, опубликовав эти номиналы частот, компания Bell Telephone System предоставила будущим фрикам всю информацию, необходимую для реализации оборудования, требуемого для генерации сигналов тех частот, которые позволяли совершать звонки бесплатно, полностью минуя систему выставления счетов и мониторинга [3].

Среди знаменитых американских телефонных фриков конца 1960-х – начала 1970-х годов следует упомянуть Джо Энгрессия, который мог насвистывать тон "ми" в высокой октаве, необходимый для установления контроля над телефонной линией. Джон Дрейпер, известный как Капитан Кранч, делал то же самое с помощью подарочного свистка, вкладываемого производителем в каждую коробку Cap&Crunch, содержащую кукурузные хлопья. Свисток воспроизводил звуковой сигнал частотой 2600 Гц. Именно эта частота использовалась телефонной компанией для предоставления междугородных услуг связи. Так родилось целое

"сообщество фриков". Чтобы расширить свои возможности по манипулированию телефонными номерами, фрики стали создавать устройства, которые назывались сначала Multi Frequency Box (многочастотная коробка); потом были переименованы в Blue Box (синяя коробка). Это были небольшие коробочки с кнопками и динамиком, позволявшие генерировать сигналы разных тональностей.

С технической точки зрения "синяя коробка" представляла собой устройство для имитации сигналов внутриполосной линейной и регистровой сигнализации с абонентской линии. Изобретателем "синей коробки" считается упомянутый выше Капитан Кранч. В 1971 году в журнале Esquire была опубликована большая статья Рона Розенбаума "Секреты маленькой синей коробки", в которой автор рассказал о сообществе фриков и самых известных представителях этого движения, об уязвимостях телефонных сетей компании Bell Telephone System и структуре "синей коробки".

В один из воскресных дней 1971 года этот журнал случайно попался 20-летнему студенту колледжа Стиву Возняку – одному из будущих основателей корпорации Apple. Идея создания "синей коробки" и ее потенциальные возможности настолько потрясли Стива Возняка, что он тут же позвонил своему приятелю 17-летнему Стиву Джобсу (тот еще учился в школе). На взгляд "технаря" Стива Возняка, в статье раскрывалось столько секретов, что изготовить "синюю коробку" и "начать создавать свои маленькие сети, чтобы пользоваться услугами больших", особого труда не представляло. В статье указывались реальные частоты 700 и 900 Гц, еще кое-какие сведения, но, чтобы приступить к собственному изготовлению "синей коробки", приятелям необходимо было иметь полный список частот, соответствующих всему набору цифр телефонной нумерации. И вот тут начинается самое интересное в контексте рассматриваемой в данной статье темы.

Воскресный день. Сразу после телефонного разговора приятели встречаются и направляются в Стэнфордский центр линейного ускорителя SLAC, где была большая библиотека с различными техническими изданиями. Ее двери никогда не закрывались (в том числе и по воскресеньям), чем Стив Возняк неоднократно пользовался, когда учился в старших классах школы, и уже потом, когда начал заниматься сборкой компьютеров. Информация, в которой нуждались будущие фрики, была найдена ими в Рекомендациях CCITT (Международный комитет по телефонии и телеграфии). Из воспоминаний Стива Возняка: "Я перелистывал страницы, и внезапно что-то меня остановило. Вот оно – полный список номиналов частот для мультичастотного телефонного оборудования. И точно, все было так, как и писал Esquire: "1" состояла из сигналов в 700 и 900 Гц, "2" – 700 и 1100 Гц, "3" – 700 и 1300 Гц. Я замер, схватил Стива за руку и чуть было не закричал. Мы оба смотрели на этот список, у нас внутри все бурлило. Мы лишь бубнили: "Ого, блин!", и "Ух ты, это все правда"! Я трясся сильнее, у меня аж мурашки побежали по телу. Эврика! По пути домой мы только об этом и говорили. Мы были сильно взволнованы. Теперь мы знали, что сможем собрать такую штуку сами" [3].

Первый изготовленный друзьями экземпляр "синей коробки" (аналоговый) оказался несовершенным, он "не позволял перенастраивать частоты, они воспроизводились с колебаниями". Тогда Возняк сделал полностью цифровое устройство, воспроизводившее частоты с необходимой точностью. Нельзя сказать, что он сразу же заставил свою "синюю цифровую коробку" работать – по его словам, "так в инженерии и не бывает". Но то, что получилось в конечном итоге, Возняк, назвав фантастикой, прокомментировал следующим образом: "После этого я уже нигде никогда не делал ничего столь инновационного в моих схемах – ни

в Hewlett-Packard, ни в Apple. Это громкое заявление, ведь мои схемы всегда признавались инновационными. Но та штука была наихитрейшей" [3].

Дальнейшая история о том, как два Стива (Возняк – будущий гениальный компьютерщик, и Джобс – будущий гениальный маркетолог) поддались соблазну легкого заработка, организовали кустарное производство и продажи "синих коробочек" среди студентов и местных жителей, а также о том, как затем они достаточно быстро отказались от рискованного бизнеса, прямого отношения к рассматриваемой теме не имеет. Но на некоторые аспекты этой истории следует обратить внимание.

Чаще всего фрикингом занимаются отдельные талантливые энтузиасты: связисты и компьютерщики, постоянно пополняющие свои знания за счет многих источников, важное место в которых занимают телекоммуникационные стандарты, общедоступная техническая документация. Тонкая грань отделяет техническое любопытство фриков от противоправных действий. Стив Возняк написал об этом так: "Нашим родителям, знавшим, чем мы занимались, мы обещали, что никогда не будем совершать такие звонки из дома. <...>. Я не собирался делать ничего плохого. Я не хотел лишать телефонные компании дохода – я хотел <...> использовать свои устройства для поиска уязвимых мест в системе" [3]. В итоге два Стива после того, как их чуть не поймали с поличным, отказались от преступной деятельности. Благо, что к тому времени у них уже появилась идея создать в гараже свой маленький бизнес по сборке компьютеров, положивший начало компании Apple. Не всегда все благополучно заканчивается в подобных историях, особенно если их участники не считают "интеллектуальные" грабежи преступлением и не верят в неизбежность наказания.

В процессе эволюции

Со временем, когда внутриполосную сигнализацию SS-5 (CCITT Signalling System No. 5) сменил общий канал сигнализации (CCS, Common Channel Signalling), в частности ОКС-7 (SS-7, CCITT Signalling System No. 7), устройства типа Blue Box стали терять свою актуальность, но появился целый ряд других, адаптированных под новые модели сетевого оборудования. Эволюционировать подобным устройствам почти одновременно с развитием телекоммуникационных сетей позволяют все те же международные стандарты, техническая документация, а также книги и статьи, воспроизводящие все технические подробности новых технологий и аппаратно-программных средств. Над тем, что таким образом легко можно находить уязвимые места, специалисты иронизируют, называя подобные публикации "поваренными книгами"; "рецептами" в них являются технические сведения, такие как структура сетей и каналов связи, описание интерфейсов и протоколов, конкретные технические параметры и др. Например, в одном из описаний практики фрикинга в России в конце 1990-х годов есть такой фрагмент: "Конечно, старые ошибки были учтены, и SS5 уже никто не применял, использовалась российская система сигнализации. Но фрикеры были уже умными, и многие из них изучили и российские системы. Тем более, что незадолго до этого вышла "поваренная книга фрикера" – бестселлер "Сигнализация в сетях связи" (в честь которой эта серия статей названа "Сигнализация в сетях связи – 2")" [4].

В период с начала 1980-х до конца 1990-х годов, отмеченный повышенной активностью фриков, взламывавших традиционные телефонные сети общего пользования и новые сети мобильной телефонии, появились персональные компьютеры, начали функционировать первые компьютерные сети и стал набирать популярность интернет. Соответственно, количество потенциальных угроз существенно возросло, и в мире заговорили о кибербезопасности. Ответом на противоправные действия киберпреступников стало усиление внимания к вопросам защиты информации и каналов связи со стороны всех международных организаций, занимавшихся вопросами стандартизации, в том числе МСЭ [5].

В начале 2000-х годов стали выпускаться обзоры содержания и применения действующих Рекомендаций МСЭ-Т для обеспечения защищенной электросвязи. Поскольку работа МСЭ осуществляется исследовательскими группами, в 2004 году было принято решение образовать на базе группы "Сети передачи данных и телекоммуникационное программное обеспечение" ИК17 МСЭ-Т "Безопасность, языки и телекоммуникационное программное обеспечение"; в 2009 году пошли дальше – эта группа стала называться "Безопасность".

В период 2003–2005 годов Всемирная встреча на высшем уровне по вопросам информационного общества (ВВУИО) определила МСЭ как единственного координатора по направлению действия ВВУИО "Доверие и безопасность при использовании ИКТ". В 2007 году генеральный секретарь МСЭ запустил в действие механизм сотрудничества по данному вопросу – Глобальную программу кибербезопасности, которую одобрили

все члены МСЭ. Всемирные ассамблеи по стандартизации электросвязи (Флорианополис, 2004 г.; Йоханнесбург, 2008 г.; Дубай, 2012 г.; Хаммамет, 2016 г.) с каждой новой встречей все большее внимание уделяют вопросам кибербезопасности. Одним из актуальных признано направление, связанное с глобальной культурой кибербезопасности.

Если рассуждать о технической стороне проблемы кибербезопасности, то исторический опыт свидетельствует: мы имеем дело с двумя сторонами медали – разными, диаметрально противоположными проявлениями одной сущности, неразрывно связанными и неотделимыми друг от друга. Речь идет о том, что столь необходимая для мировой телекоммуникационной отрасли техническая стандартизация делает уязвимыми с точки зрения информационной безопасности все виды связи, несмотря на многочисленные попытки Международного союза электросвязи противостоять этому. Единственный способ борьбы со "злоумышленниками" видится не столько в технических, сколько в правовых и этических методах. Они не забыты в концепции "Глобальной культуры кибербезопасности", но, возможно, роль и значение их еще недостаточно оценены.

ЛИТЕРАТУРА

1. Charlotte New. Hacking at the Royal Institution [Электронный ресурс]. URL: http://www.rigb.org/blog/2014/november/hacking-at-the-royal-institution (дата обращения 15.03.2017).
2. **Горелов О.И.** Адмирал Макаров: "Помни войну!" (к 100-летию окончания Русско-японской войны 1904–1905 гг.) // Национальные интересы. 2005. № 5. С. 34–37.
3. **Возняк С., Смит Дж.** Стив Джобс и Я. Подлинная история Apple/Пер. сангл. А.В.Пряжникова, А.С.Ширикова. – М.: Эксмо, 2012–288 с.
4. **Скоблов А.** Russian Phreaker's Manual или "Сигнализация в сетях связи – 2" – попытка написать аналог The Official Phreaker's Manual об особенностях фрикинга в России. [Электронный ресурс]. URL: http://www.aboutphone.info/js/phreak.html (дата обращения 15.03.2017).
5. Международный союз электросвязи [Электронный ресурс]. URL: http://www.itu.int/ru (дата обращения 15.03.2017).