ГУМАНИТАРНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.В. Котенко, К.Е. Румянцев
Россия, г. Таганрог, ТРТУ

КРИЗИС ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ УГРОЗ ТЕРРОРИЗМА

Сегодня информационная безопасность, как составная часть безопасности жизнедеятельности человечества в целом, находится в состоянии глубокого кризиса, последствия которого в условиях наблюдаемого возрастания и глобализации угроз терроризма непредсказуемы и могут оказаться критическими. На фоне широко рекламируемых в последнее время научных и инженерных достижений в области обеспечения информационной безопасности такое утверждение может показаться на первый взгляд, по меньшей мере, странным. Это объяснимо, если учесть, что понятие кризиса определяет затруднительное, тяжелое положение или резкий крутой перелом в чём-либо, например в болезни. Образно говоря, возникает вполне закономерный вопрос: как можно говорить о кризисе какой-то «болезни», если не установлена сама болезнь, то есть не выяснены её «симптомы» и не определён «диагноз»?

Симптомы и диагноз

При внимательном анализе истории развития систем и методов информационной безопасности можно выявить, по крайне мере, два деструктивных явления, необычайно бурно прогрессирующих в последнее время.

Во-первых, необходимо отметить, что используемые до настоящего времени методы и системы информационной безопасности изначально были неспособны обеспечить гарантированную (абсолютную) защиту информации. Однако, если на заре развития и применения данных методов и систем случаи успешного криптоанализа были единичными и рассматривались как исключение из правил, то сегодня, ввиду их массовости, они воспринимаются как правило. Это уже не симптом самой «болезни» - это симптом её кризиса.

Во-вторых, появление систем информационной безопасности вполне объективно повлекло за собой возникновение лиц, занимающихся их криптоанализом. На начальном этапе процессы подготовки, обучения и действия этих лиц находились под жёстким контролем государственных служб и строго регламентировались ими. Однако со временем по ряду причин данные процессы начали выходить из-под государственного контроля. Это привело к появлению своеобразного неуправляемого сообщества так называемых хакеров, первоначально включавшее энтузиастов-любителей. К сожалению, это представление о нём сохраняется и до сих пор. Поразительно, но остаётся без внимания тот факт, что сегодня это сообщество уже представляет собой развивающуюся вне государственную структуру с ярко выраженными центростремительными тенденциями, со своими философской концепцией, идеологией и источниками финансирования. Конечно, всё это находится ещё в зачаточном состоянии. Но что мешает предположить, что со временем человечество может столкнуться с мощной и организованной структурой, более опасной чем традиционный терроризм во всех его проявлениях, так как она будет воплощать терроризм уже на интеллектуальном и духовном уровнях? Может быть, какие-то силы уже сейчас предвидят и планируют это? Свидетельств этому при желании можно получить предостаточно, но это уже тема отдельного исследования. Итак, налицо второй наиболее опасный по возможным последствиям «сим-

птом» кризиса «болезни».Обозначив «симптомы», можно попытаться поставить диагноз самой «болезни».

Отметим общую тенденцию: совершенствование современных методов и систем информационной безопасности сопровождается повышением их сложности. Казалось бы, всё очевидно – более совершенная система должна быть более сложней. Всё было бы так, если не обращать внимания на то, что с самого начала развития систем и алгоритмов данного класса общий подход к их созданию оставался и остаётся неизменным. В основе этого подхода лежит использование так называемых рекуррентных последовательностей, образующие полиномы которых являются неприводимыми и примитивными. Такие последовательности обладают максимальным периодом. Сегодня можно только догадываться, как создавались первые алгоритмы этого класса, так как всё происходило в режиме строгой секретности. Однако с абсолютной уверенностью можно утверждать, что учёные и разработчики, участвовавшие в этом процессе, были знакомы с работами известных математиков, определивших условия теоретической (абсолютной) недешифруемости криптографических систем. Из них следовало, что для достижения абсолютной недешифруемости системы ключи должны формироваться по абсолютно случайному закону, а их число – стремиться к бесконечности. Однако создаваемые ими алгоритмы изначально не соответствовали условиям абсолютной недешифруемости. Остаётся только предполагать, почему был выбран именно этот подход. По-видимому здесь сыграл роль целый комплекс причин, базирующихся на простоте технической реализации и надежде в последующем максимально приблизится к выполнению условий теоретической недешифруемости. Именно эта надежда определяла весь последующий процесс развития данных алгоритмов как по пути аппаратурной, так и по пути программной их реализации. Увеличивалось число РРС, участвовавших в формировании ключевой последовательности, вводились хеш-преобразования, создавались сопутствующие алгоритмы имитозащиты, аутентификации, подписи и т.п. Всё это естественно требовало математической поддержки. В результате создавался мощный математический аппарат, объясняющий правомочность предпринимаемых практических шагов. К сожалению, надежда не оправдалась. Сегодня мы видим, что кризис «болезни» наступил. Диагноз – невыполнение условий теоретической недешифруемости. Образно создавшуюся ситуацию можно сравнить с ситуацией, когда врачи в ходе лечения болезни, диагноз которой они прекрасно знают и которая требует оперативного хирургического вмешательства, ограничиваются применением медицинских препаратов и общеукрепляющих процедур. Такой подход при прогрессирующей болезни требует применения всё более и более сильнодействующих препаратов. Как скажется на организме больного такое лечение, может предсказать и человек без медицинского образования. Метастазируя, болезнь постепенно будет нарушать естественные функции организма, что приведёт в конечном итоге к трагическому исходу. Не аналогичная ли ситуация наблюдается сегодня с информационной безопасностью? С этих позиций становится понятно, почему применение всё более и более сложных и эффективных алгоритмов информационной безопасности, которые казалось бы должны повышать криптостойкость систем, всё чаще и чаще в последнее время приводит к обратным результатам. Не свидетельствует ли это о нарушении «естественных функций» информационной безопасности и необходимости кардинальных («хирургических») изменений, заключающихся в замене общепринятого подхода на новые – более эффективные? В этом плане образное представление создавшейся ситуации высвечивает ещё одну довольно серьёзную проблему. Ситуация, когда врач отказывается от хирургического вмешательства, может объясняться двумя причинами. Первая состоит в том, что он искренне убеждён, что это

вмешательство повредит больному. Но нельзя исключать (пусть не обидятся врачи, но сейчас это реально) и ситуацию, связанную с финансовыми вопросами. Часто недобросовестному врачу оказывается выгодно длительное лечение больного, который оплачивает свое лечение и всё более и более дорогостоящие препараты. Здесь уже оказывают влияние законы бизнеса, нередко коверкающие врачебную этику. Взгляд с этих позиций на состояние информационной безопасности выявляет довольно настораживающую картину.

Необходимо отметить, что всё историческое развитие криптографии (в начале как искусства и затем как науки) происходило в строгом соответствии с основным законом философии – законом единства и борьбы противоположностей, когда усилия, направленные в противоположных направлениях (криптозащита и криптоанализ), способствовали развитию науки о защите информации в целом. Этот закон продолжал действовать и на первом этапе усиления прикладной направленности данной науки (середина пятидесятых годов двадцатого столетия), когда начинали создаваться системы информационной безопасности. Определяющими стимулирующими факторами в то время как для развития криптозащиты, так и для развития криптоанализа являлись идеологические, патриотические, национальные и государственные интересы. Однако со временем всё больший вес, как стимулирующий фактор, начинают приобретать финансовые интересы. Они становятся определяющими на этапе фактического выхода процессов развития информационной безопасности из-под контроля государств. Это приводит в действие уже новые, пока ещё недостаточно изученные, философские законы, в основе которых лежит философия бизнеса в чистом виде. Разработчикам алгоритмов информационной безопасности уже не выгодно стремиться к абсолютной недешифруемости этих алгоритмов. В этом случае они окажутся финансово невостребованными. Оптимальной для них становится разработка ограниченно эффективных алгоритмов, представляющих интерес для покупателей только на определённом отрезке времени. Тогда появляется возможность разработать новый, более сложный алгоритм и продать его через некоторое время тому же покупателю. И так далее. Кроме этого, разработчики оказываются исключительно заинтересованными в существовании некой противоборствующей силы (например, в виде хакеров), угроза которой будет держать покупателя в постоянном напряжении. Это напряжение психологически будет готовить его к восприятию более высоких цен. Отсюда более высокие прибыли. С другой стороны, такая позиция выгодна и для так называемого сообщества хакеров. Появление ограниченно эффективных алгоритмов информационной безопасности создаёт им стимул для работы и обеспечивает рынок услуг. При этом сообщество хакеров оказывается заинтересованным в рекламе эффективности существующих алгоритмов, а сообщество разработчиков – в рекламе эффективности хакеров. Налицо общность экономических и финансовых интересов. Так как это явление практически не изучалось, можно делать только предположения о дальнейшем развитии последствий такого кризиса информационной безопасности. Самый неблагоприятный прогноз, который можно предположить,– это появление некой самодостаточной замкнутой надгосударственной централизованной структуры, со своей идеологией, философией, культурой, финансовыми потоками, чётким разделением труда и, может быть, органами власти, основной целью которой будет интеллектуальное и духовное порабощение человечества. Данный прогноз ужасает, но как говорится, всегда надо готовиться к худшему. Тем более предпосылки этого худшего можно заметить уже сегодня. Прежде всего, это монополизация разработок в области информационной безопасности на уровне уже транснациональных монополий. К этому добавляются центростремительные процессы в сообществе хакеров и в дополнении ко всему, явно просматривающаяся в послед-

нее время тенденция сближения данных структур. Характерной приметой этого являются участившиеся случаи привлечения хакеров для работы в транснациональных корпорациях. Если учесть, что эти предпосылки не могут не обеспечиваться огромными финансовыми ресурсами, то самый неблагоприятный прогноз приобретает уже реальные очертания. Как следствие этого, в несколько ином свете воспринимается целый ряд событий последнего времени. Так, например, становится понятным объективный характер жёсткого, так называемого «антихакерского» закона, принятого сравнительно недавно в США. В данном случае государство, как самодостаточная и самоорганизующаяся функциональная система, объективно включает защитные механизмы противодействия угрозе, способной поставить под вопрос сам факт его существования. Вполне понятно, что «жёсткость» этих защитных механизмов должна быть прямо пропорциональна степени опасности угроз. Вспомним, какая интернациональная пропагандистская кампания была развёрнута против отмеченного закона. Весьма сомнительно, что она была стихийной. За ней определённо стояли некие мощные организующие силы. Что это за силы? Может быть сейчас, когда мы говорим о возможности появления некой монстр-структуры, она уже существует? Итак, диагноз и причины «болезни» информационной безопасности установлены. К сожалению, полученный диагноз оказался, как часто говорят, не достаточно обнадёживающим. Возникает вопрос: возможно ли ещё эффективное «лечение»? На наш взгляд – ещё возможно, если будет выбран эффективный курс.

Возможные пути преодоления кризисных явлений

Пользуясь медицинской терминологией, можно отметить, что лечение любой болезни должно включать лечение её причин и возможных последствий. В нашем случае «лечение причин» предполагает поиск принципиально новых подходов к решению проблем обеспечения информационной безопасности, предусматривающих выполнение условий абсолютной недешифруемости: Ключи должны формироваться по абсолютно случайному закону; Число ключей N_k должно быть бесконечным.

Отметим, что к этому же выводу в конечном итоге приводит использование любого из известных методов анализа эффективности обеспечения информационной безопасности. Ответим на вопрос: возможно ли практически обеспечить выполнение указанных условий, при использовании принятого в настоящее время подхода? Без сомнения ответ будет отрицательным. Прежде всего данный подход изначально предполагает дискретное множество ключей, то есть практически исключает выполнение условия $N_k = \infty$. Кроме этого, выполнение в процессе практической реализации условия абсолютно случайного характера ключей делает невозможным формирование идентичных ключевых последовательностей на передаче и приёме. Если к тому же учесть возникающие при этом практически неразрешимые проблемы синхронизации, становится понятным скептицизм в отношении практического достижения условий теоретической недешифруемости, господствующий в настоящее время в научных и инженерных кругах. По-видимому, именно этот скептицизм в многом объясняет возведение в догму мнения о том, что практически обеспечить выполнение условий теоретической недешифруемости невозможно. Не может не поражать, как загнанная в рамки этой догмы научная и инженерная мысль с какой-то обречённостью стремится максимально приблизиться к невозможному по определению самой догмы. Путь, определённый этими рамками, один – повышение сложности алгоритмов защиты. Только так можно обеспечить дальнейшее увеличение N_k, максимальное сокрытие псевдослучайного характера ключевой последовательности. Как не парадоксально, при этом всё

большее значение приобретает ещё одна проблема – проблема защиты самих алгоритмов защиты. Вполне понятно, чем сложнее алгоритм, тем сложнее предусмотреть варианты несанкционированного доступа к нему и воспрепятствовать им. Не означает ли это, что может наступить предел сложности, при котором защита алгоритма от несанкционированного доступа уже будет невозможна, что неизбежно приведёт к девальвации его практической ценности? Этот вопрос не так и беспочвенен на фоне постоянно возрастающего числа фактов «взлома» систем защиты информации, за которыми уже просматривается определённая тенденция. Как ни странно, этот вопрос до сих пор не только не исследовался, но даже не поднимался в той или иной постановке. Казалось бы, проведённые рассуждения подводят нас к неутешительному выводу о том «лечение» причин «болезни» информационной безопасности, находящейся в состоянии кризиса, невозможно. Более того, одни указывают на обязательно возможное обострение этого кризиса, со всеми очевидными последствиями. Так уж всё безнадёжно? Да, если находится в плоскости традиционного подхода, ограничиваясь рамками его догм. Возможен ли выход за эти рамки? Предварительные результаты исследований, проводимых авторами в этом направлении, позволяют уже сейчас дать положительный ответ на этот вопрос. Если опять возвратиться к условиям АНДШ, то нетрудно заметить, что их обеспечение возможно при равенстве $H_k(0) = \infty$. Это наблюдение подводит к вопросу: каким должен быть ключ, чтобы его энтропия была бесконечной? Обратившись к теории информации, находим ответ: ключ должен быть непрерывнозначной (аналоговой) величиной. Таким образом, можно сделать вывод, что **для выполнения условий абсолютной недешифруемости, необходимо осуществить переход от дискретного выборочного пространства ансамбля ключей к непрерывному**. Очевидно, что такой переход в рамках общепринятого в настоящее время подхода к обеспечению информационной безопасности невозможен. Это объясняется тем, что переход к непрерывнозначному выборочному пространству отрицает целесообразность использования самих дискретных алгоритмов формирования ключей, в том числе и основанных на формировании псевдослучайных последовательностей максимального периода. Кроме этого, такой переход порождает довольно серьёзную проблему согласования непрерывнозначных ансамблей ключей с цифровой стратегией развития систем обработки и передачи информации. По всей видимости, именно эти соображения во многом определили тот факт, что до сих пор **возможность использования аналоговых ансамблей ключей** не только не исследовалась, но даже и **не рассматривалась, как объект исследований**. Однако, как ни странно, выход можно найти именно в этом направлении.

Оказалось, что изначально задавшись целью исследования возможности применения аналоговых ансамблей ключей для защиты информации в цифровых системах, можно получить обнадёживающие результаты. Эту возможность открывает применение аппарата **теории виртуальных выборочных пространств.** Ввиду того, что данный аппарат был **открыт** сравнительно недавно и сейчас находится только в стадии разработки и апробации, говорить об окончательном успехе ещё преждевременно. Однако уже первоначальные результаты его применения внушают оптимизм. Суть открытого подхода заключается в формировании у законных отправителей и получателей так называемых виртуальных аналоговых выборочных пространств ключа, которые для посторонних наблюдателей приобретают форму реальных. Таким образом, обозначается по крайне мере один путь выхода из кризиса, определяющий реально возможный «курс лечения» причин «болезни» информационной безопасности. Нет сомнения, что существуют и другие, пока ещё не неизвестные и, быть может, более эффективные пути. Говорить об этом позволяет вера в неиссякаемые возможности человеческого разума.

Вполне понятно, что «лечение» самой болезни должно сопровождаться «лечением» уже существующих её последствий. Решение данной проблемы значительно осложняется тем, что сегодня не только не изучен, но и в достаточной мере не осознаётся даже сам факт существования этих последствий. Поэтому давать какие-то даже общие преждевременные рекомендации здесь представляется довольно рискованным занятием. Решение этой проблемы возможно только при условии использования мощного потенциала научной и инженерной мысли. Первым шагом к этому может стать широкая и плодотворная дискуссия по вопросам и проблемам, поднятым в настоящей работе.

Выводы

Выдвинутая в работе гипотеза о кризисе информационной безопасности имеет реальную почву. Прогноз последствий этого кризиса показывает возможность зарождения в недрах человеческой цивилизации некой надгосударственной террористической монстр-структуры, нацеленной на интеллектуальное и духовное порабощение человечества. Первым шагом её движения к этой цели может оказаться (а может уже есть) так называемый интеллектуальный и духовный терроризм, смыкающийся с обычным терроризмом во всех его проявлениях.

Анализ выдвинутой гипотезы позволяет прийти к следующим основным выводам: 1. Кризис информационной безопасности является в настоящее время реальным фактом глобального масштаба. 2. Последствия этого кризиса могут быть трагическими для человечества. 3. Необходимо кардинально менять существующий подход к решению задач обеспечения информационной безопасности. 4. Успешный поиск новых подходов возможен уже сейчас, свидетельством этому служат результаты ряда исследований известных авторам. 5. Необходима широкая и бескомпромиссная дискуссия по вопросам кризисных явлений в области обеспечения информационной безопасности в условиях возрастания угроз терроризма.

С.В. Дворянкин
Россия, г. Москва, МГТУ им. Н.Э. Баумана

ПРОТИВОДЕЙСТВИЕ НЕГАТИВНЫМ МУЛЬТИМЕДИЙНЫМ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИМ ВОЗДЕЙСТВИЯМ

В последнее время перед обществом все более остро ставится проблема информационно-психологической безопасности. Современные технические, технологические, информационные и организационные системы, а также люди, коллективы людей и общество в целом сильно подвержены внешним информационным воздействиям, последствия которых могут носить не просто тяжелый, но в некоторых случаях и трагический характер. Действительно, уже сегодня имеющиеся на открытом рынке предложений развитые программно-аппаратные средства ввода-вывода и обработки аудио видео сообщений, текста и графики позволяют проводить практически любые преобразования над аудио, видео, графической, анимационной и текстовой информацией, комбинацию перечисленных видов которой с учетом соответствующих аппаратных средств принято называть одним словом - мультимедиа. Наиболее полно последствия применения мультимедийных технологий, в том числе и с целью информационно-психологических воздействий на индивидуальное и общественное сознание проявляются в индустрии развлечений и в средствах массовой информации. Так ярким примером использования мультимедийных компьютерных технологий в человеческой деятельности является создание специальных видео- и аудио- эффектов в современной киновидеоиндустрии и на телевидении: наложение кадров, различные виды аудио- видеомонтажа в спе-