УДК 004.681.3

Г.Н. Гулак,
кандидат технических наук

МОДЕЛИРОВАНИЕ НА ЭТАПЕ ОЦЕНКИ БЕЗОПАСНОСТИ ШИФРАТОРОВ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

У статті розглядаються моделі, що використовуються під час проведення експертизи шифротехніки. Запропоновано уточнені моделі порушника безпеки, шифратора як електронного пристрою з відмовами.

Ключові слова: *шифратор, модель, експертиза, безпека.*

В статье рассматриваются модели, используемые при проведении экспертизы шифротехники. Предложены уточненные модели нарушителя безопасности, шифратора как электронного средства с отказами.

Ключевые слова: *шифратор, модель, экспертиза, безопасность.*

In article the models used at carrying out of examination cryptotechnics are considered. The specified models of the safety infringer, an encoder as electronic means with refusals are offered.

Keywords: *encryptor, model, evaluation, safety.*

Создание адекватных моделей субъектов, объектов и процессов при проведении оценки (экспертизы) фактически достигнутого уровня безопасности средства криптографической зашиты конфиденциальной информации (далее шифратора) является определяющим фактором обеспечения высокого качества и оперативности выполнения экспертных работ.

Под безопасностью шифратора будем понимать интегральную характеристику его криптографических и инженерно-криптографических свойств, а также уровня защищенности от утечки незашифрованной информации за счет побочных электромагнитных излучений и наводок.

Актуальность решения этой задачи обусловлена тем, что в настоящее время этап экспертизы, составляющий по времени значительную часть всей продолжительности создания новой техники, все еще недостаточно автоматизирован. Большинство исследовательских процедур требуют непосредственного участия экспертов, при этом для анализа сложнейших алгоритмических и схемотехнических решений харатерны высокая трудоемкость и весьма высокая вероятность ошибки.

Решение данной проблемы может быть получено на основе глубокой проработки формальных моделей процессов, субъектов и объектов криптографической защиты с целью создания современных комплексов автоматизации экспертных исследований.

Ключевое значение для процедур экспертизы имеют:

1. Модель нарушителя безопасности системы защищенного обмена;

2. Модель криптографической системы на уровне формального описания криптографических процедур;

3. Модель системы генерации и управления ключевыми данными;

4. Модель атак на криптографическую систему (модель угроз);

5. Модель шифратора, как микроэлектронного устройства, подверженного случайным сбоям и отказам;

6. Модель поведения системы "шифратор-оператор" в различных условиях эксплуатации;

7. Модель – программный имитатор работы шифратора с помощью компьютера;

8. Модель шифратора как основного технического средства, используемого для обработки информации с ограниченным доступом;

9. Модель взаимодействия в системе специальной связи.

При этом модели 1–4 и 6 используются при проведении исследований криптографической стойкости выбранной криптографической схемы (алгоритма шифрования плюс система генерации и управления ключами). Областью применения моделей 4–7 и 9 является верификация реализованных в шифраторое алгоритмов и иные задачи инженерно-криптографического анализа схемотехнических решений, принятых на этапе его технического проектирования.

Модели 4,5,7,8 необходимы для проведения исследований на наличие технических каналов утечки из шифратора незашифрованной и критичной для его безопасности информации.

Модель информационного ресурса, определяющая особенности жизненного цикла защищаемой информации, имеет по отношению к экспертизе шифратора вторичное значение, если исследуемое средство по отношению к выбранной модели нарушителя декларируется стойким. В случае так называемой "временной" стойкости шифрования, что является допустимым в некоторых ситуациях (например, для нужд управления авиацией или передачи служебной информации по оперативной/текущей обстановке), можно воспользоваться одной из моделей, учитывающих изменение ценности информации в течение ее жизненного цикла [1].

Изменение ценности информации от времени можно оценить приблизительно с помощью выражения: $C(t)=C_0 e^{-2,3t/\tau}$, где C_0 – ценность информации в момент ее возникновения; t – время от момента ее возникновения до момента определения текущей стоимости; τ – время от момента возникновения до момента старения информации.

Из приведенного выражения, в частности, следует, что в случае дешифрования информации за время τ "остаточная" стоимость информации к этому моменту будет составлять около 10 % от первоначальной.

Очевидно, что этим же выражением можно также воспользоваться для оценки правильности выбора периода смены ключей.

Остановимся на некоторых из перечисленных моделей более подробно.

Нормативными документами системы криптографической защиты определяется четыре уровня возможностей нарушителя [2]. Наибольшую опасность для конфиденциальной информации представляют нарушитель корпоративного типа (в случае коммерческой информации) и нарушитель типа специальной службы развитого в научно-техническом плане государства, если речь идет об информации, принадлежащей государству.

Вместе с тем, рамки нормативно-правового акта существенно ограничивают возможности технической спецификации моделей, поэтому полагаем, что для

оценки уровня безопасности шифротехники необходимо уточнить категории нарушителя системы безопасности с учетом современного видения методов и средств [3], имеющихся у него на вооружении, а также способов их применения (табл. 1).

Модель нарушителя строится с учетом особенностей конкретной области применения шифротехники (используемых технологий обработки информации) и может быть охарактеризована в терминах, приведенных в таблице. При этом она отражает потенциал нарушителя, его финасовые и иные ресурсные возможности, априорные знания, время и место действия, потенциальные затраты, которые необходимы для достижения поставленных целей.

Таблица 1

Параметры классификации нарушителя безопасности криптосистемы

№№ п.п.	Группа признаков нарушителя	Содержание признака
1.	***Уровень знаний***	• степень знания криптоалгоритмов, протоколов, методов генерации и управления ключами, использованных в конкретной шифросистеме; • наличие информации о точных значениях сменных параметров и функциональных особенностях системы; • знание порядка и особенностей эксплуатации шифротехники в конкретной системе специальной связи; • уровень методологической и научной базы проведения атак на криптографические системы; • знание структуры; • знание функций и механизмов защиты от несанкционированного вмешательства в работу шифратора.
2.	***Уровень возможностей и оснащенности***	• возможности перехвата шифрованных сообщений с требуемой полнотой и качеством; • наличие финансовых ресурсов для покупки/разработки специальных технических и программных средств; • наличие кадрового потенциала; • возможности собственной и привлеченной ЭВТ для распараллеливания вычислений; • наличие материально-технических расходных ресурсов; • потенциал скрытого добывания необходимых данных о шифросистеме (скрытые каналы); • наличие образца шифратора; • возможность применять методы и средства активного воздействия на шифратор, систему генерации и управления ключами (модификация и подключение дополнительных технических средств, влияние на каналы передачи данных, внедрение аппаратных и программных закладок, использование специальных инструментальных и технологических программ).
3	***Уровень доступа на объект***	• без доступа на контролируемую территорию органа специальной связи; • с контролируемой территории без доступа в здания и сооружения; • внутри помещений, но без доступа к техническим средствам системы; • с рабочих мест операторов; • с доступом в зону управления средствами обеспечения безопасности.
4.	***Уровень доступа к шифратору по времени***	• в процессе функционирования системы специальной связи (во время работы ее компонентов); • в период неактивности компонентов системы (нерабочее время, регламентное обслуживание, "кофебрейк" атаки).

Говоря о модели криптографической системы на уровне формального описания криптографических процедур, следует отметить, что точность отображения ею объективной реальности имеет особое значение в нескольких случаях:

– первое применение нового криптоалгоритма;

– нестандартное использование ранее хорошо исследованного алгоритма;

– применение для защиты информации комбинации криптоалгоритмов разных типов.

Последний вариант может иметь место, например, в случае использования для зашифрования сообщений доказуемо стойкого симметричного алгоритма, а для формирования сеансовых ключей к нему некоторого криптографического протокола, базирующегося на асиметричном алгоритме.

В настоящее время на практике повсеместно для защиты конфиденциальной информации используется симметричный алгоритм шифрования блочного типа ГОСТ 28147-89 в режиме гаммирования с обратной связью.

Алгоритм построен на схеме Фейстеля, чем повторяет известный американский стандарт шифрования DES. Главными отличиями от "прототипа" являются наличие долговременного ключа – мощных блоков замены (512 бит), большая длина сеансового ключа (256 бит у ГОСТа против 56 бит у DES), увеличенное вдвое число циклов шифрования (32 против 16).

Следует отметить, что реально значимых аналитических атак на DES практически не было получено, несмотря на математически элегантные решения (например, атака по методу "разделяй и побеждай" [4]), что является следствием эффективного применения в этом алгоритме методов рассеивания и перемешивания каждого бита ключа с каждым битом шифруемого блока.

Несмотря на определенные вопросы к алгоритму ГОСТ в части требований по генерации долговременного ключа, проведенные исследования последних лет свидетельствуют о его высоких криптографических качествах. Наиболее сильные атаки, основанные на методе "связанных ключей", методе "бумеранга" со "связанными ключами" [5, 6], имеют по меткому выражению исследователей нулевую значимость.

Теоретически остаются возможности разработки атак на основе методов "скрытого канала" [7], однако это уже по сути дела атаки не на криптосистему, а на ее реализацию.

Поскольку вопрос генерации качественных блоков замены для ГОСТ 28147-89 можно считать "закрытым" (согласно нормативным документам их генерацию и поставку осуществляет Госспецсвязь Украины), то на повестке дня очевидное решение о допуске алгоритма в определенных реализациях к защите информации с грифом ограничения на одну ступень выше (в соответствии с самим стандартом). Отметим, что в "подстрочнике" научных публикаций [8] можно "увидеть" основные требования к блокам замены ГОСТа:

1. Нелинейность бент-функций, описывающих блоки;

2. Выравнивание соотношения количества нулей и единиц в замененном блоке.

Целесообразность создания в настоящее время альтернативного стандарта шифрования имеет весьма спорный характер, так как не учитывает фактора высокой стоимости наработки методологической базы проведения экспертиз соответствующих средств криптозащиты.

Тема создания модели генерации и управления ключами в каждом конкретном случае решается отдельно, так как в соответствии с законом генерация ключей является прерогативой Госспецсвязи Украины [9].

Модели атак на симметричные криптографические системы в открытой литературе освещены достаточно глубоко [8, 10] и с учетом ежегодных публикаций материалов соответствующих международных конференций могут оперативно корректироваться.

Суть неформальной модели поведения системы "шифратор-оператор" в различных условиях эксплуатации фактически определяется правилами ее эксплуатации с учетом конкретных реалий применения шифротехники.

При создании модели шифратора как микроэлектронного устройства, подверженного случайным сбоям и отказам, следует исходить из того факта, что отказы могут быть двух типов [11]: отказы (сбои), не приводящие к снижению безопасности устройства в смысле возникновения каналов утечки информации, и опасные отказы, вследствие которых может снижаться уровень безопасности шифратора.

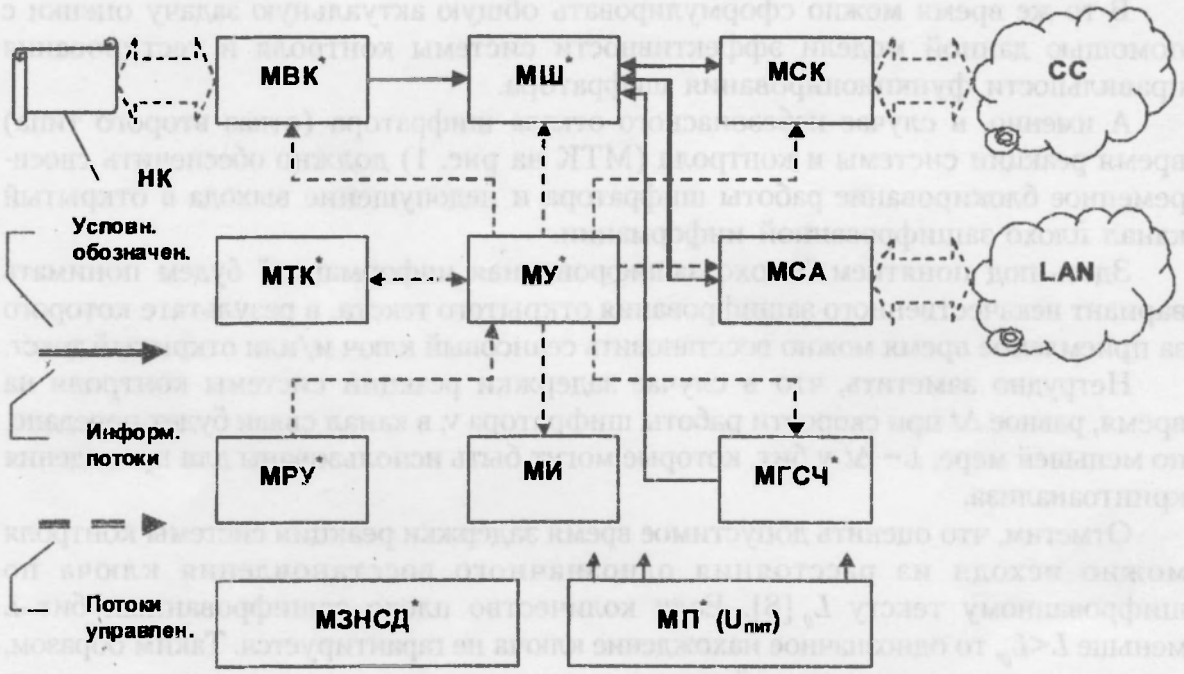

Рис. 1 Типовая функциональная схема шифратора

На рис. 1 представлена типовая схема шифратора поточного типа, на которой модули, отмеченные символом *, являются потенциальными источниками отказов второго типа, в том числе:

- МВК – модуль ввода ключа с помощью некоторого носителя (НК);
- МГСЧ – модуль генератора случайных чисел;
- МЗНСД – модуль защиты от несанкционированного доступа;
- МП – модуль питания;
- МРУ – модуль ручного управления (пульт оператора);
- МУ – модуль управления и синхронизации;
- МТК – модуль тестирования и контроля;
- МШ – модуль шифрования, который в свою очередь может состоять из нескольких узлов.

Сервисные и интерфейсные модули, как правило, не являются источниками отказов второго типа:

– МИ – модуль индикации (состояний шифратора);

– МСА – модуль сопряжения абонентской части (возможно, с локальной вычислительной сетью);

– МСК – модуль сопряжения с канальной частью (выхода на систему связи).

Степень детализации данной модели существенно зависит от использованых для построения шифратора алгоритмических и схемотехнических решений, а также элементной базы. Анализ данной модели проводится, как правило, по принципу "снизу вверх" или иначе "от частного к общему".

Во многих случаях принципы построения модулей являются конфиденциальной информацией предприятий-разработчиков, что не позволяет сделать обзор используемых решений и предложить публичную методику формирования модели данного типа.

В то же время можно сформулировать общую актуальную задачу оценки с помощью данной модели эффективности системы контроля и тестирования правильности функционирования шифратора.

А именно, в случае небезопасного отказа шифратора (отказ второго типа) время реакции системы и контроля (МТК на рис. 1) должно обеспечить своевременное блокирование работы шифратора и недопущение выхода в открытый канал плохо зашифрованной информации.

Здесь под понятием "плохо зашифрованная информация" будем понимать вариант некачественного зашифрования открытого текста, в результате которого за приемлемое время можно восстановить сеансовый ключ и/или открытый текст.

Нетрудно заметить, что в случае задержки реакции системы контроля на время, равное Δt при скорости работы шифратора v, в канал связи будет передано, по меньшей мере, $L = \Delta t \cdot v$ бит, которые могут быть использованы для проведения криптоанализа.

Отметим, что оценить допустимое время задержки реакции системы контроля можно исходя из расстояния однозначного восстановления ключа по шифрованному тексту L_0 [8]. Если количество плохо зашифрованных бит L меньше $L<L_0$, то однозначное нахождение ключа не гарантируется. Таким образом, в ходе исследования указанной модели нужно показать, что, как минимум, время задержки системы контроля $Дt$ удовлетворяет неравенству:

$$\Delta t < L_0 / v$$

Модель – программный имитатор позволяет с помощью компьютера проводить широкий комплекс испытаний шифратора от статистических исследований по входу и выходу до проведения экспериментов с имитацией различных отказов. Главной проблемой создания имитатора является обеспечение точного соответствия модели спецификациям и алгоритмам, заданным конструкторской документацией на шифратор.

Один из простейших методов ее решения – независимая разработка двух имитаторов разными программистами на разных языках с последующим сравнением по выходу.

Специфическая модель шифратора как основного технического средства, используемого для обработки информации с ограниченным доступом, строится

исходя из задач, которые нужно решить в рамках проведения специальных исследований.

И, наконец, модель взаимодействия в системе специальной связи позволяет изучить использованные криптопротоколы, надежность и безопасность системы управления и генерации ключей в различных ситуациях.

В настоящее время рядом отечественных компаний-разработчиков и производителей независимо созданы современные шифраторы, позволяющие надежно защищать конфиденциальную информацию (Табл. 2). Ряд изделий уже прошли экспертизу и получили необходимые документы от Госспецсвязи Украины, некоторые находятся в процессе экспертизы.

Таблица 2

Шифраторы потокового типа для защиты конфиденциальной информации

№№ п.п.	Условное наименование	Тип	Характеристика	Заявленная скорость	Фирма
1.	"CryptoIP-448"	АШ,КШ, ЭЦП	TCP/IP, IEEE 802.3, НК – смарт-карта	6 Мб/	А
2.	"CryptoIP-248"	АШ,КШ, ЭЦП	TCP/IP, IEEE 802.3, НК – смарт-карта	1 Мб/	А
3.	"Оникс-100"	КШ	TCP/IP, IEEE 802.3, НК - МКД	75 Мб/	К
4	Д-300	КШ	E1, ITU-T G.703, G.704, G.706, НК - МКД	2048 Кб/с	К
5.	"Пелена" В371-Е	КШ	TCP/IP, Ethernet.IEEE 802.3-2002 100Base-TX/FX, НК – ISO 7816	70 Мб/с	Г
6.	В271-Е	АШ	TCP/IP, 4 Ethernet 100Base-TX, НК – ISO 7816	30 Мб/с	Т

Сокращения, абревиатуры:
АШ – абонентское шифрование, КШ – канальное шифрование, ЭЦП – формирование электронной цифровой подписи, TCP/IP – стек протоколов, E1 – основной поток 2048 кб/сек, "А" – ООО "Автор", "К" – ООО "НВФ "Криптон", "Т" – ООО "Трител"

При проведении экспертизы представленных в таблице 2, типов поточных шифраторов были в той или иной степени использованы предложенные выше модели в виде программных продуктов, таблиц, описаний, схем.

Дальнейшее исследование моделей целесообразно продолжить в плане формализации их описаний и разработки методов их автоматизированного применения.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Мельников В.П.* Информационная безопасность и защита информации: учебное пособие для студентов высших учебных заведений / В.П. Мельников, С.А. Клейменов, В.М. Петраков ; под. ред. С.А. Клейменова. – М. : Изд. центр "Академия", 2009. – 336 с.

2. Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису: Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141.

3. *Гатчин Ю.А.* Основы информационной безопасности компьютерных систем и защиты государственной тайны : учебное пособие / Ю.А. Гатчин, Е.В. Климова, А.А. Ожиганов. – СПб. : СПбГУ ИТМО, 2001. – 60 с.

4. *Бабенко Л.К.* Алгоритмы "распределенных согласований" для оценки вычислительной стойкости криптоалгоритмов / Л.К. Бабенко, А.М. Курилкина. – М., ЛКИ, 2008, – 112 с.

5. *Пудовкина М.* Атаки на основе метода связанных ключей : Доклад на конференции "РусКрипто", апрель, 2010 год [Электронный ресурс]. – Режим доступа : http ://www.ruscrypto.ru/sources/conference/rc2010/.

6. *Vladimir Rudskoy* On zero practical significance of "Key recovery attack on full GOST block cipher with zero time and memory" [Электронный ресурс]. – Режим доступа : Cryptology ePrint Archive, Report 2010/111, http ://eprint.iacr.org/2010/111.pdf.

7. *Жуков А.Е.* Исторический обзор технологий атак по побочным каналам : Доклад на конференции "РусКрипто", апрель 2010 год, материалы [Электронный ресурс]. – Режим доступа : http://www.ruscrypto.ru/sources/conference/rc2010/.

8. *Бабаш А.В.* Криптография / А.В. Бабаш, Г.П. Шанкин ; под редакцией В.П. Шерстюка. М. СОЛОН-Р, 2002. – 512 с.

9. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України [Электронный ресурс].– Режим доступа : http ://zakon.rada.gov.ua/.

10. *Грушо А.А.* Анализ и синтез криптоалгоритмов, курс лекций / А.А. Грушо, Э.А. Применко, Е.Е. Тимонина. – М., – 2000. – 109 с.

11. *Беляев Ю.К.* Производительность при наличии двух типов отказов / Ю.К. Беляев ; в сб. : "Кибернетику – на службу коммунизму". – Т. 2. – М.– Л. "Энергия", 1964. – С. 303–309.

Отримано 15.04.2011