УДК 004.056.55

С.М. Авдошин [1], А.А. Савельева[2]

Криптографические методы защиты информационных систем

(*Представлено членом – корреспондентом АИН С.Н. Митяковым*)

Рассматриваются методики оценки уровня ИТ-безопасности организации. Описываются требования к надежному криптографическому программному обеспечению. Приводится обзор самых распространенных алгоритмов шифрования и тенденции развития современной криптографии. В заключение предлагаются рекомендации по обеспечению надежного функционирования механизмов системы защиты информации.

In this article, we discuss some techniques for organization IT-security evaluation together with a set of requirements to robust encryption software. An overview of popular crypto algorithms is provided; current cryptography development trends are considered as well. In conclusion, we give some recommendation for ensuring reliable performance of information security system.

Введение

Проблема защиты информационных ресурсов в настоящее время приобретает все более важное значение. Так, по данным отчета CSI/FBI Computer Crime and Security Survey 2005 [1], средний ущерб каждой компании, в которой в минувшем году была зафиксирована утечка конфиденциальных данных, составил 355,5$ тыс. (причем по сравнению с 2004 годом эта цифра возросла почти вдвое). По некоторым оценкам, экономические потери от злонамеренных атак на банковские системы по всему миру составляют ежегодно около 130 млрд. долларов.

Отметим некоторые факторы, которые определяют трудоемкость решения задач защиты информации [2]:

- увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютерной техники;
- сосредоточение в единых базах данных информации различного назначения и принадлежности;
- расширение круга пользователей, имеющих доступ к ресурсам компьютерной системы и находящимся в ней массивам данных;
- усложнение режимов функционирования технических средств компьютерной системы;
- увеличение количества технических средств и связей в автоматизированных системах;
- повсеместное распространение сетевых технологий, объединение локальных систем в глобальные.

Можно выделить следующие методы защиты информации от умышленных деструктивных воздействий:

- методы обеспечения физической безопасности компонентов системы;
- ограничение доступа;
- разграничение доступа;

[1] Государственный Университет – Высшая Школа Экономики, Москва, Россия.
[2] МАТИ - Российский государственный технологический университет им. К.Э. Циолковского, Москва, Россия

- разделение доступа (привилегий) – разрешение доступа только при одновременном предъявлении полномочий всех членов группы;
- криптографическое преобразование информации и реализованные на его основе криптографические протоколы.

Аудит информационной безопасности

Необходимость использования криптографических систем на предприятиях и в финансовых институтах возрастает с каждым днем. Как следствие, исключительную практичность приобретает вопрос о методах и критериях оценки безопасности информационных систем. Система оценок должна носить интегральный характер, так как руководство организации по сути дела интересует не столько конкретный уровень безопасности в частных технологических вопросах, сколько общий уровень качества функционирования самой организации, обеспечиваемый, в том числе, и уровнем безопасности информационных систем. С практической точки зрения этот вопрос — самый тяжелый. Имеющиеся подходы к проблеме создания инструментов и методик оценки интегрального уровня ИТ-безопасности организации весьма противоречивы [3]:

- **Использование стандартов и норм аудита финансовых организаций, включая аудит их информационных систем и аудит безопасности этих систем.** Важнейшей особенностью используемых в этой сфере подходов является комплексность оценки всех сторон деятельности организации, каким-либо образом влияющих на риски безопасности. В силу ясного осознания сложности описания аудируемого объекта, в методиках этой категории применяется механизм качественного описания результатов проверки и мягкая рейтинговая система их оценки. Наиболее распространенный рейтинговый стандарт проверки информационных технологий — американский URSIT (Uniform Rating System for Information Technology) [4]. Представляется, что этот подход наиболее объективен, однако он принят только в финансовом секторе и не находит применения вне него.
- **Проведение аудита ИТ-инфраструктуры организации по стандарту безопасности компьютерных систем ISO 17799 [5].** Пока известно лишь о первых, весьма ограниченных попытках применения этого метода, поэтому о практическом опыте говорить рано. Между тем разработчики стандарта заявляют, что после проведения подобного аудита информационная система организации становится «прозрачнее» для менеджмента, выявляются основные угрозы безопасности для бизнес-процессов, вырабатываются рекомендации по повышению текущего уровня защищенности для защиты от обнаруженных угроз и недостатков в системе безопасности и управления. К сожалению, комплексный характер данного стандарта и более широкая и приближенная к жизни модель угроз не соответствует рамкам полномочий ведомств, осуществляющих государственное регулирование в этой сфере в России.
- **Применение для оценки защищенности информационных систем стандартов ISO 15408 «Открытые критерии» [6].** В этих стандартах детально проработаны вопросы разработки информационных систем с учетом требований и гарантий их безопасности. Вместе с тем авторами стандарта сделаны серьезные ограничения, которые фактически не позволяют использовать его в качестве универсального инструмента комплексной оценки безопасности и жестко ограничивают область его применения только вопросами безопасности информационных систем. Стандарт не затрагивает административных и правовых вопросов обеспечения безопасности и далеко не полностью учитывает роль легального пользователя во всей совокупности проблем обеспечения безопасности.
- **Использование для оценки защищенности информационных систем частных методик и критериев, предназначенных для оценки криптографической**

стойкости алгоритмов шифрования и защищенности информации от утечки по техническим каналам. При этом происходит фактическая подмена модели угроз, в центре которой стоят проблемы борьбы с легальным пользователем системы, моделью соответствующих ведомств, в центре которых стоят субъекты несанкционированного доступа.

Как известно [7], далеко не все присутствующие на рынке криптографические средства обеспечивают обещанный уровень защиты. Это связано с нарушением нижеперечисленных требований, предъявляемых к криптографическому программному обеспечению [8]:

- использование проверенных алгоритмов, выдержавших попытки взлома в течение достаточного времени;
- длина ключей, достаточная, чтобы исключить снижение безопасности в результате увеличения вычислительных ресурсов потенциальных оппонентов (удваивающихся каждый год, согласно закону Мура) в течение длительного периода времени;
- локальная генерация и локальный менеджмент ключей, исключающие их попадание в чужие руки;
- гибкая схема удостоверения действительности ключей, допускающая как распределенное управление доверием ("сеть доверия"), так и централизованную архитектуру сертификации;
- открытость и доступность для проверки и критики не только алгоритмических решений и форматов файлов, но и исходного текста самой программы.

Классификация криптографических алгоритмов

В настоящее время общепризнанным является подразделение криптографических алгоритмов на следующие основные категории:

- алгоритмы шифрования с секретным ключом (симметричные)
  - блочные шифры
  - поточные шифры
- алгоритмы шифрования с открытым ключом (асимметричные)

Системы блочного шифрования

Идея, лежащая в основе большинства итерационных блочных шифров, состоит в построении криптографически стойкой системы путем последовательного применения относительно простых криптографических преобразований. Принцип многоразового шифрования с помощью простых криптографических преобразований был впервые предложен Шенноном в работе [9]: он использовал с этой целью преобразования перестановки и подстановки. Первое из этих преобразований переставляет отдельные символы преобразуемого информационного блока, а второе – заменяет каждый символ (или группу символов) из преобразуемого информационного блока другим символом из того же алфавита (соответственно группой символов того же размера и из того же алфавита). Узлы, реализующие эти преобразования, называются, соответственно, ***P-блоками*** (*P-box, permutation box*) и ***S-блоками*** (*S-box, substitution box*).

DES, Triple DES и AES. В 1973-74 гг. Национальное Бюро Стандартов США (NBS) опубликовало документы, содержащие требования к криптографическому алгоритму, который мог бы быть принят в качестве стандарта шифрования данных в государственных и частных учреждениях. В 1976 г. в качестве такового стандарта был утвержден алгоритм, разработанный фирмой IBM. В 1977 г. этот стандарт был официально опубликован и вступил в силу как федеральный стандарт шифрования данных – Data Encryption Standard или сокращенно DES [10].

В самом схематичном виде DES представляет собой 16-цикловой итерационный блочный шифр. DES работает с блоками данных разрядностью 64 бита с ипользованием 56-разрябного ключа. Применяемые преобразования – поразрядное сложение по модулю два, подстановки и перестановки. Алгоритм выработки 48-битовых цикловых ключей из 56-битового ключа системы и ряд преобразований служат для обеспечения необходимого перемешивания и рассеивания перерабатываемой информации, однако при анализе DES чаще всего играют не самую существенную роль.

В 1999 г. на конференции, организованной RSA, компания Electronic Frontier Foundation взломала ключ DES менее чем за 24 часа. Одной из замен DES, получившей широкое распространение, стал алгоритм Triple DES. В этом случае алгоритм DES выполняется трижды, при этом используются 3 ключа, каждый из которых состоит из 56 битов (что, по сути, соответствует использованию 168-битного ключа). Тем не менее, криптоаналитики обнаружили способ, позволяющий сделать атаку прямого перебора эквивалентной атаке на 108-битовый ключ. Второй проблемой является значительное снижение скорости зашифрования и расшифрования данных.

В ответ на проблемы с длиной ключа и производительностью, проявившиеся в Triple DES, многие криптографы и компании разработали новые блочные шифры. Наиболее популярными предложениями стали алгоритмы RC2 и RC5 корпорации RSA Data Security, IDEA компании Ascom, Cast компании Entrust, Safer компании Cylink и Blowfish компании Counterpane Systems. Коммерческие альтернативы DES получили определенное распространение, но ни одна из них не стала стандартом.

В 2001 г. на смену DES и Triple DES пришел стандарт AES (Advanced Encryption Standard), действующий и по сей день. Шифр AES основан на алгоритме Rijndael [11], разработанном бельгийцами Д. Дейменом и В. Райменом. Он быстрый, простой, защищенный, универсальный и хорошо подходит для реализации на смарт-картах. Rijndael – это итерационный блочный шифр, имеющий архитектуру «Квадрат». Шифр имеет переменную длин у блоков и различные длины ключей. Длина ключа и длина блока могут быть равны независимо друг от друга 128, 192 или 256 битам. В стандарте AES определена длина блока, равная 128 битам.

ГОСТ 28147-89 [12]. Отечественный стандарт шифрования носит официальное название «Алгоритм криптографического преобразования ГОСТ 28147-89». Как явствует из его номера, стандарт был принят в СССР в 1989 г. Если охарактеризовать алгоритм ГОСТ в самом общем виде, то он является блочным шифром, построенным по схеме Фейстеля с 32 циклами шифрования. Длина информационного блока – 64 бита, длина ключа – 256 бит.

Основные отличия алгоритма ГОСТ от алгоритма DES – в строении функции, которая осуществляет отображение $\mathbf{Z}_2^{32} \times \mathbf{Z}_2^{48} \to \mathbf{Z}_2^{32}$, и алгоритме выработки цикловых ключей. И в том и в другом случае преобразования, используемые в алгоритме ГОСТ, проще для программной реализации. Исследования [13] показывают, что российский стандарт не уступает по стойкости американскому AES.

Системы поточного шифрования

Основная идея поточного шифрования состоит в том, что каждый из последовательных знаков открытого текста подвергается своему преобразованию. В идеале разные знаки открытого текста подвергаются разным преобразованиям, т.о. преобразование, которому подвергаются знаки открытого текста, должно изменяться с каждым следующим моментом времени. Реализуется эта идея следующим образом. Некоторым образом получается последовательность знаков $k_1, k_2, \ldots$, называемая ключевым потоком (keystream) или бегущим ключом (running key, RK). Затем каждый знак x_i открытого текста

подвергается обратимому преобразованию, зависящему от k_i – соответствующего знака ключевого потока.

Хотя подавляющее большинство существующих шифров с секретным ключом с определенностью могут быть отнесены или к поточным или к блочным шифрам, теоретически граница между этими классами остается довольно размытой. Так, например, допускается использование алгоритмов блочного шифрования в режиме поточного шифрования (например, режимы CBF и OFB для алгоритма DES или режим гаммирования для алгоритма ГОСТ 28147-89).

Поточные шифры почти всегда работают быстрее и обычно требуют для своей реализации гораздо меньше программного кода, чем блочные шифры. Наиболее известный поточный шифр был разработан Р. Ривестом; это шифр RC4, который характеризуется переменным размером ключа и байт-ориентированными операциями. На один байт требуется от 8 до 16 действий, программная реализация шифра выполняется очень быстро. Независимые аналитики исследовали шифр, и он считается защищенным. RC4 используется для шифрования файлов в таких изделиях, как RSA SecurPC. Он также применяется для защиты коммуникаций, например, для шифрования потока данных в Интернет-соединениях, использующих протокол SSL.

В одноключевых системах существуют две принципиальные проблемы:

- **Распределение секретных ключей по информационному каналу;**
- **Аутентификация секретного ключа** (процедура, позволяющая получателю удостовериться, что секретный ключ принадлежит законному отправителю)**.**

Наиболее известный и широко распространенный протокол открытого распределения ключей [14] был разработан У. Диффи и М. Хеллманом в 1976 г. Протокол позволяет двум пользователям обмениваться частным ключом по уязвимым каналам, не имея никаких предварительных договоренностей. Безопасность протокола Диффи-Хеллмана основана на трудности вычисления дискретного логарифма в конечном поле. Существует ряд модификаций этого алгоритма, предусматривающих аутентификацию участников.

Криптосистемы с открытым ключом

В асимметричной криптографии для зашифрования и расшифрования используются различные функции. Асимметричные алгоритмы основаны на ряде математических проблем, на которых и базируется их стойкость. Пока не найден полиномиальный алгоритм решения этих проблем, данные алгоритмы будут стойки. В этом заключается ещё одно отличие симметричного и асимметричного шифрования: стойкость первого является непосредственной и научно доказуемой, стойкость второго – предположительной.

Наиболее известные криптосистемы с открытым ключом:

- Рюкзачная криптосистема (Knapsack Cryptosystem);
- Криптосистема RSA;
- Криптосистема Эль-Гамаля – EGCS (El Gamal Cryptosystem);
- Криптосистема, основанная на свойствах эллиптических кривых – ECCS (Elliptic Curve Cryptosystems).

Применение алгоритмов шифрования с открытым ключом позволяет:

- избавиться от необходимости секретных каналов связи для предварительного обмена ключами;
- свести проблему взлома шифра к решению трудной математической задачи, т.е. в конечном счете, принципиально по-другому подойти к обоснованию стойкости криптосистемы;

- решать средствами криптографии задачи, отличные от шифрования, например, задачу обеспечения юридической значимости электронных документов.

Последний пункт означает, что подтверждение авторства сообщений может осуществляться при помощи криптографических средств, что абсолютно необходимо для дистанционного управления ресурсами. Лицо, управляющее чьими-либо ресурсами по распоряжениям владельца, должно обладать возможностью доказать, что выполненное им распоряжение было получено именно от владельца. Данная задача стала особенно актуальной с появлением электронной коммерции, в качестве ресурса здесь выступают деньги на банковском счету владельца.

Любая схема ЭЦП обязана определить три следующих алгоритма:

- алгоритм генерации ключевой пары для подписи и ее проверки;
- алгоритм подписи;
- алгоритм проверки подписи.

Для ее решения были предложены различные схемы электронно-цифровой подписи (ЭЦП). Первая схема ЭЦП — RSA — была разработана еще в конце 1970-х годов.

RSA [15]. RSA – криптографическая система с открытым ключом, обеспечивающая оба механизма защиты: шифрование и цифровую подпись. Криптосистема RSA была разработана в 1977 году и названа в честь авторов: Рональда Ривеста, Ади Шамира и Леонарда Адельмана. В PGP алгоритм RSA также используется для шифрования и генерации ЭЦП.

Принцип её действия в следующем. Берутся два больших случайных простых числа p и q приблизительно равной разрядности и вычисляется их произведение $n = p \cdot q$. Затем выбирается число e, взаимно простое с произведением $(p-1)\cdot(q-1)$ и вычисляется число $d = e^{-1}\left(\mathrm{mod}(p-1)\cdot(q-1)\right)$, взаимно простое с n.

Числа e и n становятся открытым ключом, число d – закрытым. Чтобы создать шифротекст c, отправитель возводит сообщение m в степень e по модулю n, где e и n – показатели открытого ключа получателя: $c = m^e (\mathrm{mod}\, n)$.

Чтобы расшифровать полученный шифротекст c, получатель вычисляет c в степени d по модулю n: $m = c^d (\mathrm{mod}\, n)$.

Если абонент А хочет подтвердить свое авторство сообщения, он сначала шифрует его на своем секретном ключе, а потом на открытом ключе абонента Б. Соответственно, абонент Б применяет к полученному сообщению свой секретный ключ и открытый ключ абонента А; успешное расшифрование является гарантией того, что отправить сообщение мог только абонент А.

Схема Эль-Гамаля [16]. Схема Эль-Гамаля основана на трудности вычисления дискретных логарифмов в конечном поле в сравнении с лёгкостью возведения в степень в том же самом поле.

Для генерации пары ключей сначала выбирается простое число p и два случайных числа, g и x; оба эти числа должны быть меньше p. Затем вычисляется $y = g^x (\mathrm{mod}\, p)$.

Открытым ключом становятся y, g и p. И g, и p можно сделать общими для группы пользователей. Закрытым ключом является x. Теперь, чтобы зашифровать сообщение m, сначала выбирается случайное k, взаимно простое с $p-1$. Затем вычисляются $a = g^k (\mathrm{mod}\, p)$, $b = y^k \cdot m (\mathrm{mod}\, p)$. Пара a и b является шифротекстом, что увеличивает исходное сообщение в два раза. Для расшифрования вычисляется $m = b / a^x (\mathrm{mod}\, p)$.

Стандарты ЭЦП в России и США, принятые в 1994 году [17, 18] и действовавшие до 2001 г., базировались на схеме Эль-Гамаля.

Криптосистемы на основе эллиптической кривой. Последние достижения теории вычислительной сложности показали, что общая проблема логарифмирования в конечных полях, не может считаться достаточно прочным фундаментом. Наиболее эффективные на сегодняшний день алгоритмы дискретного логарифмирования имеют уже не экспоненциальную, а субэкспоненциальную временную сложность. Это алгоритмы "index-calculus", использующие факторную базу, к числу которых относятся алгоритм Адлемана [19], несколько версий «COS» (алгоритма Копперсмита-Одлыжко-Шреппеля) [20] и решето числового поля [21]. Ведутся работы по повышению эффективности этих алгоритмов. Так, метод, описанный в [22], направлен на повышение эффективности решения линейных уравнений в кольцах вычетов, поскольку все субэкспоненциальные методы дискретного логарифмирования сводятся к этой задаче.

Ряд успешных атак, например, описанные в [23], на системы, основанные на сложности дискретного логарифмирования в конечных полях, привел к тому, что стандарты ЭЦП России и США в 2001 году были обновлены: переведены на эллиптические кривые [24, 25]. Схемы ЭЦП при этом остались прежними, но в качестве чисел, которыми они оперируют, теперь используются не элементы конечного поля $GF(2^n)$ или $GF(p)$, а эллиптические числа — решения уравнения эллиптических кривых над указанными конечными полями. Роль операции возведения числа в степень в конечном поле в обновленных стандартах выполняет операция взятия кратной точки эллиптической кривой — «умножение» точки на целое число.

Надлежащий выбор типа эллиптической кривой позволяет многократно усложнить задачу взлома схемы ЭЦП и уменьшить рабочий размер блоков данных. Старый российский стандарт ЭЦП оперирует 1024-битовыми блоками, а новый, основанный на эллиптических кривых, — 256-битовыми, и при этом обладает большей стойкостью.

Криптосистемы на основе эллиптической кривой получают все большее распространение скорее как альтернатива, а не замена системам на основе RSA. Они имеют некоторые преимущества, особенно при использовании в устройствах с маломощными процессорами и/или маленькой памятью. Типичные области применения:

- m-commerce - мобильная торговля (WAP, сотовые телефоны, карманные компьютеры);
- смарт-карты (например, EMV);
- e-commerce - электронная торговля и банковские операции (например, SET);
- Интернет-приложения (например, в протоколе SSL).

Существуют, однако, и некоторые проблемы, которые ограничивают широкое распространение систем на основе эллиптических кривых:

- реальная безопасность таких систем все еще недостаточно осознана;
- трудность генерации подходящих кривых;
- несовместимость;
- лицензирование и патентование;
- относительно медленная проверка цифровой подписи.

Заключение

Автоматизация (без которой невозможно развитие организаций) приводит к росту угроз несанкционированного доступа к информации, как следствие, к необходимости постоянной поддержки и развития системы защиты. Защита информации является не разовым мероприятием и даже не совокупностью мероприятий, а непрерывным процессом,

который должен протекать во времени на всех этапах жизненного цикла автоматизированной системы обработки информации. Повышение производительности вычислительной техники и появление новых видов атак на шифры ведет к понижению стойкости известных криптографических алгоритмов. Таким образом, используемые криптографические средства должны постоянно обновляться. Поддержание и обеспечение надежного функционирования механизмов системы защиты информации сопряжено с решением специфических задач и поэтому может осуществляться лишь специалистами – высококвалифицированными криптографами и криптоаналитиками, которые могут гарантировать надежность используемых алгоритмов и программных средств, реализующих функции защиты информации.

Библиографический список

1. **Gordon L.A., Loeb M.P., Lucyshyn W., Richardson R.** CSI/FBI Computer Crime and Security Survey 2005. Computer Security Institute Publications, 2005 – 26 p.
2. **Иванов М.А.** Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001 – 368 с.
3. **Курило А.** Информационная безопасность в организации: взгляд практика. // Открытые системы, #07-08/2002.
4. Uniform Rating System for Information Technology. Federal financial institutions examination council.1999 – 11 p.
5. International Organization for Standardization. Code of Practice for Information Security Management / ISO 17799.
6. International Organization for Standartization. The Common Criteria for Information Technology Security Evaluation / ISO 15408.
7. **Schneier B.** Snake Oil, Crypto-Gram *<http://www.counterpane.com/Crypto-Gram.html>*, February, 1999.
8. **Отставнов М.** Краткий путеводитель по миру PGP // "Компьютерра" №48, 1997.
9. **Шеннон К.Э.** Работы по теории информации и кибернетике. М.: И.Л., 1963, с. 333-402.
10. ANSI X3.92, “American National Standard for Data Encryption Algorithm (DEA),” American National Standards Institute, 1981.
11. RIJNDAEL description. Submission to NIST by Joan Daemen, Vincent Rijmen. http://csrc.nist.gov/encryption/aes/round1/docs.htm.
12. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
13. **Винокуров А., Применко Э.** Сравнение российского стандарта шифрования, алгоритма ГОСТ 28147-89, и алгоритма Rijndael, выбранного в качестве нового стандарта шифрования США.// «Системы безопасности», М.: Гротэк, 2001, №№1, 2.
14. **Diffie W., Hellman M.E.** New Directions in Cryptography // IEEE Transactions on Information Theory, v. IT-22, n. 6, Nov 1976, pp. 644 – 654.
15. **Rivest R.L., Shamir A., Adleman L.M.** A Method for Obtaining Digital Signatures and Public Key Cryptosystems// Communications of the ACM, v. 21, n. 2, Feb 1978, pp. 120-126.
16. **ElGamal T.** A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Transactions on Information Theory, v. IT-31, n. 4, 1985, pp. 469-472.
17. ГОСТ Р34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронно-цифровой подписи на базе асимметричного криптографического алгоритма.
18. FIPS PUB 186. Digital Signature Standard (DSS).

19. **Adleman L.** A Subexponential Algorithm for the Discrete Logarithm with Application to Cryptography, Proc. IEEE 20-th Annual Symposium on Foundations of Computer Science (FOCS), 1979.
20. **Coppersmith D., Odlyzko A., Schroeppel R.** Discrete logarithms in GF(p) // Algorithmica. 1986. V. 1. pp. 1—15.
21. **Schirokauer O.** Discrete logarithms and local units. Phil. Trans. R. Soc. Lond. A. 1993. V. 345. pp. 409—423.
22. **Авдошин С.М., Савельева А.А.** Алгоритм решения систем линейных уравнений в кольцах вычетов // Информационные технологии. 2006. № 2. с.50-54.
23. **Odlyzko A.M.** Discrete logarithms: The past and the future. AT&T Labs–Research, 1999.–25 p.
24. ГОСТ Р34.10-01. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
25. FIPS PUB 186-2. Digital Signature Standard (DSS).