Численный метод для защиты от несанкционированного доступа

А.Е. Дубовик, Е.А. Дубовик (ИНЭУМ)

Рассмотрен численный метод, позволяющий создавать нетривиальные динамически изменяющиеся матрицы чисел, которые могут использоваться для генерации разнообразных ключей защиты от несанкционированного доступа к любым информационным системам, АСУТП, БД и т.д.

Прежде чем рассмотреть использование нового численного метода для защиты от несанкционированного доступа к информации, а также для защиты данных, передаваемых в сетях различных АСУТП, кратко оценим существующие методы защиты. Это тем более актуально, так как считается, что цена вопроса защиты информации составляет порядка 10% от общих затрат на построение и эксплуатацию информационных систем. При выборе средств защиты (как, впрочем, и других решений в области информационных технологий) пользователь, в первую очередь, сталкивается с каскадом маркетинговых заявлений поставщиков того или иного решения. Некоторые предлагают "уникальные технологии, обеспечивающие комплексную защиту информации", другие пропагандируют "бесплатный" проект для своего решения, а третьи объясняют в своем учебном центре, как правильно выбрать их систему защиты информационных ресурсов.

Рынок информационных технологий (ИТ) вследствие высочайших темпов его развития находится под мощным воздействием маркетинговых механизмов, которые способны дать искаженное представление о свойствах продукта и критериях выбора. Дело в том, что хотя маркетинг и дает искаженную картину, под ней скрываются вполне реальные свойства и характеристики решений. Если при этом еще и понимать причины, искажающие картину в ту или иную сторону, то окажется, что из маркетинговых и рекламных материалов можно извлечь гораздо больше информации, чем в них содержится и, как правило, больше, чем хотели бы сообщить авторы рекламы. Вопросы производительности также значимы при выборе методов защиты информации. При этом стоит отдавать себе отчет, что целью функционирования каждой информационной системы является обеспечение заданного качества сервисов, предоставляемого этой системой, и с осторожностью относиться к изобретаемым некоторыми производителями количественным характеристикам, которые лучше, чем у конкурентов, и отражают якобы эффективность защиты информации. Единственный надежный показатель сегодня – это реальные сравнительные испытания систем. В таких испытаниях необходимо, во-первых, полностью моделировать среду передачи данных и реальные скорости, реализуемые в сети. В каналах Ethernet 100 Мбит и FrameRelay 64 Kbit, например, эффективность решений будет определяться принципиально разными факторами, поэтому испытания в условиях простого стенда из четырех машин, объединенных локальной сетью, практически не дает никаких данных о том, как все это будет работать на самом деле в реальных производственных условиях. Во-вторых, необходимо учитывать специфику "коллективных эффектов", проявляющихся в том, что если система защиты из двух узлов показывает прекрасные результаты на испытаниях, из этого совсем не следует, что такая же система из сотни узлов вообще будет работать. Наконец, в-третьих, существенным оказывается моделирование реальной структуры информационных сервисов, а не запуск тестовых утилит, в противном случае результаты испытаний также могут оказаться неадекватными. Сегодня те или иные методы защиты обычно используются не только для защиты передачи данных, но и для информационных систем и мультимедийных сервисов, реализованных на той же инфраструктуре, что и АСУТП, IP телефония и видеоконференции. Чтобы применение методов защиты не приводило к потере качества и сервиса, решения должны обеспечивать приоритеты в передаваемой информации. Если предполагается часть информационных потоков направлять во внешнее информационное пространство (без шифрования), необходимо убедиться, что шлюз защиты достаточно эффективен. Иначе придется организовывать доступ к этим ресурсам в обход средств защиты, что само по себе создает дополнительные угрозы информационным ресурсам [1].

Для решения проблем разграничения доступа на уровне ОС и СУБД используется та или иная модель доступа к информационным ресурсам. Хотя набор таких моделей достаточно широк, но только относительно небольшое их число реализовано в конкретных продуктах либо может быть туда "встроено" без значительной модификации исходного кода. Наиболее совершенными являются системы, которые способны обеспечить получение любых выборок и статистики из архива по создаваемым запросам, создание специфических запросов на SQL и/или генерацию любых видов отчетов для анализа эффективности. Чтобы выяснить, какие средства защиты применимы для конкретной информационной системы, необходимо сформулировать требования к ним и помнить, что все средства защиты всего-навсего предоставляют собой инструментарий для реализации политики безопасности, набор управленческих решений, направленных на защиту информации, и установленных на их основе правил работы пользователей и администраторов. Поэтому основные требования при выборе того или иного средства защиты информации должны отвечать на вопросы: для чего будет применяться данное средство защиты; от каких угроз это средство будет ограждать и в какой степени; какие правила работы с информационными ресурсами могут быть реализованы.

Именно для реализации этих требований, предлагается новый численный метод защиты информации.

На сегодняшний день существуют в основном логические методы средств защиты информации. В отличие от них предложенный метод является численным и базируется на математическом аппарате. В ра-

Таблица 1

1,5 - 1	1	2,5 - 2	2	3,5 - 3		3,5 - 4	4	5,5 - 5		5,5 - 6	6	7,5 - 7		7,5 - 8	8	9,5 - 9		11,5 - 10	10	11,5 - 11		11,5 - 12	12	13,5 - 13	
2,6 - 1		2,6 - 2		2,6 - 3	3	5,6 - 4		5,6 - 5		5,6 - 6		5,6 - 7	7	9,6 - 8		9,6 - 9		9,6 - 10		13,6 - 11	11	13,6 - 12		13,6 - 13	
4 - 1		4 - 2		4 - 3		4 - 4		4 - 5	5	9 - 6				9 - 8		9 - 9	9	13 - 10		13 - 11		13 - 12		13 - 13	13

боте [2] был рассмотрен численный метод диспетчеризации вычислений с динамически изменяющимися приоритетами, где численные вычисления использовались исключительно для получения управляющих воздействий, для выбора приоритетов при регистрации (опросе) различных по спектральным характеристикам датчиков (сенсоров) управляемого объекта.

Покажем возможность применения этого метода для защиты информации от несанкционированного доступа. Для этого следует использовать нетривиальную, формализованную матрицу динамически изменяющихся чисел как результат численных вычислений. Именно различные наборы динамически изменяющихся чисел матриц можно использовать как эффективное средство защиты информации.

Рассмотрим на простом, приведенном в работе [2], численном примере получение этой динамической матрицы. Использование приведенного численного примера позволит более полно оценить уникальные возможности нового численного метода для защиты информации и его значительные перспективы практического использования. В этом случае задача формулируется следующим образом. Выберем три разных любых числа K1, K2, K3, которые зададим равными 1,5; 2,6 и 4,0. Для простоты вычислений в качестве второго числа возьмем 1. Следуя решающему правилу, приведенному в [2], к каждому моменту необходимо определить минимальное значение разности, т.е. вычесть из значений 1,5; 2,6; 4,0 по единице. Очевидно, минимум этой разности даст первое заданное число. Поэтому зафиксируем первое число динамической матрицы K1. Затем суммируем 1,5 + 1 и осуществляем динамическое смещение начала отсчета K1 в значение 2,5. Продолжаем вычисления, вычитая из 2,5; 2,6; 4 число 2. Минимум разности опять дает первое число. Фиксируем K1=1,5+2= 3,5. Продолжаем вычисления с числами 3,5; 2,6; 4,0, вычитая число 3. Минимум разности в этот раз соответствует второму числу, поэтому фиксируем K2=2,6+3=5,6. Продолжаем аналогичные вычисления, определяя минимальные значения, которые фиксируются в матрице (табл. 1).

Выделенные значения представляют собой динамическую, нетривиальную матрицу чисел, которую можно эффективно использовать, выбирая разнообразные алгоритмы расчета, для организации защиты информации. Любые наборы из полученных чисел и их сочетание в динамической матрице могут быть использованы для получения ключей доступа к информационной и/или автоматизированной системе. Например, при запросе разрешения доступа в систему выставляются три цифры – в нашем случае 1,5; 2,6 и 4,0. Система защиты, используя любое секретное число (аналогично приведенному в примере) запускает программу, которая реализует простой, но формализованный и эффективный алгоритм. В результате получается непрерывный нетривиальный набор чисел в РВ. Например, для приведенного примера, выписав отдельно численные результаты, получим новую динамическую матрицу специальных чисел любой продолжительности, динамически появляющихся по строкам и столбцам с разной интенсивностью (табл. 2).

Таблица 2

	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9
N_1	1	2	4	6	8	10	12	14	
N_2	3	7	11	15					
N_3	5	9	13						

Следует отметить, что подобных примеров можно привести много, так как рекуррентные вычислительные процедуры в масштабе РВ могут продолжаться сколь угодно долго и не зависят от набора цифр. В результате получаем большую динамически изменяющуюся нетривиальную матрицу $M_x \times N_y$. Процедура приведенных вычислений и полученные результаты показывают, что процесс выбора чисел и получения динамических матриц в масштабе РВ позволяют их использовать в любом числе для защиты от несанкционированного доступа, а также для специального кодирования при защите информации. Приведем небольшой пример. Вначале, на первом этапе доступа к системе первого пользователя можно использовать цифры из трех рядов 1,3,5. При втором доступе первого пользователя можно динамически добавлять по одной появившейся в РВ цифре – 1,3,5,2 и т. д. Второй пользователь при первом доступе к информационной системе может использовать три цифры 2, 7, 9, а при втором доступе – четыре цифры 2, 7, 9, 4. и т.д. Следует обратить внимание, что наборы динамически получаемых цифр для заданных исходных данных четко повторяются и могут быть использованы различным образом. Численный метод жестко формализован и, хотя основан на простых арифметических действиях, позволяет динамически в РВ получать нетривиальные самые различные ключи доступа, состоящие из любых наборов чисел матриц данных.

Таким образом, предложенный численный метод позволяет создавать нетривиальные динамически изменяющиеся матрицы чисел, которые могут использоваться для генерации разнообразных ключей защиты от несанкционированного доступа к любым информационным системам, АСУТП, БД и для защиты приема/передачи данных.

Список литературы

1. *Трифаленков И., Макоев О.* Критерии выбора средств защиты информации // CIO. 2002. № 5.
2. *Дубовик А.Е.* Численный метод диспетчеризации вычислений для систем промышленной автоматизации // Автоматизация в промышленности. 2004. №1.

Дубовик Александр Евгеньевич *– канд. техн. наук,* ***Дубовик Евгений Александрович*** *– канд. техн. наук, ведущий научный сотрудник Института электронных управляющих машин. Контактный телефон (095) 455-55-71.*