УДК 681.3

А.А. Емельянов

МЕТОДИКИ ОЦЕНКИ ВАРИАНТОВ ПОСТРОЕНИЯ СИСТЕМЫ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ (СКЗИ) ПРИ ПРОЕКТИРОВАНИИ АСУ КОРАБЛЕЙ

Емельянов Александр Алексеевич, *кандидат технических наук, окончил Военную академию им. Ф.Э. Дзержинского. Заместитель генерального директора ФНПЦ ОАО «НПО «Марс» по качеству, эффективности и инженерно-техническому обеспечению - начальник управления. Имеет публикации в области создания систем менеджмента качества и защиты информации. [E-mail: mars@mv.ru].*

Аннотация

Синтезирована методика технико-экономической оценки (ТЭО) вариантов построения СКЗИ при проектировании АСУ. Разработана методика количественной оценки программно-аппаратной защищенности разработки АСУ в автоматизированной среде.

Ключевые слова: система комплексной защиты информации (СКЗИ), технико-экономическая оценка (ТЭО) защищенности информации, количественная оценка защищенности информации, защита информации от несанкционированного доступа, критические информационные ресурсы, автоматизированная система проектирования (АСП), Средства защиты информации (СрЗИ).

Abstract

The article synthesizes a procedure for technical and economic evaluation of variants of integrated information security system during design of C2 systems. It also deals with a quantitative evaluation procedure developed for software and hardware security of C2 system development in computer-aided environment in case of unauthorized access.

Key words: integrated information security system, technical and economic assessment (evaluation) of information security, quantitative assessment (evaluation) of information security, information protection against unauthorized access, critical information resources, computer-aided design system, information security facilities

1 Технико-экономическая оценка вариантов построения СКЗИ при проектировании АСУ

Концепция информационной безопасности автоматизированной системы проектирования (АСП) потребовала создания комплекса моделей и методик для оценки степени влияния защищенности на конечный результат проектирования. Вполне очевидно, что количественные оценки могут быть выполнены только с использованием специальных расчетных методик, которые в совокупности определяют содержание и структуру методического обеспечения ТЭО защищенности проектирования АСУ кораблей.

Структура научно-методического аппарата в

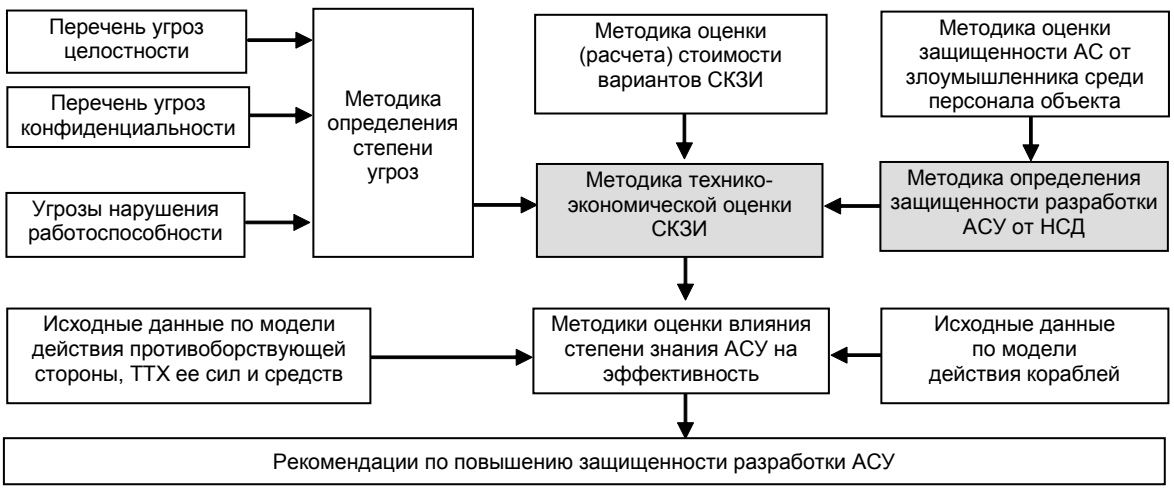


Рис. 1. Структура методического обеспечения ТЭО защищенности проектирования АСУ

этих исследованиях в обязательном порядке должна содержать как собственно методики оценки защищенности критичных информационных ресурсов (КИР) от НСД, так и методики оценки конкретной личности, способной реализовать, в частности, одну из возможных угроз безопасности проектирования. В конечном счете, в состав структуры (комплекса) должна входить методика, позволяющая оценить влияние защищенности информации на конечный результат — эффективность корабля при выполнении поставленных задач.

Чем выше степень готовности АСУ к принятию на эксплуатацию, тем достовернее информация о её основных характеристиках и тем выше должна быть степень ее защиты. Анализ содержания этапов создания АСУ показывает, что процесс проектирования в целом должен предусматривать выполнение соответствующих оценок защищенности на всех этапах (от замысла до серии), включая применение и модернизацию.

На рисунке 1 приведена упрощенная структура комплекса методик для оценки степени влияния защищенности информации на результаты научно-исследовательских и опытно-конструкторских работ в обеспечение проектирования АСУ кораблей.

Сущность упрощения заключается в том, что приведены не все частные (обеспечивающие) методики оценки степени влияния и реализации каждой из угроз, а только рассмотренные в данной работе.

Практика исследований, проводимых при проектировании изделий, показывает, что основу обеспечивающих методик могут составлять имитационные, аналитические, алгоритмические, смешанные модели, а также (полу)натурные испытания и макетирование [1].

Необходимо также отметить, что ввиду очень широкого спектра требуемых параметров, специфичности моделей и методик, в сложившейся практике взаимодействия организаций заказчика и промышленности существует определенное распределение функций при их разработке. Для достижения целей исследования целесообразно рассматривать единую обобщенную методику как некую структуру взаимосвязанных методик, обеспечивающих получение необходимых параметров.

Вполне очевидно, что реальное количество связей и блоков значительно превышает представленные на схеме. В данном случае целью иллюстрации является попытка показать и исследовать те звенья сложной системы, которые позволяют определить возможность обеспечения безопасности информации.

Принципиально новыми, ранее не использовавшимися в практике подобных исследований, являются методики, позволяющие оценивать влияние защищенности информации на конечный результат.

Требования к точности обеспечивающих методик при заданной точности на общую методику изложены в доступной научно-технической литературе. Суть этих положений сводится к тому, что имеются четыре группы ошибок, определяющих точность получаемых при моделировании результатов:

— упрощение исходного моделирующего алгоритма;

— неточность дискретной реализации;

— неточность задания исходных данных;

— ограниченность статистики.

В основе упрощения исходного алгоритма лежит аппроксимация алгоритмов элементов системы более простыми, но эквивалентными математическими конструкциями.

Если при этом реализовавшаяся точность имитации процессов будет лежать в области допустимых значений, то данную аппроксимацию следует принять в качестве рабочего моделирующего алгоритма, иначе нужно переходить к более точным описаниям. По характеру ошибки, влияющие на точность имитации, чаще всего составляют сумму случайных и методических составляющих.

При разработке моделей и расчетных методик целесообразно выбирать такие методы дискретной реализации, которые на основании априорных сведений позволяют утверждать, что ошибки моделирования, то есть ошибки, сопровождающие реализацию моделирующих алгоритмов на ЭВМ, ошибки численного интегрирования, решения дифференциальных и алгебраических уравнений не будут превышать заданных значений. При калибровке методик это априорное утверждение необходимо доказать с использованием результатов натурных испытаний. Данная группа ошибок также приводит как к случайным, так и к методическим ошибкам расчета показателей функционирования сложной системы.

Неточность задания исходных данных вызывается тем, что параметры модели методики определяются с ошибками из-за ограниченности статистики при обработке результатов натурных испытаний и неточностью априорной информации. Для учета влияния этих ошибок на точность расчета показателей эффективности системы обычно применяются методы чувствительности. Из-за большой размерности вектора параметров и возникающими в связи с этим трудностями на практике уравнение чувствительности составляют для наиболее значимых для точности параметров.

В результате моделирования при статистических испытаниях будут присутствовать случайные ошибки, обусловленные числом реализаций. Характеристики распределения этих ошибок зависят от выбранного метода планирования статистических испытаний и принятого способа обработки полученных результатов.

Эти ошибки контролируемы исследователем в том смысле, что их можно уменьшать путем увеличения числа моделирования. Вполне очевидно, что это ведет к увеличению затрат, поэтому требует разумного подхода.

Данные, приведенные в ряде публикаций [2,3], показали, что точности обеспечивающих методик должны быть на 1 - 2 порядка выше точности, с которой требуется получить численное значение целевой функции, поэтому разработка обеспечивающих (частных) методик производилась с учетом того, что к обеспечивающим методикам должны предъявляться достаточно жесткие требования на точность и надежность полученных результатов (исходных данных).

Вполне очевидно, что типы и количество используемых средств защиты зависят от важности объекта (ценности защищаемой информации), доступности (наличия на рынке услуг) необходимых технических средств и финансовых возможностей.

Существуют различные подходы к определению состава средств, используемых в системах защиты информации. Применительно к коммерческим, промышленным и банковским структурам в основу может быть положен экономический ущерб, при обеспечении безопасности информации в АСП — показатели уровня снижения эффективности кораблей, оснащенных АСУ [3]. Однако при любом подходе показателем эффективности системы защиты должен служить, как показано ранее, уровень (вероятность) сохранения конфиденциальности информации. Исходя из этого уровня тем или иным способом обосновывается структура системы защиты, определяются номенклатура и состав используемых технических средств.

Сущность предлагаемой методики заключается в том, что на основе исходных данных, в качестве которых используются технические характеристики средств защиты информации, вероятность решения свойственной задачи, стоимостного показателя и коэффициента важности задачи, сначала выбирается конкретный тип средства по частной задаче (например, по защите от НСД), а затем определяется количество выбранных средств в структуре системы защиты в целом.

Для решения указанной задачи предлагается использовать методы экспертных оценок [4]. В качестве показателя степени рациональности предлагается использовать величину «потенциала» полезности. Под потенциалом образца или одного из его элементов понимается безразмерная величина, отражающая степень «полезности» образца (элемента).

При выборе наилучшего образца (элемента) из нескольких альтернативных каждый образец представляется как многоуровневая техническая система, состоящая из нескольких подсистем, элементов. Каждый элемент образца также может быть представлен как система подэлементов и так далее до установления целесообразной для данной задачи степени детализации.

Расчет потенциала системы защиты начинается с расчета потенциалов его элементов (подэлементов). Исходными данными для расчета потенциалов являются технические характеристики образцов (элементов, подэлементов), стоимости и весовые коэффициенты значимости каждой характеристики, назначаемые экспертами. Набор характеристик должен отражать основное свойство образца (элемента). Сравниваемые образцы и их элементы должны иметь идентичный набор характеристик, выбор числа и номенклатуры характеристик осуществляется экспертом.

Рассчитанные потенциалы элементов (подэлементов) вводятся в расчет потенциалов элементов более высокого иерархического уровня в качестве одной из их характеристик. Образец (элемент), обладающий наибольшим потенциалом, является наиболее предпочтительным.

Ниже приведена методика выбора наиболее предпочтительного варианта состава программных, программно-аппаратных и технических средств из нескольких альтернативных.

Пусть имеется $i = 1,2,...,n$ образцов, каждый из которых может быть представлен как техническая система из $l = 1,2,.. .,s$ элементов. Каждый образец имеет $j = 1,2,...,h$ характеристик; аналогично образцу каждый элемент имеет $e = 1,2,...,h$ характеристик.

Расчет масштабированных значений характеристик каждой группы осуществляется следующим образом. Для заданной характеристики y определяется диапазон изменения значений:

$$x_{i,j}^{min} \le x_{i,j} \le x_{i,j}^{max}, \quad (1)$$

где $x_{i,j}$ - значение *j*-ой характеристики *i*-го образца;

$x_{i,j}^{\min}$ и $x_{i,j}^{\max}$ - наименьшее и наибольшее значения *j*-ой характеристики *i*-го образца соответственно.

Положительный эффект характеристики может быть связан как с увеличением ее значения, так и с его уменьшением. Для характеристик, с увеличением значения которых «полезность» образца увеличивается, масштабирование выполняется по формуле:

$$x_{i,j}^{m} = \frac{x_{i,j} - x_{i,j}^{min}}{x_{i,j}^{max} - x_{i,j}^{min}}, \quad (2)$$

где $x_{i,j}^{m}$ - масштабированная характеристика образца.

Для характеристик, с увеличением значения которых «полезность» образца уменьшается, (например стоимости) масштабирование выполняется по формуле:

$$x_{i,j}^{m} = \frac{x_{i,j}^{max} - x_{i,j}}{x_{i,j}^{max} - x_{i,j}^{min}}. \quad (3)$$

Каждая характеристика вносит определенный вклад в «полезность» образца. Эксперт определяет этот вклад для каждой группы характеристик коэффициентом «полезности» $K_j \in [0,1]$. Коэффициент K_j для характеристики, имеющей наибольшее значение, $K_j \rightarrow max$, в противном случае - $K_j \rightarrow min$.

При присвоении значений K_j должно выполняться требование:

$$\sum_{1}^{m} K_j = 1, \quad (4)$$

где m - количество характеристик образца (элементов).

Потенциал образца рассчитывается по следующей формуле:

$$P_i = \sum_{1}^{m} K_{i,j} * x_{i,j}^{m}, \quad (5)$$

где P_i - потенциал i - го образца;

$i = 1,2,.....,n$;

n - количество сравниваемых образцов;

$j = 1,2,....,m;$

m - количество характеристик образца.

Приоритет отдается образцу, потенциал которого выполняет условие $P_i \rightarrow max$.

Аналогичным образом рассчитываются потенциалы элементов (подэлементов). Полученные потенциалы элементов (подэлементов) P_i (l=1,2,...,s) используются в расчете потенциалов образцов (элементов).

Анализ результатов вычислений позволяет эксперту отранжировать ряд альтернативных образцов в порядке возрастания их «полезности».

На основе данного математического аппарата разработана расчетная методика, позволяющая количественно оценить технико-экономическую эффективность варианта построения СКЗИ.

Сущность методического подхода к оценке влияния выбранного для СКЗИ как сложной технической системы состава технических средств, обеспечивающих решение свойственных задач, на величину показателя эффективности заключается в сравнении интегральных возможностей СКЗИ в одинаковых условиях применения.

Выполнение такой оценки возможно с использованием специально разработанной расчетной методики.

Методика обеспечивает:

- расчет показателя технико-экономической эффективности СКЗИ (до 5 вариантов) с учетом состава технических средств, влияющих на её возможности, их размещение на объектах АСП принятого класса защиты (модели использования СКЗИ);

- оценку степени выполнения требований ТТЗ (ОТЗ) на комплексную СЗИ.

В качестве основных исходных данных используются:

- численные значения показателей эффективности [3] - математическое ожидание доли сохраненной информации решения свойственных задач (z) каждым средством (i) – $M_{z,i}$;

- заданные в ТТЗ уровни решения z-ой задачи защиты – $M_{mp.z,j}$;

- коэффициенты «важности» z-ой задачи защиты для i-го средства - $K_{z,i}$;

- стоимость i-го средства.

Исходные данные представляются в табличном виде:

- на каждый вариант СКЗИ заполняется таблица «$M_{z,i}$» (см. табл. 1), численные значения показателя рассчитываются по специальным методикам или выбираются из прайс-листов и каталогов;

- заполняется таблица «$K_{z,i}$» (см. табл. 2), численные значения коэффициентов Kz,i представляют экспертную оценку значимости каждой решаемой задачи для i-го средства;

- по данным ТТЗ заполняется таблица «$M_{mp.z,j}$» (см. табл. 3), представляющая собой вариант использования СКЗИ (класс защиты);

- заполняется таблица стоимостных показателей «$C_{к,i}$» (см. табл. 4) для средств, используемых для каждого класса защиты;

- заполняется таблица требований к техническим средствам по каждой задаче в зависимости от класса защиты.

Таблица 1

	$i=1$	$i=2$	...	i	...	$i=10$
$z=1$	$M_{1,1}$					
...			...			
z				$M_{z,i}$		
...					...	
$z=10$						$M_{10,10}$

Таблица 2

	$i=1$	$i=2$	...	i	...	$i=10$
$z=1$	$K_{1,1}$					
...			...			
z				$K_{z,i}$		
...					...	
$z=10$						$K_{10,10}$

Таблица 3

	j=1	*j=2*	...	*j*	...	*j=10*
z=1	$Mmp._{1,1}$					
...			...			
z				$Mmp._{z,k}$		
...					...	
z=5						$Mmp._{5,10}$

Таблица 4

	i=1	*i=2*	...	*i*	...	*i=10*
K =1	$C_{1,1}$					
K=2			...			
K=3						$C_{3,10}$

Упрощенная блок- схема алгоритма методики представлена на рисунке 2.

Результаты расчетов представляются в табличной форме и в виде диаграмм относительных показателей технико-экономической эффективности каждого варианта СКЗИ применительно к каждому классу защиты (см. табл. 5) и оценки степени выполнения требований ТТЗ по каждой задаче защиты (см. табл. 6).

Таблица 5

КЛАСС ЗАЩИТЫ	ВАРИАНТ СИСТЕМЫ ЗАЩИТЫ				
	С-1	С-2	С-3	С-4	С-5
КЛАСС А					
КЛАСС В					
КЛАСС С					

2 Методика количественной оценки защищенности информации от НСД при проектировании АСУ

По существу, в РД ГТК перечислены функции, подлежащие реализации в СЗИ от НСД. Эти функции позволяют достаточно полно представить состав системы защиты от НСД на концептуальном уровне. Однако этого совершенно недостаточно для решения задачи построения рациональной (выбора рационального варианта) или оценки существующей СЗИ, так как названный перечень требований изложен на качественном уровне. Качественные требования должны быть дополнены количественными.

Вся совокупность количественных требований к СЗИ от НСД к АСП может быть представлена двумя группами. В одну входят требования, значения которых регламентируются нормативными документами аналогично тому, как это сделано для качественных требований в приводимом руководящем документе. Другая группа включает требования, уровень которых задается Заказчиком НИОКР.

Чаще всего это требование задается вероятностью несанкционированного доступа $W_{НСД}$, то есть вероятностью появления события, состоящего в преднамеренном либо (реже) случайном взломе системы защиты и компрометации

Таблица 6

ВАРИАНТЫ СКЗИ	ЗАДАЧИ, РЕШАЕМЫЕ СКЗИ									
	1	2	3	4	5	6	7	8	9	10
С-1										
С-2										
С-3										
С-4										
С-5										

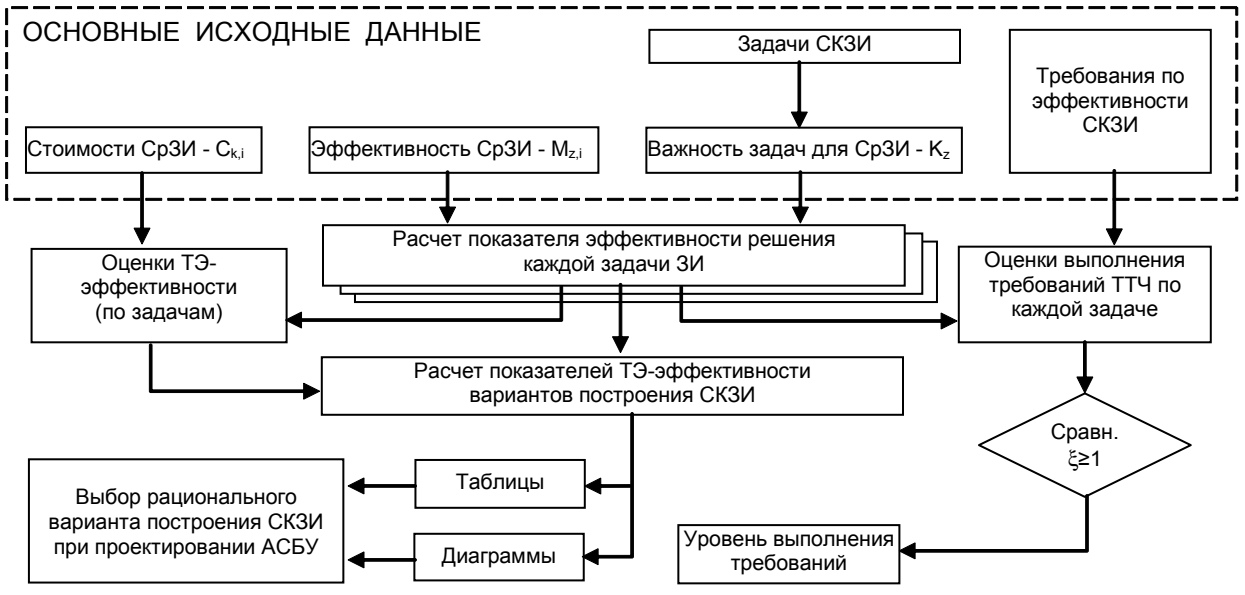


Рис. 2. Блок - схема алгоритма решения задачи технико-экономической эффективности вариантов построения СКЗИ

информации (по определению Гостехкомиссии России — «Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств»). Причем названное требование должно быть определено для КИР всех категорий секретности, циркулирующих в АСП.

Практика построения и эксплуатации СЗИ от НСД показывает, что наиболее действенной является криптографическая защита информации. Поэтому достижимый уровень защиты с помощью названного способа может служить отправным пунктом формирования требований к системе защиты.

В научно-технической и специальной литературе приводятся характеристики наиболее употребимых методов и алгоритмов криптографической защиты (см. табл. 7). Очевидно, что величина, обратная криптостойкости, представляет собой вероятность вскрытия системы криптозащиты.

Другая составляющая искомых требований, соизмеримая по значимости с рассмотренной, задается процедурами идентификации/аутентификации. Причем эти процедуры часто дифференцируют, выделяя более простые составляющие, по которым имеются оценки. К последним принято относить:

- проверку регистрации пользователей (первичную идентификацию);
- аутентификацию запросов на решение задач;
- проверку полномочий пользователя;
- вторичную идентификацию пользователя, проводимую при обращении к информации с грифом "секретно" и выше.

Экспертные оценки показывают, что первые три составляющие обеспечивают уровень защищенности информации примерно 10^{-2}, 10^{-3} и 10^{-4} соответственно. Четвертая имеет достаточно большой диапазон разброса, объясняемый существенным различием используемых методов идентификации.

Методы идентификации/аутентификации обычно классифицируют по используемым средствам:

1) Методы, основанные на знании пароля.

В большинстве АС используются многоразовые пароли. При этом пароль не изменяется в течение установленного администратором системы времени его деятельности. Это упрощает процедуры администрирования, но повышает угрозу рассекречивания пароля путем запуска программы подбора. Более надежный способ — использование одноразовых или динамически меняющихся паролей по закону функции парольного преобразования. Однако они также не обеспечивают абсолютной защиты (например, при подключении злоумышленника к сети и перехвата передаваемых пакетов).

Таблица 7

Стойкость основных алгоритмов криптографической защиты

Алгоритм	Длина ключа (бит)	Скорость шифрования (Кб/с)	Криптостойкость (кол-во операций)	Реализация
DES	56	10-200	10^{17}	Программная
Triple DES	112	1/3 DES	> DES	Программная
ГОСТ 28147-89	256	50-70	10^{70}	В основном аппаратная
RSA	300-600	300-500	Зависит от длины ключа, как правило, 10^{23}	Программная, аппаратная

2) Комбинированные методы идентификации, требующие кроме знания пароля и наличия устройства, подтверждающего подлинность субъекта.

К таким устройствам можно отнести пассивные карточки с магнитной полосой и интеллектуальные карточки. Использование первых исключает возможность перехвата по каналам связи, однако они существенно дороже паролей, требуют специальных устройств чтения, известны случаи их подделки. Вторые позволяют реализовать различные варианты защиты ввиду своей многофункциональности, однако имеют высокую стоимость.

3) Методы аутентификации, основанные на измерении биометрических параметров человека.

Эти методы нельзя использовать при идентификации процессов или данных, они требуют сложного и дорогостоящего оборудования, что обуславливает их использование только в особо важных системах.

Наиболее широко используемые биометрические атрибуты и соответствующие им методы идентификации следующие:

- отпечатки пальцев (сканеры отпечатков пальцев имеют небольшой размер, универсальны и относительно недороги; биологическая повторяемость отпечатка составляет 10^{-5} %,);
- геометрия руки - биологическая повторяемость около 2 %;
- радужная оболочка глаза — теоретическая вероятность совпадения двух оболочек составляет ничтожно малую величину;
- термический образ лица — соответствующие сканеры позволяют идентифицировать человека на расстоянии до десятков метров, однако при изменении освещенности они имеют относительно высокий процент ошибок;
- голос — данная технология стоит менее 25$, а вероятность ошибки составляет 2-5 %.

4) Доказательство подлинности пользователя по его местоположению.

Данный механизм аутентификации основан на использовании системы GPS (Global Positioning System), которая может с точностью до метра определить местоположение пользователя. Аппаратура GPS проста, надежна в использовании и сравнительно недорога. Это позволяет применять ее в случаях, когда удаленный пользователь должен находиться в определенном месте.

Резюмируя возможности механизмов и средств аутентификации по уровню информационной безопасности, можно выделить 3 вида аутентификации: статическую, устойчивую и постоянную.

Статическая - обеспечивает защиту только от НСД в системах, где нарушитель не может во время сеанса работы прочитать аутентификационную информацию (например, пароли). Ее эффективность преимущественно зависит от сложности процедуры угадывания и собственной защищенности. Для компрометации статической аутентификации нарушитель может подсмотреть, подобрать, угадать или перехватить аутентификационные данные.

Устойчивая - использует динамические данные аутентификации, меняющиеся с каждым сеансом работы (например, одноразовые пароли). Устойчивая аутентификация обеспечивает защиту от атак, где злоумышленник может перехватить и в дальнейшем использовать аутентификационную информацию. Однако она не обеспечивает защиту от активных атак, в ходе которых злоумышленник может в течение сеанса аутентификации перехватить, модифицировать информацию и вставить ее в поток передаваемых данных.

Постоянная - обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной модификации или вставки.

Диапазон стоимости и уровня эффективности методов и технологий аутентификации иллюстрируют рисунки 3.а) и 3.б) соответственно.

Полная вероятность ошибочной идентификации определяется произведением аналогичных вероятностей частных независимых процедур. Тогда потенциально достижимая вероятность НСД будет произведением вероятностей ошибочной идентификации и вероятности вскрытия системы криптозащиты.

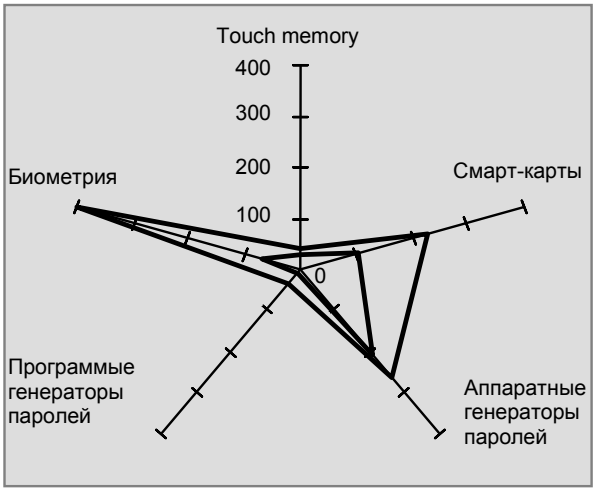
Очевидно, что выбор требований, соответствующих граничным значениям этого диапазона, не может быть признан удовлетворительным:

- минимальному значению удовлетворяет любое сочетание методов идентификации и криптографии, что, с одной стороны, сводит задачу построения СЗИ от НСД к тривиальной, а, с другой стороны, неоправданно занижает достижимый наличными методами уровень защищенности информации;

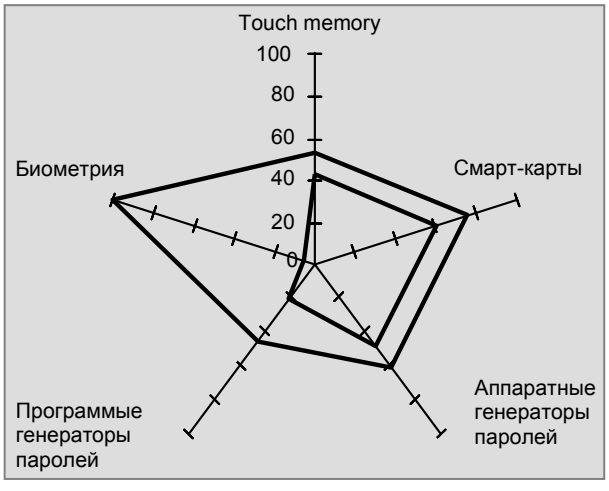
- максимальному значению соответствует единственный вариант СЗИ от НСД, который в той же мере тривиален. Достижимый при этом уровень защищенности информации сопряжен с максимальными издержками и поэтому не может приниматься как оптимальный.

Требования к создаваемой СЗИ от НСД должны лежать в найденном диапазоне и задаваться с учетом степени конфиденциальности защищаемых КИР. Более того, полученный выше диапазон возможного изменения требований по вероятности НСД не является непрерывным, а представляет собой апериодический ряд дискретных значений, что объясняется конечным числом сочетаний различных методов криптографии и идентификации. Этот факт можно рассматривать как еще одно дополнительное ограничение при формировании требований. Правда, это ограничение нельзя признать сильным, поскольку решение задачи рационализации СЗИ от НСД в любом случае сведет начальное требование к ближайшему дискретному значению.

На практике Исполнитель НИОКР самостоятельно формирует указанные требования, оценивая их реализуемость с точки зрения своих



а)



б)

Рис. 3. Диапазон стоимости (на одного пользователя, в у.е.) и уровня эффективности методов и технологий аутентификации

производственных, технологических и финансовых возможностей. Последнее означает лишь то, что в этом случае Исполнитель выполняет обязанности Заказчика. Такой порядок нельзя признать удовлетворительным - формирование требований к СЗИ от НСД должно исходить из потребности внешней по отношению с АСП системы. Возникающие расхождения в уровнях потребных и реализуемых значений могут устраняться путем взаимных согласований.

Для повышения обоснованности требований Заказчика по защищенности информации в АСП, согласования их с возможностями Исполнителя по построению рациональной СЗИ от НСД требуется инструмент количественной оценки вероятности НСД, а именно методика оценки защищенности информации от НСД. Кроме указанной задачи такая методика была бы полезна для научно-обоснованной ревизии существующих нормативных требований. Сегодня подобная методика отсутствует, однако, уже наработаны отдельные ее элементы, позволяющие получать количественные оценки защищенности информации.

Полученное в [5] выражение целевой функции СЗИ от НСД является функцией многих переменных, каждая из которых относится к одному из трех типов. Поскольку каждый блок алгоритма описывается двумя переменными — временем T_i и стоимостью S_i, а блок условного перехода еще и $P_{i,j}$, то общее количество аргументов рассматриваемой функции составляет:

$$l = 2^* n + m, \quad (6)$$

где n - общее количество блоков;

m - число количества условного перехода.

Учитывая, что $n = 42$, а $m = 13$, можно получить $l = 97$.

Столь большое число аргументов значительно затрудняет подготовку исходных данных. Поэтому целесообразно ввести некоторую их классификацию, объединив близкие по значению переменные в отдельные группы.

Применительно к временным параметрам достаточно выделить четыре характерных значения T_i.

Наибольшим быстродействием отличаются блоки условного перехода. Таким образом, можно записать:

$$t_1 = Ti,\ i \in \{1,\ 5,\ 6,\ 12,\ 15,\ 18,\ 19,\ 22,\ 25,\ 33,\ 34,\ 37,\ 38,\ end\}, \quad (7)$$

где end - индекс конечного блока алгоритма.

Целесообразно выделить блоки, требующие однократного обращения к внешней памяти, а также блоки, время выполнения которых условно можно считать коротким и длинным.

К блокам с однократным обращением к внешнему запоминающему устройству (ВЗУ) можно отнести те, которые связаны с вызовом подпрограммы и ее достаточно быстрым выполнением. Это блоки, заполняющие различные журналы, формирующие сообщения оператору, осуществляющие различные блокировки и т.п. Обозначая время их работы через t_2, можно записать:

$$t_2 = Ti,\ i \in \{2,\ 3,\ 4,\ 7,\ 8,\ 9,\ 10,\ 11,\ 14,\ 21,\ 24,\ 26,\ 27,\ 30,\ 31,\ 36,\ 39,\ 40,\ 41\}. \quad (8)$$

Третью группу (с коротким временем t_3) составляют блоки, выполняющие, с одной стороны, многократное обращение к ВЗУ, а с другой - относительно определенный и постоянный объем вычислительной работы. В эту группу входят два блока, для которых:

$$t_3 = Ti,\ i \in \{13,\ 28\}. \quad (9)$$

Наконец, в четвертую группу следует включить блоки с неопределенно большим временем выполнения, например такие, как инициализация вирусных детекторов или проверка целостности информационной базы. Таких блоков в рассматриваемом алгоритме пять. Для них:

$$t_4 = Ti,\ i \in \{16,\ 17,\ 20,\ 23,\ 29\}. \quad (10)$$

Таким образом, классифицированы все блоки, за исключением 32-го и 35-го, реализуемых несколькими альтернативными способами.

Аналогичным образом можно поступить со стоимостью обработки запросов в различных блоках.

Если предположить, что весь алгоритм функционирования СЗИ, исключая 32-й и 35-й блоки, реализуется программно, причем на основном оборудовании стенда главного конструктора АСУ, то стоимость каждого блока должна быть пропорциональна времени его работы. Поэтому разбиение параметров S_i может повторять аналогичную процедуру для T_i:

$$\begin{aligned} s_1 &= S_i,\ i \in \{1,5,6,12,15,18,19,22,25,33,34,37,38,end\}; \\ s_2 &= S_i,\ i \in \{2,3,4,7,8,9,10,11,14,21,24,26,27,30,31,36,39,40,41\}; \\ s_3 &= S_i,\ i \in \{13,28\}; \\ s_4 &= S_i,\ i \in \{16,17,20,23,29\}. \end{aligned} \quad (11)$$

Теперь целевая функция становится зависимой от 2*4 + 13 + 4 = 25 переменных и приобретает вид:

$$C = \frac{1}{1 - P_{1,3}P_{5,1}}\left(t_1^{k1}\, s_1^{k2} + P_{1,2}\, C_{2,end} + P_{1,3}(t_2^{k1}\, s_2^{k2} + t_1^{k1}\, s_1^{k2} + P_{5,7}\, C_{7,end})\right), \quad (12)$$

где

$$\begin{aligned} C_{2,k} &= 2t_2^{k1}\, s_2^{k2} + t_1^{k1}\, s_1^{k2} + P_{6,8}\, C_{8,end} + P_{6,9}\, C_{9,end}; \\ C_{7,k} &= 2t_2^{k1}\, s_2^{k2} + t_3^{k1}\, s_3^{k2} + t_1^{k1}\, s_1^{k2} + P_{15,16}\, C_{16,end} + P_{15,17}\, C_{17,end}; \\ C_{8,k} &= 3t_2^{k1}\, s_2^{k2} + t_4^{k1}\, s_4^{k2} + t_1^{k1}\, s_1^{k2} + P_{18,20}\, C_{20,end} + P_{18,24}\, C_{24,end}; \\ C_{9,k} &= t_2^{k1}\, s_2^{k2} + P_{9,31}\, C_{31,k} + P_{9,12}\, C_{12,end} + t_1^{k1}\, s_1^{k2}; \\ C_{16,k} &= t_4^{k1}\, s_4^{k2} + t_1^{k1}\, s_1^{k2} + P_{18,20} C_{20,end} + P_{18,24}\, C_{24,end}; \end{aligned}$$

$$C_{17,k} = t_4^{k1} s_4^{k2} + t_1^{k1} s_1^{k2} + P_{19,16} C_{16,k} + P_{19,21}\left(t_2^{k1} s_2^{k2} + t_1^{k1} s_1^{k2}\right);$$
$$C_{20,k} = t_4^{k1} s_4^{k2} + t_1^{k1} s_1^{k2} + P_{22,end} t_1^{k1} s_1^{k2} + P_{22,23} C_{23,end};$$
$$C_{24,k} = 2t_2^{k1} s_2^{k2} + t_4^{k1} s_4^{k2} + C_{20,end};$$
$$C_{31,k} = t_2^{k1} s_2^{k2} + T_{32}^{n} S_{32} + t_1^{k1} s_1^{k2} + P_{34,8} C_{8,end} + P_{34,36} C_{36,end};$$
$$C_{33,k} = t_1^{k1} s_1^{k2} + P_{33,33} C_{33,end} + P_{33,end} t_1^{k1} s_1^{k2};$$
$$C_{23,k} = t_4^{k1} s_4^{k2} + t_1^{k1} s_1^{k2} + P_{25,27} C_{27,end} + P_{25,28}\left(t_3^{k1} s_3^{k2} + t_1^{k1} s_1^{k2}\right);$$
$$C_{36,k} = t_2^{k1} s_2^{k2} + t_1^{k1} s_1^{k2} + P_{38,8} C_{8,k} + P_{38,40} C_{40,end};$$
$$C_{27,k} = 2t_2^{k1} s_2^{k2} + t_1^{k1} s_1^{k2};$$
$$C_{40,k} = 2t_2^{k1} s_2^{k2} + F_{35,end};$$
$$C_{35,k} = T_{35}^{n} S_{35} + t_1^{k1} s_1^{k2} + P_{37,35} C_{35,end} + P_{37,39}\left(t_1^{k1} s_1^{k2} + t_2^{k1} s_2^{k2}\right).$$

Дальнейшее упрощение целевой функции может быть связано с приданием числовых значений переменным $P_{i,j}$. При этом необходимо иметь в виду, что классификация вероятностей переходов по некоторым типовым значениям невозможна, ибо значение каждой $P_{i,j}$ определяется статистическими данными. За подобными данными можно обратиться к экспертным методам. В таблице 8 приведены оценочные значения вероятностей переходов алгоритма с указанием основных факторов, определяющих их значения.

Таблица 8

Оценочные значения вероятностей переходов

Вероятность	Значение	Доминирующий фактор
$P_{1,2}$	$0,5$	Коэффициент занятости СЗИ
$P_{5,7}$	10^{-12}	Сбой системы
$P_{6,8}$	10^{-10}	Сбой аппаратных средств
$P_{12,33}$	$0,6$	Удельный вес «закрытой» информации
$P_{15,17}$	$0,5$	Возникновение ошибки из-за СЗИ
$P_{18,24}$	10^{-10}	Доступность АСП вирусам
$P_{19,21}$	10^{-3}	Совершенство методов восстановления СЗИ
$P_{22,23}$	10^{-12}	Совершенство методов поддержания целостности информационной базы (ИБ)
$P_{25,27}$	10^{-3}	Совершенство методов восстановления ИБ
$P_{33,k}$	10^{-4}	Длительность обработки запроса
$P_{34,8}$	10^{-3}	Устойчивость процедур идентификации к преднамеренным действиям
$P_{37,39}$	10^{-4}	Длина данных, подлежащих криптографической обработке
$P_{38,8}$	10^{-3}	Частость попыток превышения полномочий

Подстановка этих значений сокращает число аргументов до 12. В результате:

$$C = 2\left(t_1^{k1} s_1^{k2} + 0,5\, C_{2,end} + 0,5\left(t_2^{k1} s_2^{k2} + t_1^{k1} s_1^{k2} + P_{5,7}\, C_{7,end}\right)\right), \qquad (13)$$

где

$$C_{2,k} = 2t_2^{k1} s_2^{k2} + t_1^{k1} s_1^{k2} + 10^{-10} C_{8,k} + C_{9,end};$$
$$C_{7,k} = 2t_2^{k1} s_2^{k2} + t_3^{k1} s_3^{k2} + t_1^{k1} s_1^{k2} + 0.5C_{16,k} + 0.5\, C_{17,end};$$
$$C_{8,k} = 3t_2^{k1} s_2^{k2} + t_4^{k1} s_4^{k2} + t_1^{k1} s_1^{k2} + C_{20,end} + 10^{-10} C_{24,end};$$
$$C_{9,k} = t_2^{k1} s_2^{k2} + 0.6\, C_{31,end} + 0.4\, C_{12,end} + t_1^{k1} s_1^{k2};$$
$$C_{16,k} = t_4^{k1} s_4^{k2} + t_1^{k1} s_1^{k2} + C_{20,end} + 10^{-10} C_{24,end};$$
$$C_{17,k} = t_4^{k1} s_4^{k2} + t_1^{k1} s_1^{k2} + C_{16,end} + 10^{-3}\left(t_2^{k1} s_2^{k2} + t_1^{k1} s_1^{k2}\right);$$
$$C_{20,k} = t_4^{k1} s_4^{k2} + 2t_1^{k1} s_1^{k2} + 10^{-12} C_{23,end};$$
$$C_{24,k} = 2t_2^{k1} s_2^{k2} + t_4^{k1} s_4^{k2} + C_{20,end};$$
$$C_{31,k} = t_2^{k1} s_2^{k2} + T_{32}^{n} S_{32} + t_1^{k1} s_1^{k2} + 10^{-3} C_{8,end} + C_{36,end};$$
$$C_{33,k} = t_1^{k1} s_1^{k2} + C_{33,end};$$
$$C_{23,k} = t_4^{k1} s_4^{k2} + 2t_1^{k1} s_1^{k2} + 10^{-3} C_{27,end} + t_3^{k1} s_3^{k2};$$
$$C_{36,k} = t_2^{k1} s_2^{k2} + t_1^{k1} s_1^{k2} + 10^{-3} C_{8,end} + C_{40,end};$$
$$C_{27,k} = 3t_2^{k1} s_2^{k2};$$
$$C_{40,k} = 2t_2^{k1} s_2^{k2} + C_{35,end};$$
$$F_{35,k} = T_{35}^{n} S_{35} + t_1^{k1} s_1^{k2} + \left(1 - 10^{-4}\right) C_{35,end} + 10^{-4}\left(t_1^{k1} s_1^{k2} + t_2^{k1} s_2^{k2}\right).$$

После решения системы уравнений целевая функция сводится к трехчлену вида:

$$C = a + b \cdot T_{32}^{k1} \cdot S_{32}^{k2} + c \cdot T_{35}^{k1} \cdot S_{35}^{k2}, \qquad (14)$$

где $b = 0,6$;

$c = 6*10^3$;

$$a = 10,8 t_1^{k1} s_1^{k2} + 8,4 t_2^{k1} s_2^{k2} + 1,03 t_3^{k1} s_3^{k2} + 2 t_4^{k1} s_4^{k2};$$

T_{32} – продолжительность процедуры вторичной идентификации;

S_{32} - стоимость процедуры вторичной идентификации;

T_{35} – продолжительность процедуры шифрования/дешифрования;

S_{35} - стоимость процедуры шифрования/дешифрования.

Дальнейшая работа по методике заключается в экспериментах с моделью методом прямого перебора на предмет получения ее количественных оценок на множестве характеристик рассматриваемого массива СрЗИ по отношению к параметрам, критичность результатов которых представляет для исследователя наибольший интерес.

СПИСОК ЛИТЕРАТУРЫ

1. Емельянов А.А., Бочков М.В., Малыш В.Н. Алгоритм адаптивной защиты информации от НСД в корпоративной компьютерной сети // Проблемы информационной безопасности, 2004. - № 3.

2. Осипов В.Ю. Оценка защищенности информационно-вычислительных ресурсов от НСД // Приборы и системы управления, 1996. - № 7.— С. 16-19.

3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях.— М.: Радио и связь, 1999.

4. Буйневич М.В., Туровский О.М. Методология оценки вероятностно—временных характеристик функционирования АСУ аналитическим моделированием.— В сб.: Тез. докл. отраслевой научно-техн. конф. «Моделирование—3».— Л.: ЛГУ, 1986.

5. Емельянов А.А. Модель функционирования системы защиты от НСД к критическим информационным ресурсам при проектировании АСУ // Автоматизация процессов управления, 2009. - №3 (17).