СЕГМЕНТНАЯ МОДЕЛЬ МНОГОУРОВНЕВОГО ДОСТУПА

Я. А. Быков, М. В. Тарасюк

Санкт-Петербургский институт информатики и автоматизации РАН
199178, Санкт-Петербург, 14-я линия ВО, д. 39
<yar@rol.ru>

УДК 681.322.067
Я. А. Быков, М. В. Тарасюк. **Сегментная модель многоуровневого доступа** // Труды СПИИРАН, Вып. 2, т. 2. — СПб.: Наука, 2005.
Аннотация. *В работе рассмотрен сегментный принцип построения автоматизированных систем с многоуровневым доступом, направленный на решение проблемы недекларированных возможностей системо-образующего ПО, прежде всего ОС и СУБД. Главной особенностью предложенного подхода является возможность использования в составе критичных систем несертифицированных компонентов для обработки секретной информации различного уровня доступа при исключении взаимодействия между сегментами либо при использовании в качестве посредников такого взаимодействия специальных компонентов, называемых шлюзами безопасности.* — Библ. 7 назв.

UDC 681.322.067
Y.Bykov, M.Tarasuk. **Segment model of multilevel data processing system** // SPIIRAS Proceedings. Issue 2, vol. 2. — SPb.: Nauka, 2005.
Abstract. *In the paper the segments principles of multilevel automation information systems developing are described. The main advanced of approach is possibility implementation entrusted information technology (for example operations system and data base management system) for processing of data, which are obtained various security classification levels. The supposed approach my be applied under absent straightforward communication between security segments or under implementation in system special components, called by security gateway in order transfer security data from one segment to another*. — Bibl. 7 items.

В условиях рынка информационных технологий (ИТ) РФ актуальны вопросы разработки автоматизированных систем (АС) с многоуровневым доступом на базе недоверенных программно-технических средств (далее ИТ компонентов). Сертифицированные [1] для применения в АС класса 1В и выше средства[1] обладают ограниченной функциональностью и технологически не совершенны по сравнению с их несертифицированными аналогами. Эти средства мало пригодны для решения задач автоматизации военных и правительственных учреждений РФ, являющихся главными, если не единственными, потребителями защищенных ИТ. С другой стороны средства защиты информации (СЗИ), имеющиеся на рынке ИТ РФ[2], не решают проблему недекларированных возможностей (НДВ) и, строго говоря, не могут применяться в составе систем с многоуровневым доступом[3].

[1] К таковым относится, например, сертифицированные по требованиям 3-го класса РД СВТ и 2-го класса РД НДВ операционная система МСВС 3.0 (построена на базе открытого дистрибутива ОС LINUX) и система управления базами данных ЛИНТЕР-ВС (поострена на базе открытых исходных текстов СУБД ORACLE 6.0).

[2] Внешние программные комплексы для несертифицированных ОС (например, ОС WINDOWS 95/98/NT/2000 и межсетевые экраны для IP сетей.

[3] В частности объединение сетей через межсетевые экраны допускается нормативными документами РФ только при условии, что во всех, объединяемых таким образом сетях, обрабатывается информация одного уровня доступа.

В сложившейся ситуации естественным компромиссом является адаптация каждой конкретной системы под специфические требования политики безопасности (ПБ) с целью вычленения и изоляции друг от друга критичных и некритичных ИТ компонентов. Это позволит использовать несертифицированные ИТ в обмен на доработку СЗИ под условия конкретной системы.

Для подавляющего большинства автоматизируемых объектов должностные лица (пользователи систем) могут быть разделены на относительно небольшое число групп, в пределах которых имеют место единые требования к безопасности информации. Частным и наиболее важным с практической точки зрения случаем являются системы, отдельные фрагменты которых обрабатывают информацию одного уровня допуска. Группы ДЛ (доверенных лиц), обладающие равными правами допуска обычно ассоциируются со структурными подразделениями объектов, ДЛ которых выполняют сходные функции. В соответствии с делением ДЛ на однородные группы, произведем декомпозицию многоуровневой системы на соответствующее число частей, называемых далее “сегментами безопасности”, относительно которых будем предполагать выполненными следующие ограничения.

- Отдельные сегменты “информационно” изолированы друг от друга в том смысле, что не используют общих информационных массивов с прямым доступом и напрямую не взаимодействуют между собой.
- Отдельные сегменты используют общие технические ресурсы, например, каналы связи или дисковые накопители файл сервера. Данные средства формируют инфраструктуру безопасности (ИБ). К типовым компонентам ИБ относится коммутационное оборудование ЛВС, маршрутизаторы для подключения к внешним каналам и сетям, операционные системы, средства телекоммуникаций и документооборота, использующие стандартные прикладные протоколы ЭМВОС.
- Доступ пользователей к сегменту предусматривает аутентификацию сертифицированными средствами[4]. Будучи аутентифицированным, пользователь получает формальный доступ ко всей информации, обрабатываемой в сегменте[5].

Возможность для декомпозиции систем заложена в руководящих документах Гостехкомиссии РФ, где выделяется класс систем (2А и 2Б), обрабатывающих информацию одного уровня доступа, однако здесь не приводится каких либо указаний в части возможности объединения двух и более одноуровневых систем в одну многоуровневую и какие при этом требования должны быть выполнены. Нормативно-методическую и правовую основу решения этой проблемы представляют Общие критерии оценки защищенности информационных технологий [2], представляющих определенную степень свободы в трактовке концептуальных вопросов построения модели защиты в системах, где допускаются сложные политики безопасности. Рассматриваемая далее сегментная модель может рассматриваться как базис для построения телекоммуникационных сетей и систем, использующих общие ресурсы. Основные проблемы построе-

[4] Доверенная аутентификация может быть обеспечена большинством внешних средств защиты информации, сертифицированных как программно-аппаратный комплекс, например АККОРД-АМДЗ.

[5] Формальный доступ не означает фактическое предоставление доступа и является правом ДЛ на обработку информации заданного грифа и категории секретности, полученным в соответствии с нормативными документами и процедурами, регламентирующими работу с такими документами. Формальный допуск к информации целесообразно сопоставлять с мандатной, а фактический с дискреционный ПБ.

Труды СПИИРАН. 2005. Вып. 2. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2005. Issue 2. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

ния таких систем возникают при организации взаимодействия сегментов, разделяющих общие информационные массивы. Следуя [3] указные проблемы проистекают из двух типов угроз, далее называемых угрозами каскадирования и угрозами комплексирования.

Суть проблемы каскадирования можно пояснить на следующем примере. Пусть в одном из сегментов (А) обрабатывается информация с грифом “секретно” и “сов. секретно”, а в другом сегменте (Б) - информация с грифом “несекретно” и “секретно”. Тогда при взаимодействии сегментов А и Б возможно понижение грифа сов. секретной информации путем выполнения следующих шагов:

- Понижение грифа сов. секретной информации прямым или скрытым преобразованием в информацию с грифом "секретно" в сегменте А.
- Передача информации из сегмента А в сегмент Б (такая операция является допустимой поскольку ДЛ, допущенные к обоим сегментам, имеют формальный допуск к общей (в данном случае секретной) информации.
- Понижение грифа секретной информации прямым или скрытым преобразованием в информацию с грифом "несекретно".

В [4] вопросы каскадирования риска рассмотрены применительно к системам, для которых определены формальные условия защищенности от подобных угроз. Применительно к сегментной модели данные условия могут быть сформулированы следующим образом: Определим область локализации (Protection Region) как пару чисел $R = (H,S)$, где H — сегмент безопасности, S — уровень секретности, входящий в число разрешенных для обработки в сегменте H. Определим информационный поток, как упорядоченную последовательность областей локализации $R_1R_2...R_N$ такую, что для каждой смежной пары R_iR_{i+1} имеет место H_iH_{i+1} (обработка информации в пределах сегмента) или $S_i = S_{i+1}$ (передача информации из сегмента H_i в сегмент H_{i+1}). Каскадирование риска не возникает, когда для любого информационного потока $R_iR_{i+1}...R_j$ между любой парой сегментов существует, по крайне мере, один переход вида $R_kR_{k+1}..(i < k < j)$, такой, что $H_k = H_{k+1}$, $S_k \geq S_{k+1}$, а класс защищенности сегмента H_k соответствует минимальным требованиям, предъявляемым к системам, обрабатывающим информацию с уровнями критичности S_1 и S_N.

Для борьбы с угрозами каскадирования необходимо административно ограничивать информационные потоки таким образом, что бы решетки ценности (множества грифов и категорий секретности) любой пары сегментов не пересекались друг с другом, либо решетка ценности одного сегмента являлась собственным подмножеством решетки ценности другого сегмента. Подобные требования естественно увязать с иерархическим принципом формирования сегментной структуры, когда к сегментам более высокого уровня иерархии предъявляются более жесткие требования, чем для сегментов низшего уровня иерархии. Иными словами для борьбы с угрозами каскадирования угроз необходимо:

- Исключить или минимизировать горизонтальные потоки информации между компонентами одного уровня иерархии, которые допускаются только при наличии одинаковых требований ПБ во взаимодействующих сегментах.

Труды СПИИРАН. 2005. Вып. 2. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2005. Issue 2. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

- Определять требования к сегментам в соответствии с уровнем иерархии, по отношению к центральному сегменту (корню дерева).

На рис. 1 иллюстрируется принцип формирования решетки ценностей для сегментов *S*, *S*1, *S*2, *S*3, *S*11, *S*12, , для которой проблема каскадирования угроз не возникает.

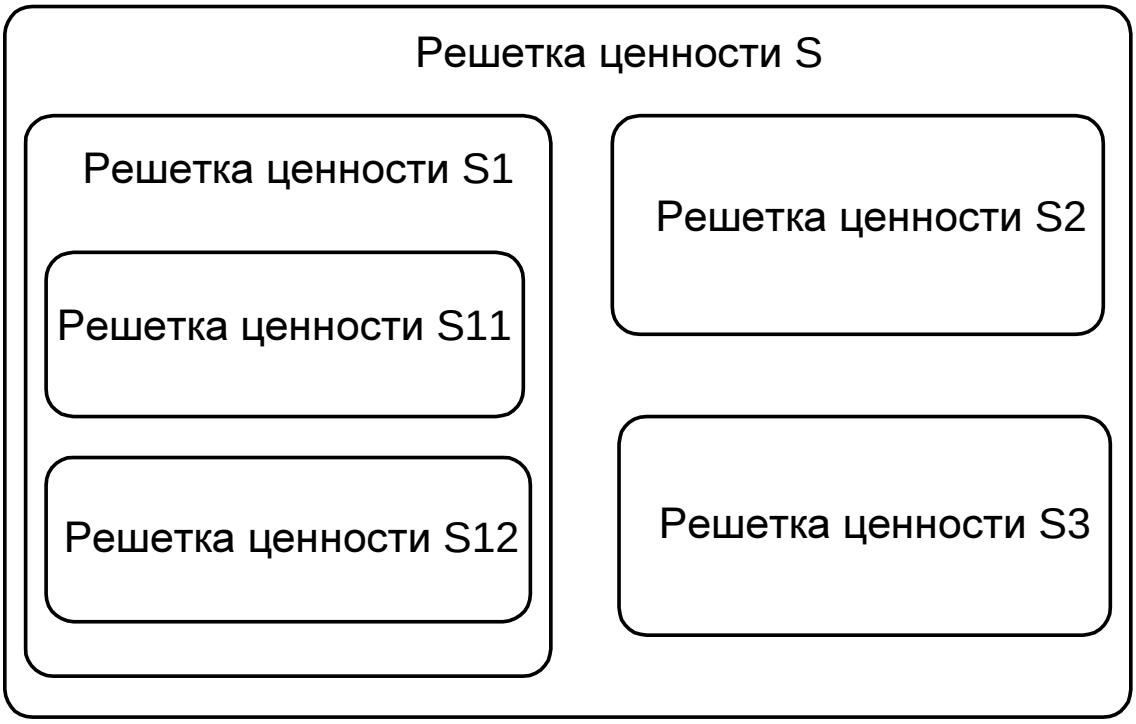

Рис. 1. Решетка ценности в системе с сегментной структурой.

В отличие от угроз каскадирования, проблематика угроз комплексирования связана с НДВ и скрытыми каналами утечки информации, потенциально существующими в ИТ компонентах. В виду этого, для организации взаимодействия сегментов безопасности используются специальные пограничные устройства, далее именуемые шлюзами безопасности (ШБ).

Таксономический анализ природы НДВ и возможных последствий их проявления в ИТ приводит к необходимости рассмотрения следующих классов угроз:

- Нарушение идентификации субъектов и объектов доступа, выражающегося в отсутствии надежных гарантий сопоставления информационных объектов корректным адресам или иного рода локализующим идентификаторам.
- Существование скрытых интерфейсов доступа к системным ресурсам, блокирующих встроенные СЗИ компонентов и приводящих к нарушению правил предоставления доступа к информации.
- Скрытое взаимодействия субъектов и объектов доступа путем модуляции (наложения) данных большего уровня секретности на данные меньшего уровня секретности [5]. Подобные явления принято называть скрытыми кана-

Труды СПИИРАН. 2005. Вып. 2. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2005. Issue 2. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

лами (СК). Например, в [6] рассмотрена схема модуляции и произведена оценка пропускной способности СК VPN устройств, не поддерживающих режим маскировки трафика.

Рассмотрим сегменты А и Б. С учетом влияния угроз НДВ, ШБ должен позволять гарантированно разделять передаваемую информацию на два класса: информацию для локального использования и общую информацию. С этой целью ШБ должен:

- строиться на базе сертифицированных ИТ компонентов по требованиям классов РД, определенных для систем обработки информации соответствующего грифа и категории секретности,
- исключать прямое взаимодействие приложений сопрягаемых сегментов, то есть выдачи запросов обмена информацией,
- обеспечивать идентификацию входящих сообщений от ИТ компонентов, основываясь на анализе структуры данных и априорно заданных ограничениях целостности отдельных атрибутов,
- обеспечивать буферизация потоков данных с целью устранения временной связи между ИТ компонентами,
- исключать передачу между сегментами массивов неструктурированной информации (например, файлов или почтовых сообщений).

Четких рецептов создания ШБ на все случаи жизни существовать не может, поскольку недоверенная среда не гарантирует даже правильной идентификации потоков данных. Кроме того, из выше приведенного перечня функций ШБ следует, что использование технологии шлюзов предъявляет определенные требования к приложениям. В этой связи нужно подчеркнуть, что ШБ не является прозрачным компонентом и по этой причине его нельзя рассматривать как межсетевой экран. ШБ может работать только в конкретной среде с функциональным ПО, реализующим вполне конкретную семантику обработки информации.

Рассмотрим наиболее распространенный случай построения распределенной информационной системы, базирующейся на технологии реляционных СУБД. Для контроля взаимодействия серверов БД, ШБ представляет собой доверенный КЭШ, в который помещается информация, удовлетворяющая ограничениям классификации. Такой шлюз уместно назвать шлюзом репликации, поскольку в его функции входит периодическое обновление той части распределенной БД сегментов, которая сформирована в одном сегменте, но должна быть также передана в другой сегмент. Взаимодействие приложений БД должно осуществляться исходя из предварительного описания схемы данных (атрибутов, сообщений и других реплицируемых объектов), а также ограничения целостности для отдельных атрибутов обновляемых данных. На рис. 2 приведена схема шлюза репликации БД, включающая структуру и взаимосвязь отдельных модулей в процессе репликации БД.

Приведенный пример шлюза репликации для двух сегментов включает три автономно функционирующие подсистемы, в том числе:

- подсистемы формирования запросов, буферизации и предварительной обработки сообщений поступающих из сопрягаемых сегментов, подключенных к физически или логически изолированным интерфейсам;
- подсистема перемещения данных из одного буферного кэша в другой по расписанию или по внешнему событию.

Труды СПИИРАН. 2005. Вып. 2. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2005. Issue 2. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

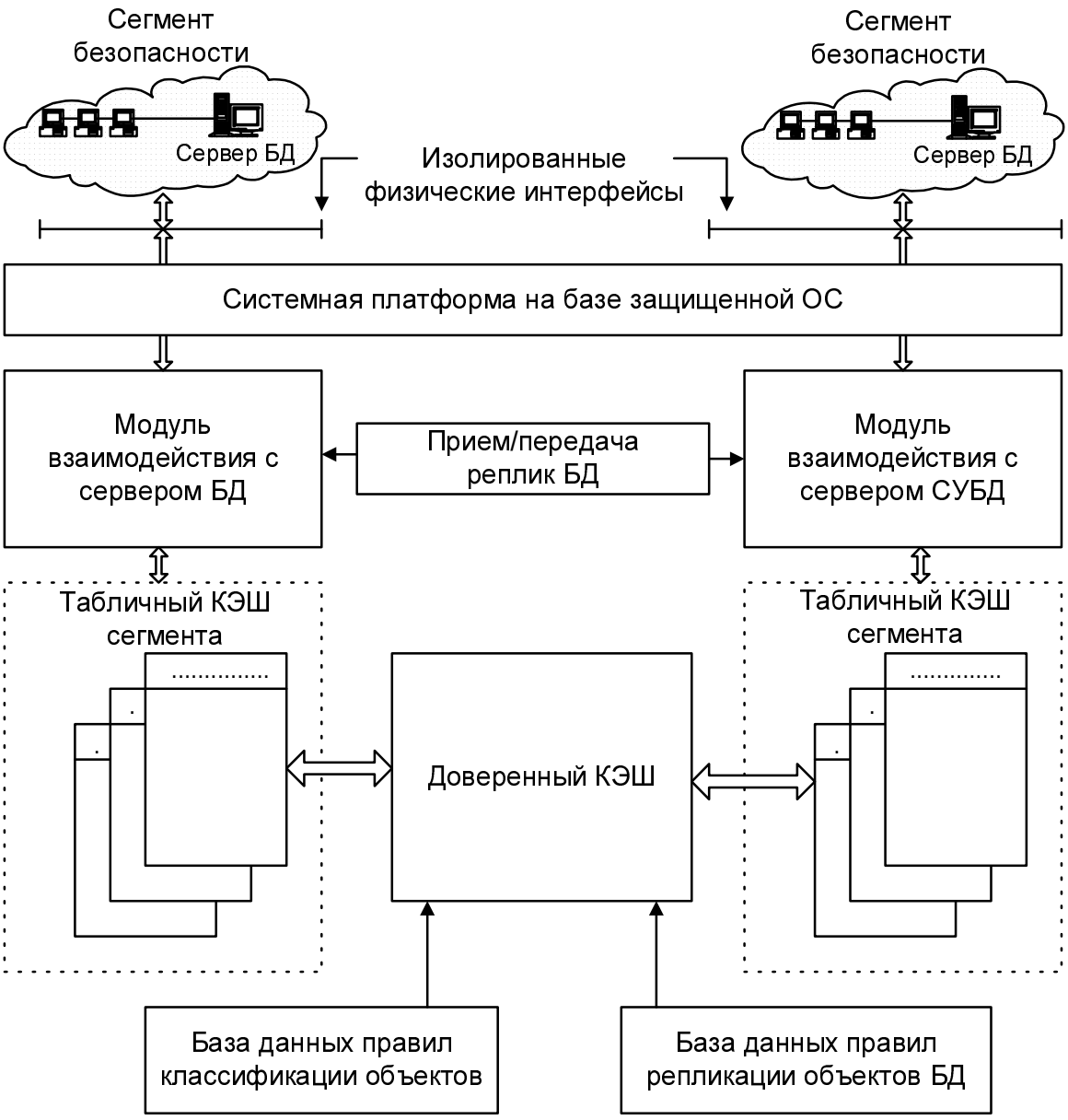

Рис. 2. Структурная схема шлюза репликации распределенной БД.

Труды СПИИРАН. 2005. Вып. 2. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2005. Issue 2. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Заметим, что объединение сегментов шлюзом с целью совместного использования общих БД оправдано в случае если:

- объем реплицируемых данных не слишком велик. В противном случае требования к шлюзу в части производительности и прочих показателей будут расти, в пределе приближаясь к показателям, которые позволят не использовать для построения систем несертифицированные ИТ.
- Сообщения репликации хорошо структурированы, что позволит с большей степенью гарантий выделить характерные элементы и произвести проверку целостности сообщений для ограничения скрытой передачи с использованием методов стеганографии.

В заключении рассмотрим вопрос качественной оценки защищенности сегментированной системы. Для этого каждый ИТ компонент будем характеризовать следующими параметрами:

- A_i - интенсивность прямого воздействия на компонент со стороны потенциального нарушителя,
- P_i - вероятность успешной атаки, обусловленная гарантиями архитектуры и уровнем контроля отсутствия НДВ компонента.

Уровень защищенности отдельных компонентов без учета влияния других компонентов логично характеризовать интенсивностью локально реализованных атак $I_i = A_i P_i$

Для определения уровня защищенности компонентов с учетом влияния других компонентов введем матрицу T. Компоненты S_i и S_j сопряжены по угрозе, если успешная атака на S_i приводит к появлению направленной атаки на компонент S_j. При этом: $T[j,i]=1$. В противном случае $T[j,i]=0$.

Суммарный входной поток атак компонента S_i без учета влияния опосредованных, успешно осуществленных атак[6], определяется соотношением

$$A_i^{\Sigma} = A_i + \sum_{j-1, j+1}^{N} T_{ji} I_j$$

Для упрощения анализа будем предполагать, что каждый компонент системы воздействует строго на K компонентов и, в свою очередь подвергается воздействию на себя со стороны K компонентов. Все компоненты характеризуются едиными значениями S_j и $P_i = P_0$, в результате чего обеспечен баланс потока угроз, то есть для каждого компонента суммарный поток атак равен суммарному выходному потоку деструктивного воздействия на другие компоненты [7]. Интенсивность потока атак на компонент с учетом опосредованного влияния других компонентов A^{∞} определяется уравнением:

$$A^{\infty} = A_0 + PKA^{\infty} \tag{1}$$

Зададимся критерием, согласно которому система защищена при условии если $I^{\infty} = A^{\infty} P \le A_0$. Разумность критерия можно обосновать тем, что при выполнении (1) каждый скомпрометированный компонент в среднем не приведет к

[6] То есть атак на компонент Si, вызванных Sj путем промежуточного воздействия на Sk, когда схема атаки имеет вид Sj→Sk→Si.

Труды СПИИРАН. 2005. Вып. 2. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2005. Issue 2. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

превышению общего потока атак на другие компоненты. С учетом (1) для несегментированной АС, у которой $K = N$ требования к компонентам определяются числом взаимодействующих компонентов системы $P = 1/(1+N)$.

Для выделенного сегмента безопасности поток внешних атак равен потоку угроз ШБ, индицируемых N_1 компонентами других сегментов. Собственный поток угроз ШБ будем полагать равным нулю, поскольку ШБ является по определению доверенной системой. Оценка P для сегментированной системы будет иметь следующий вид $P = 1/(P_{ШЛ} + N_1)$, где $P_{ШЛ}$ - вероятность успешной атаки на ШБ. Таким образом, использование ШБ позволяет снизить требования к компонентам $\approx N/N_1$ раз.

Литература

[1] Руководящий документ Гостехкомиссии при президенте РФ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. 1992.

[2] ГОСТ ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

[3] National Computer Security Center. NCSC-TG-11. Trusted network Interpretation environments Guideline. USA P. 40. — 1990.

[4] National Computer Security Center. NCSC-TG-005. Trusted Computer System Evaluation Criteria. Trusted Network Interpretation. USA P. 203. — 1987.

[5] National Computer Security Center. NCSC-TG-030. Guide to Understanding Covert Channel Analysis of Trusted System. USA P.

[6] *Тарасюк М.* Модель коллизий и оценка пропускной способности скртых каналов в шлюзе VPN сети. // Безопасность информационных технологий, №3, 2002. — с. 10-15.

[7] *Тарасюк М.* Вопросы проектированя защищенных информационных технологий. // СПб: Изд. СПбГИТМО (ТУ), 2002. — 77 с.