ОЦЕНКА ЧИСЛА КАТЕГОРИЙ ДОСТУПА МНОГОУРОВНЕВОЙ СЕТИ НА ОСНОВЕ АНАЛИЗА РИСКОВ КАСКАДИРОВАНИЯ

Я. А. Быков, М. В. Тарасюк

Санкт-Петербургский институт информатики и автоматизации РАН

СПИИРАН, 14-я линия ВО, д. 39, Санкт-Петербург, 199178

<yar@avantlab.com>, <yar@rol.ru>

УДК 681.51.001.57

Быков Я. А., Тарасюк М. В. **Оценка числа категорий доступа многоуровневой сети на основе анализа рисков каскадирования** // Труды СПИИРАН. Вып. 4. — СПб.: Наука, 2007.

Аннотация. *Рассматривается проблема каскадирования рисков применительно к оценке допустимого числа мандатных категорий обработки информации в распределенной системе с многоуровневым доступом. В основе предлагаемого подхода к оценке числа категорий лежит использование меток достижимости для симметричного случайного графа, моделирующего информационное взаимодействие между точками доступа многоуровневой сети.* — Библ. 4 назв.

UDC 681.51.001.57

Bykov Y. A., Tarasuk M. V. **The evaluation of the number of catagories of access of multilevel network based on the analysis of the cascading risk** // SPIIRAS Proceedings. Issue 4. — SPb.: Nauka, 2007.

Abstract. *The problem of cascading of the risk, applied to the evaluation of the number of mandate categories of the information processing in the distributed system with multilevel access is considered. The proposed approach for evaluation of number of categories is based on the usage of marks of attainability for simmetric random graph, that models informational interaction between points of access of multilevel networks.* — Bibl. 4 items.

1. Введение

В основе современных подходов к повышению эффективности управления вооруженными силами лежит концепция «сетеориентированности» боевых действий, в рамках которой инвертируется стандартный цикл обработки информации и принятия решений органами военного управления, что позволяет обеспечить информационное превосходство при оперативном принятии решений. При этом распределению первичной информации среди всех заинтересованных лиц (бойцов и командиров, оснащенных интеллектуальными терминалами для ее интерпретации и анализа) должна предшествовать обработка этой информации вышестоящими объектами в структуре иерархии Вооруженных Сил (ВС).

Подробно данная концепция, а также некоторый весьма успешный опыт ее применения в рамках боевых действий армии США в Иракской войне 2003 года изложены, например, в [1]. Сетеориентированный подход обладает высокой гибкостью и обеспечивает динамическое связывание источников и потребителей информации в условиях априорной неопределенности текущей обстановки на театре военных действий (ТВД).

Вместе с тем указанная гибкость приводит к дополнительным проблемам защиты информации, поскольку значительно затрудняется управление правилами взаимодействия узлов сети, задающими разрешенные информационные потоки в сети (соответствующие принятой политике безопасности).

Политика безопасности в условиях сетеориентированности должна выбираться с учетом специфических угроз безопасности, имеющих место в распределенных многоуровневых системах, одна из которых связана с так называемой проблемой «каскадирования рисков» [2]. Суть данной проблемы в целом сводится к тому, что объединение двух многоуровневых систем с определенным уровнем безопасности в одну систему автоматически не обеспечивает для данной системы уровень безопасности исходных (подлежащих объединению) систем.

2. Основная часть

Вопросы безопасности сетеориентированных систем имеют ряд особенностей, вызванных применимостью к ним так называемых «законов малого мира», согласно которым, несмотря на большое число потенциальных пользователей, существует «относительно короткий» путь, образованный каналами потоков данных, произвольно выбранных пользователей данной сети[1].

Такой путь потенциально обусловливает существование в сетевой инфраструктуре составного, несанкционированного маршрута распространения информации от одного пользователя услуг к другому.

Учитывая, что политика безопасности сетевой инфраструктуры может состоять из множества доменов безопасности, такая инфраструктура подвержена проблеме «каскадирования риска». Данная проблема диктует необходимость ужесточения требований доверия безопасности для сетевой инфраструктуры, лежащей в основе применения сетеориентированного подхода.

В рамках действующей системы классификации и оценки защищенности информационных технологий России, определенной руководящими документами Гостехкомиссии[2], проблема каскадирования риска не рассматривается и не упоминается. Данное обстоятельство в целом обусловлено существовавшей на момент введения данных руководящих документов архитектурной парадигмой, согласно которой:

- автоматизированные и информационные системы создаются для автономной обработки и распределения информации между отдельными объектами в соответствии с жестко предопределенными правилами — (автономные системы);
- вся функциональность обработки, хранения и использования данных реализуется в выделенных системах высокой производительности с доступом в терминальном режиме — (системы терминального доступа на базе больших ЭВМ);
- управление политикой безопасности автоматизированных систем осуществляется централизованным способом — (системы с централизованным управлением).

Данная архитектурная парадигма в настоящее время давно устарела и не соответствует требованиям сетеориентированных систем, которые являются существенно распределенными по обработке, хранению, распределению и доступу к информации и услугам. Однако именно для сетеориентированных систем

[1] Согласно закону Эрдоса Реньи, среднее расстояние связности между узлами большой сети имеет логарифмическую зависимость от радиуса данной сети (числа узлов).

[2] В настоящее время приемником полномочий Гостехкомиссии России является Федеральная служба по техническому и экспортному контролю (ФСТЭК РФ).

Труды СПИИРАН. 2007. Вып. 4. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2007. Issue 4. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

и инфраструктур в основе их построения проблема каскадирования рисков в наибольшей степени актуальна.

Для решения проблемы каскадирования рисков можно предложить следующие меры повышения безопасности, в числе которых[3]:

- повышение уровня качества и общей программной надежности средств обработки и защиты информации;
- исключение использования в оконечных системах сетевой инфраструктуры недоверенных программных средств;
- ограничение режима функционирования оконечных систем для минимизации вероятности неконтролируемого распространения информации между разными уровнями доступа.

При взаимодействии двух и более систем с пересекающимися категориями конфиденциальности потенциальный информационный поток между произвольно выбранными узлами сети, очевидно, определяется числом категорий (меток) конфиденциальности, в рамках которых передача информация разрешена политикой безопасности.

На рис. 1 показан пример взаимодействия двух систем с перекрывающимися «решетками» ценности. Логично предположить, что несанкционированный поток информации между компонентами взаимодействующих систем пропорционален «степени перекрытия» множеств неиерархических категорий конфиденциальности для взаимодействующих сегментов сети.

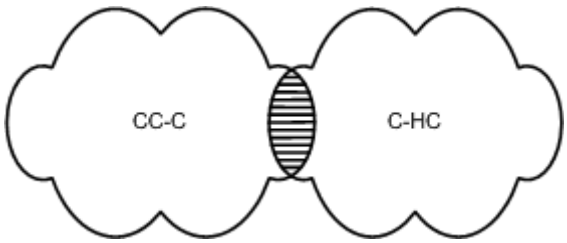

Рис. 1. Пример взаимодействия двух систем с перекрывающимися «решетками» ценности.

В качестве меры уменьшения рисков каскадирования можно предложить увеличить число уровней обработки информации — включить в модель защиты инфраструктуры и оконечных систем достаточное число неиерархических категорий конфиденциальности [3]. При этом минимизируется уровень избыточности мандатных прав доступа для потенциального взаимодействия систем.

Повышение числа уровней обработки (категорий конфиденциальности) позволит увеличить степень охвата услуг и ресурсов мандатными механизмами контроля, обеспечивающими бо́льший уровень доверия безопасности, чем дискреционные (избирательные) механизмы управления доступом. Далее, будем предполагать, что домены инфраструктуры состоят из одного или более «сегментов безопасности», число которых пропорционально числу категорий конфиденциальности, разрешенных для обработки в домене политикой безопасности данного домена.

[3] В документе [2] доказана теорема, дающая необходимые и достаточные условия, выполнение которых исключает возникновение рисков каскадирования. Частым случаем данных условий является построение систем на принципе иерархической упорядоченности сегментов безопасности.

Труды СПИИРАН. 2007. Вып. 4. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2007. Issue 4. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Для оценки эффекта каскадирования рисков сетевой инфраструктуры и обоснования требуемого числа уровней конфиденциальности в оконечных системах будем основываться на следующих предположениях:

- в доменах безопасности инфраструктуры обрабатывается информация разного уровня конфиденциальности, в том числе информация, предназначенная для локального использования, и информация, разделяемая посредством сетевых услуг с другими доменами;
- инфраструктура в целом состоит из определенного числа сегментов безопасности, наложенных на доменную структуру (состоящую из N сегментов), в пределах которых эффектами каскадирования рисков можно пренебречь.

Оценка эффекта каскадирования может быть выполнена исходя из наиболее общих представлений о распределенных сетях, а именно степень безопасности сети обратно пропорциональна связности сети. В среднем менее связанные сегменты будут более защищены (фактически любая возможность взаимодействия несет потенциальную угрозу безопасности). Соответственно вероятность задания направлений взаимодействия между сегментами в домене косвенно определяет вероятность несанкционированной связи (маршрута) между произвольно выбранными сегментами.

Риск каскадирования может быть определен через вероятность «просачивания» информации по составному маршруту скрытого взаимодействия (между системами, подключенными к инфрастуктуре), которая в общем случае будет увеличиваться с ростом числа сегментов безопасности в каждом из доменов.

Связность сети можно охарактеризовать множеством коэффициентов $\{A_{ij}\}$, где $A_{ij} \in [0,1]$, выражающих вероятность прямого взаимодействия между произвольно выбранной парой сегментов безопасности S_i и S_j. Случайный составной маршрут может быть представлен как маршрут в ориентированном графе между сегментами S_i и S_j при условии, что прямое взаимодействие между ними не определено.

В произвольной инфраструктуре, обладающей сложными взаимосвязями и сложной политикой безопасности, установить или даже оценить порядок значений $\{A_{ij}\}$ не представляется возможным. Для оценки граничных рисков каскадирования без учета особенностей обработки и распространения информации можно рассмотреть простейший случай, когда все сегменты одинаково критичны к угрозам безопасности и способу нацеливания угрозы (все значения $\{A_{ij}\}$ одинаковы). Сеть моделируется случайным графом с равновероятной связностью вершин, где каждая из вершин в среднем связана с другими вершинами одинаковым числом направлений [3]. По соображениям симметрии данная упрощенная модель в среднем будет оптимальной для нарушителя, случайно выбирающего конечную цель (объект) НСД.

Реализация угрозы (несанкционированный поток данных) представляет собой возникновение составного пути в случайном графе, связывающем две произвольные вершины (сегмента). Пусть требуется передать информацию из сегмента S_i в сегмент S_j.

Оценка вероятности случайного возникновения маршрута (риск каскадирования) P_N между произвольными сегментами инфраструктуры радиуса N

Труды СПИИРАН. 2007. Вып. 4. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2007. Issue 4. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

(из N сегментов) с учетом транзитивных связей в зависимости от значения параметров A и N задается рекуррентным соотношением

$$P_N = A + (1-A)(1-(1-A)^{N-1})P_{N-1},$$

где P_N и P_{N-1} — вероятности взаимодействия в сетях, состоящих из N и $N-1$ сегментов;

A — средний коэффициент связи по направлениям для сетевой инфраструктуры в целом (о его вычислении будет сказано далее).

Информация с вероятностью $1-(1-A)^{N-1}$ будет передаваться и использоваться в каком-либо промежуточном сегменте, если прямое направление взаимодействия не определено, после чего процедура повторяется с уменьшенным на единицу числом сегментов (предполагается, что в сети отсутствуют петли и любая информация передается между сегментами не более одного раза).

Зависимости P_N от A и N ($A=0.05$, $A=0.1$, $A=0.15$) представлены на рис. 2 и показывают, что с ростом A и N вероятность неконтролируемого распространения информации между любыми выбранными сегментами безопасности быстро возрастает. При этом большее значение A соответствует более выраженному возрастанию P_N.

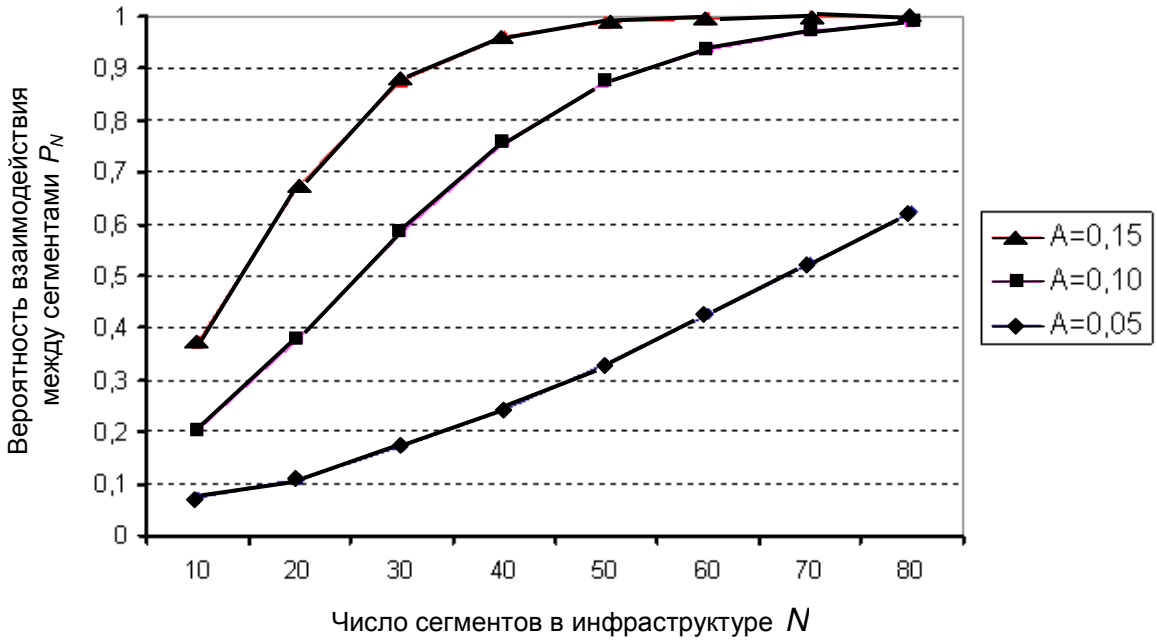

Рис. 2. Примеры зависимостей $P_N(A,N)$.

Граничную оценку допустимости угрозы каскадирования риска можно задать, если трактовать характеристику P_N как усредненное число непосредственно взаимодействующих сегментов. Тогда при выбранной структуре взаимодействий приращение $D[P_n]$ величины P_N можно считать критическим, если оно соответствует увеличению на единицу среднего числа скрытых взаимодействий для каждого сегмента. Тогда $D[P_N]+P_N = 1-(1-P_N)(1-1/N)$ и относи-

Труды СПИИРАН. 2007. Вып. 4. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2007. Issue 4. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

тельно A может быть вычислено критическое приращение $D[A]$, вызывающее появление несанкционированных потоков информации.

На рис. 3 показаны примеры построения граничной оценки каскадирования риска в зависимости от числа сегментов N и параметра A.

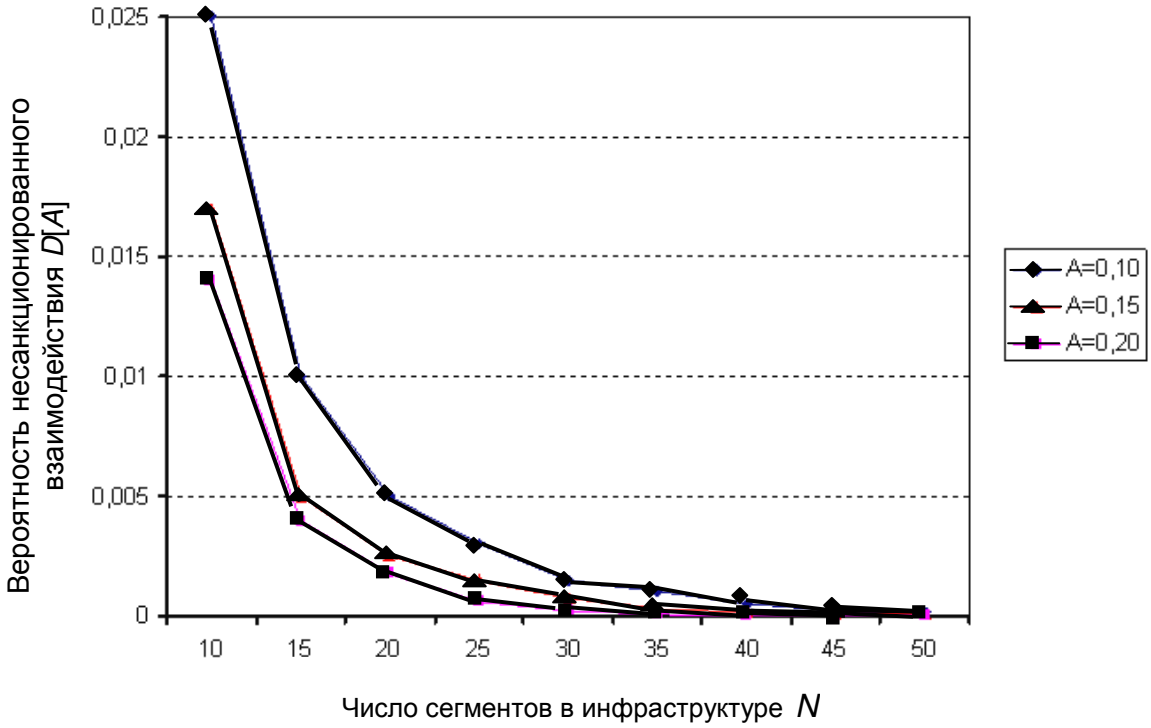

Рис. 3. Примеры построения граничной оценки каскадирования риска в зависимости от числа сегментов N и параметра A.

Точки, лежащие левее и ниже на соответствующих графиках, задают предельно допустимые значения $D[A]$, из которых определяется число уровней безопасности для оконечных систем (L) и соответственно число категорий конфиденциальности (неиерархические метки конфиденциальности) по формуле $L = 1/D[A]$. Для оценки числа уровней функционирования должна использоваться следующая методика:

- устанавливается общее число объектов (автоматизированных систем или терминалов абонентов), использующих услуги инфокоммуникационной инфраструктуры — N;
- для каждой автоматизированной системы S определяется среднее число направлений взаимодействия с другими автоматизированными системами, подключенными (предполагающими подключение) к сетевой инфраструктуре — N_S;
- вычисляется средний коэффициент связи по направлениям для сетевой инфраструктуры в целом — $A = \sum N_S / N^2$;
- по графикам (рис. 3) на основе значений A и N вычисляются значения $D[A]$ и L (число неиерархических категорий конфиденциальности).

Для организации взаимодействия доменов безопасности автоматизированной системы в пределах сетевой инфраструктуры должны использоваться пограничные системы — шлюзы, выполняющие конвертацию и контроль пото-

Труды СПИИРАН. 2007. Вып. 4. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2007. Issue 4. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

ков информации. При этом для взаимодействия доменов, обладающих одинаковым набором категорий конфиденциальности, можно ограничиться устройствами защиты (межсетевыми экранами или шлюзами взаимодействия), реализующими политику безопасности на уровне служебных атрибутов.

Для снижения дополнительных рисков «просачивания» информации при взаимодействии доменов, обрабатывающих информацию разных классов конфиденциальности, потребуется применение семантических механизмов контроля содержимого передаваемых данных.

3. Заключение

Рассмотренная модель позволяет задать множество неиерархических категорий конфиденциальности, которые минимизируют скрытые несанкционированные потоки в рамках мандатной политики безопасности. Множество категорий является входной информацией для задания конфигурации мандатных правил разграничения доступа в системе, как предписывается соответствующими стандартами и нормативными документами, например [4]. Однако при этом система в целом становиться более «жесткой» с точки зрения возможности взаимодействия вне рамок детерминированных правил безопасности. В конечном счете данная ситуация потребует разработки специальных подходов и механизмов автоматического управления политикой безопасности для оперативного предоставления прав взаимодействия по требованию вместо априорного задания всего множества правил, что является очень сложной самой по себе задачей.

Литература

1. *MacDonald Bradley.* The semantic web foundations of net-centric warfare [Электронный ресурс]. USA. 2004 // <http://www.mcdonaldbradley.com> (по состоянию на 20.05.2005).
2. NCSC-TG-005. Trusted Computer System Evaluation Criteria. Trusted Network Interpretation. USA: National Computer Security Center, 1987. 203 p.
3. *Тарасюк М. В.* Вопросы проектирования и применения защищенных информационных технологий. М.: СОЛОН-Пресс, 2004. 192 с.
4. Standard Security Label for Information Transfer. USA: National Institute of Standard and Technology FIPS PUB 188, 1994. 27 p.