УДК 681.322.067

И.Ю. Гришин[1]

АНАЛИЗ ПЕРСПЕКТИВНЫХ ПОДХОДОВ К ПРОЕКТИРОВАНИЮ СИСТЕМ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Работа посвящена анализу современных подходов к построению систем безопасности распределенных компьютерных сетей (корпоративных, банковских, учебных заведений и т.п.). Исследованы наиболее распространенные за последние 10 лет подходы, сделаны выводы об их эффективности, осуществлен выбор систем защиты для различных условий применения распределенных сетей.

Ключевые слова: *распределенная компьютерная сеть, система безопасности, корпоративная сеть, анализ эффективности, криптографические методы, операционная система.*

I.Yu. Grishin

ANALYSIS OF PROMISING APPROACHES TO DESIGN OF DISTRIBUTED COMPUTER NETWORKS SECURITY SYSTEMS

This article is devoted to analysis of promising approaches to design of distributed computer networks security systems (corporate, banking, educational institutions, etc.). The most common over the last 10 years approaches are explored, and the conclusions on their effectiveness and selection of protection systems for different applications of distributed networks ade made.

Keywords: *distributed computer network, security, enterprise network, efficiency analysis, cryptographic techniques, operating system.*

На рубеже веков существенно возрос объем циркулирующих в компьютерных сетях информационных потоков, характеризующих различные стороны деятельности человеческого общества. Отмечается тенденция экспоненциального увеличения объемов информации, необходимой для принятия решений в различных отраслях народного хозяйства, государственном управлении, финансовом и банковском секторах, научных исследованиях, образовании и т.д. Появилось новое понятие – “big data”, отражающее указанные выше тенденции и указывающее на необходимость обработки нетрадиционно больших объемов информации и их передачи в сетях. Способность общества и его институтов собирать, обрабатывать, анализировать, систематизировать и накапливать информацию является важной предпосылкой социального и технологического прогресса, фактором национальной безопасности, одной из основ успешной внутренней и внешней политики.

В этих условиях становится чрезвычайно актуальной проблема защиты информации, циркулирующей в распределенных компьютерных сетях, поскольку возможное несанкционированной уничтожение, копирование или искажение информации затрагивает интересы как государственных органов, так и юридических и физических лиц, может привести к ошибкам в принятии решений и, как следствие, – к тяжелым последствиям в сфере экономики, экологии, промышленности, государственного и муниципального управления.

Базой для совершенствования систем защиты информации в распределенных компью-

[1] Доктор технических наук, профессор, профессор кафедры компьютерных технологий и информационной безопасности ФГБОУ ВПО «Кубанский государственный технологический университет».

терных сетях являются достижения в области информатики и вычислительной техники, телекоммуникаций, микроэлектроники, системного анализа и ряда других наук.

Таким образом, актуальность проблемы повышения эффективности систем защиты информации в распределенных компьютерных сетях целесообразно анализировать в аспектах мирового общественного развития, экономического развития и развития науки, техники и технологий.

Новые информационные технологии, которые активно развиваются в различных сферах деятельности общества, формируют повышенный спрос на создание систем защиты информации, причем этот спрос часто превышает потребности государственных заказчиков.

Значительный вклад в совершенствование различных аспектов подходов к проектированию систем безопасности распределенных компьютерных сетей внесли такие ученые, как В.А. Хорошко, А.А. Молдовян, В.А. Герасименко, М. Хеллман, Ж. Брассар [1–6] и др.

Однако в сфере проектирования систем защиты информации остается целый ряд проблем, решение которых имеет важное научно-техническое и государственное значение. Одной из таких задач является совершенствование подходов к проектированию систем защиты информации в распределенных компьютерных сетях.

Целью настоящей работы является проведение анализа новых, перспективных подходов к проектированию систем безопасности распределенных сетей с целью выработки методологии такого анализа и рекомендаций по применению того или иного подхода.

В ходе проведения анализа необходимо учитывать обстоятельство, что целью создания систем безопасности является защита субъектов, которые участвуют в процессах информационного взаимодействия, от нанесения им существенного материального, морального, иного ущерба в результате воздействия на информационную систему со стороны злоумышленника [7–10].

В результате анализа современных тенденций развития информационных технологий могут быть выделены следующие направления совершенствования систем информационной безопасности [СБ РФ 12]:

– создание специальных защищенных операционных систем, особенно для тонких и нулевых клиентов;

– создание специальных архитектур безопасного администрирования со средствами управления безопасностью и обнаружения атак;

– развитие важнейших прикладных и фундаментальных криптографических методов.

При анализе степени защищенности распределенных компьютерных сетей необходимо учитывать, что большинство распределенных корпоративных сетей используют глобальную сеть Интернет в качестве транспортной системы. Данное обстоятельство существенно усложняет требования к построению безопасности таких сетей.

Существующие в настоящее время отечественные и зарубежные требования исходят из того, что политика безопасности рассматриваемых систем должна опираться на модели разграничения прав доступа – дискреционную и мандатную [13]. При этом в основе дискреционной модели лежат идентификаторы субъекта и объекта, а также право доступа определенного субъекта к конкретному объекту, а модели мандатного доступа – официальный допуск субъектов к информации определенного уровня конфиденциальности безотносительно пары субъект – объект.

Известно [14; 15], что в структуру политики безопасности входит множество возможных операций над объектами, а также множество разрешенных операций подмножества всего множества возможных операций. В результате проецирования основных требований политики безопасности на параметры и топологию компьютерной сети может быть получена архитектура безопасности [16; 17], представляющая план и множество принципов, описывающих службы безопасности системы для удовлетворения требований пользователя, состав элементов системы для реализации этих служб, а также необходимые уровни производительности указанных элементов системы.

В случае решения указанных задач администраторами безопасности возникает угроза ошибок администрирования либо пропуска организации защиты каких-либо функций, что приводит к выводу о необходимости применения средств автоматизации проектирования архитектур безопасности [18]. В основе автоматизированного проектирования лежат модели объекта проектирования и приемов решения проектных задач [19].

В работе [20] архитектура безопасности распределенной сети представляется в виде проекции схемы информационных потоков на семантическую сеть, в которой узлы выполняют те или иные функции защиты, а дуги – связи между ними (рис. 1).

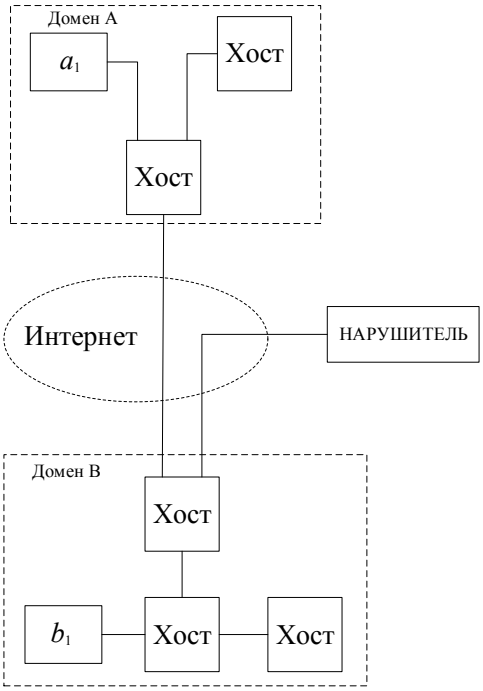

Рис. 1. Архитектура безопасности распределенной сети [20]

Предложена модель, состоящая из функциональных защитных компонент нескольких типов, связанных между собой. Данная модель (высокоуровневый аспект) представлена на рис. 2.

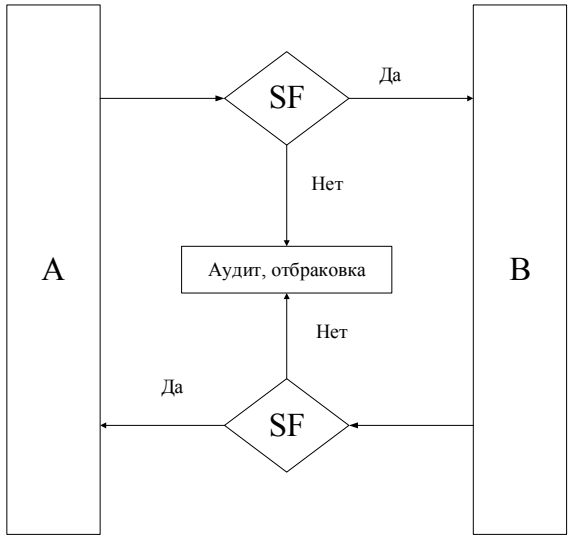

Рис. 2. Высокоуровневая модель архитектуры безопасности [20]

В приведенной на рис. 2 модели разделение функции защиты (SF) на две составляющие обусловлено возможностью передачи данных в двух направлениях. Аргументами функции защиты SF являются часть или вся порция обмена информацией. В случае успешной проверки на безопасность формируется значение функции ИСТИНА, а порция обмена передается к месту назначения, в противном случае формируется значение ЛОЖЬ – и порция обмена отбраковывается с соответствующей записью в контрольном журнале.

Управление доступом, проверка аутентичности, а также проверка целостности могут осуществляться в рассматриваемой модели на границе защищенного сетевого домена либо внутри него, однако в обоих случаях необходимо гарантировать защиту любого пути прохождения порции обмена к месту назначения в защищенном домене.

Для обеспечения аутентичности и целостности целесообразно применять криптографические протоколы с участием отправителя (например, для выработки сеансовых ключей отправитель генерирует свой ключ).

При построении математических моделей, предназначенных для исследования и построения политик безопасности в распределенных сетях, часто опираются на матричную модель [20], в которой присутствуют сеансовая и почтовая матрицы. Сеансовая матрица позволяет описать политику доступа каждой категории пользователей к различным файлам, а почтовая – определяет возможность передачи файлов между пользователями различной категории:

$$\mathbf{M} = \begin{pmatrix} M_{1,1} & M_{1,2} & \cdots & M_{1,n} \\ M_{2,1} & M_{2,2} & \cdots & M_{2,n} \\ \vdots & \vdots & M_{i,j} & \vdots \\ M_{m,1} & M_{m,2} & \cdots & M_{m,n} \end{pmatrix}, \qquad (1)$$

$$\mathbf{MT} = \begin{pmatrix} MT_{1,1} & MT_{1,2} & \cdots & MT_{1,m} \\ MT_{2,1} & MT_{2,2} & \cdots & MT_{2,m} \\ \vdots & \vdots & MT_{i,j} & \vdots \\ MT_{m,1} & MT_{m,2} & \cdots & MT_{m,m} \end{pmatrix}. \qquad (2)$$

При этом элементы указанных матриц определяются следующим образом:

$$M_{i,j} = \begin{cases} r, \text{ чтение;} \\ rw, \text{ редактирование;} \\ 0, \text{ нет доступа.} \end{cases} \qquad (3)$$

$$MT_{i,j} = \begin{cases} 1, & i\text{-й субъект может посылать данные } j\text{-му субъекту,} \\ 0, & i\text{-й субъект не может посылать данные } j\text{-му субъекту.} \end{cases} \qquad (4)$$

Следует учитывать, что множество объектов и субъектов в процессе функционирования изменяется ввиду появления или уничтожения объектов и субъектов, а также изменения их статуса (прав доступа). Поэтому и матрицы доступа также динамически меняются.

В работе [7] предложено развитие рассмотренного подхода. Указанная модель является многоуровневой, объекты могут иметь разные уровни доступа, а субъекты – степени доступа. В основе такой модели лежит теория алгебраических решеток. Для обеспечения более гибкого управления безопасностью могут применяться комбинированные модели (совокупность мандатной и дискреционной моделей), когда в дискреционной модели для контроля за информационным взаимодействием одноуровневых пользователей применяется мандатная модель, к примеру модель Белла – Лападулы [21] (рис. 3).

Рис. 3. Структура модели Белла – Лападулы

Составляющими данной модели являются множества субъектов S, объектов O и уровней защиты L, прав доступа G, а также списки текущего доступа b и запросов Z. Определяющим в задании политики безопасности является множество прав доступа, имеющее вид $G = \{r, a, w, e\}$, где признаки r, a, w, e означают, соответственно, чтение, дополнение, модификацию и исполнение иных действий. Матрица доступа $\mathbf{M} = \|M_{i,j}\|$ в данной модели не должна содержать пустых столбцов, однако ненулевое значение элемента $M_{i,j}$ не является достаточным условием разрешения доступа.

В рассматриваемой модели используются два условия защиты – простое и так называемое *-условие. При этом простое условие обеспечивает исключение прямой утечки охраняемых данных и накладывает ограничения на базовые уровни защищенных объектов, а *-условие предотвращает косвенную утечку данных, например чтение для переписи данных в объект с низшим уровнем защиты. В данной модели описываются разрешения для каждого из одиннадцати возможных видов запросов. Главным достоинством рассматриваемой модели является формализация анализа выполнения политики безопасности, что позволяет осуществлять эти действия с помощью соответствующего программного обеспечения информационной системы.

Рассмотренные модели и методы ложатся в основу методологии проектирования систем безопасности распределенных корпоративных сетей, в которых связанные между собой локальные сети являются важнейшими их составляющими.

Под проектированием архитектуры безопасности обычно понимают средства, реализующие функции защиты с необходимым набором параметров, их место в вычислительной сети и способы связи друг с другом [Cisco].

Предложенная в работе [20] методология включает следующие этапы: задание обобщенной исходной топологии защищаемой системы, локализация информационных потоков, систематизация функций защиты информации и их локализация, введение классов защищенности, построение поэтапного алгоритма проектирования архитектуры безопасности.

В связи с появлением новых угроз информационной безопасности (быстрое распространение ботнетов, постоянное усложнение сетевых атак, тревожащий рост организованной киберпреступности и шпионажа с использованием Интернета, хищение персональных и корпоративных данных, более сложные способы инсайдерских атак, развитие новых форм угроз для мобильных систем) компанией Cisco предложена своя концепция информационной безопасности Cisco Security Framework (CSF), которая определяет концепцию создания системы информационной безопасности, ориентированной на обеспечение доступности сети и сервисов и поддержание непрерывности бизнеса. Угрозы безопасности характеризуются высокой динамикой, и концепция CSF предусматривает способы выявления текущих направлений угроз, а также отслеживания новых и развивающихся угроз за счет следования лучшим практическим рекомендациям и использования комплексных решений. Новая архитектура системы безопасности Cisco использует подходы, определенные в концепции CSF, для определения продуктов и функций, позволяющих надежно обеспечить безопасность во всей сети [концепция Cisco].

Концепция CSF предполагает наличие политик безопасности, разработанных по результатам анализа угроз и рисков и согласованных с бизнес-целями и задачами. Критически важным фактором для достижения успеха бизнеса является создание таких политик безопасности, которые не только не препятствуют, а, напротив, способствуют достижению организацией

поставленных бизнес-целей и плановых показателей. Поэтому разработка политик должна начинаться с четкого определения бизнес-целей и задач. После определения этих целей необходимо выявить возможные угрозы для выделенных целей и задач. Следует иметь в виду, что цели, задачи и возможные угрозы могут сильно меняться в зависимости от организации и среды.

В заключение можно отметить, что проведенный анализ существующих подходов к проектированию систем безопасности распределенных компьютерных сетей позволяет выделить наиболее важные тенденции совершенствования методологии проектирования и применения систем безопасности. Следует, однако, иметь в виду, что методы атак корпоративных сетей также постоянно совершенствуются, и это требует разработки новых подходов к проектированию и применению систем безопасности.

Литература

1. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. – К. : Юниор, 2003. – 504 с.
2. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. – Петербург, БХВ, 2005. – 288 с.
3. Брассар Ж. Современная криптология / пер. с англ. – М. : Издательско-полиграфическая фирма ПОЛИМЕД, 1999. – 176 с.
4. Герасименко В.А. Защита информации в автоматизированных системах обработки данных : в 2 кн. – М. : Энергоатомиздат, 1994.
5. Hellman, M.E. An overview of public key cryptography // IEEE Communication Magazine. – 2002. – Iss. 50. – P. 42–49.
6. Diffie, W. and Hellman, M.E. New directions in cryptography // IEEE Trans. Inform. Theory. – 1976. – V. 22. – P. 644–654.
7. Чураев Л.А., Просихин В.П. Построение алгоритма проектирования архитектуры безопасности распределенных вычислительных систем // Проблемы информационной безопасности высшей школы. – М. : МИФИ, 2000. – С. 126–127.
8. Аносов В.Д., Зегжда П.Д., Курило А.П. Современные требования к информационной безопасности и актуальные направления разработки средств защиты // Методы и технические средства обеспечения безопасности информации. – СПб., 1995. – С. 12–16.
9. Бронников В.А., Просихин В.П. Телекоммуникации в аспекте национальной безопасности // READ.ME. – 1998. – № 10. – С. 7.
10. Першин А.Ю. Организация защиты вычислительных систем // Компьютер-пресс. – 1992. – № 10. – С. 35–50; № 11. – С. 33–42.
11. Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации. – URL: http://www.scrf.gov.ru/documents/6/94.html (дата обращения 06.06.2015).
12. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. – М. : МИФИ, 1997.
13. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. – М., 1992.
14. Клир Д. Системология. Автоматизация решения системных задач / под ред. А.И. Горлина. – М. : Радио и связь, 1990.
15. Щербаков А.Ю. К вопросу о гарантированной реализации политики безопасности в компьютерной системе // Безопасность информационных технологий. – 1997. – № 1. – С. 15–26.
16. CERT. IP Spoofing Attacks and Hijacked Terminal Connections, CA-95:01. // Computer Emergency Response Team. – Carnegie Mellon University, 1995.
17. Held, G., Hundley, K. Cisco Security Architectures // Computing McGraw-Hill, 1999.
18. Kaufman, C.W., Perlman, R., Speciner, M. Network Security. Private Communication in a Public World // Prentice-Hall, Englewood Cliffs. – New Jersey. – 1995.
19. Amoroso, E.G. Fundamentals of computer security technology // Prentice Hall, 1994.
20. Просихин В.П. Методология построения архитектуры безопасности распределенных компьютерных систем: дис. … д-ра техн. наук. – СПб., 2001. – 199 с.
21. Bell, D.T., LaPadula, L.J. Secure Computer System: Unified Exposition and Multics Interpretation // The Mitre Corp., ESD-TR-75-306. Hanscom AFB, Massachusetts, March 1976.
22. Обзор архитектуры безопасности версии 1.0. // Информационный бюллетень Cisco, 2009.