На правах рукописи

СЫЧЕВ Артем Михайлович

ОБОСНОВАНИЕ ТРЕБОВАНИЙ К МЕЖСЕТЕВЫМ ЭКРАНАМ И СИСТЕМАМ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Специальность 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Автореферат

диссертации на соискание ученой степени

кандидата технических наук

Санкт - Петербург, 2002 г.

Работа выполнена на кафедре «Информационная безопасность компьютерных систем» Санкт – Петербургского Государственного Технического Университета.

Научный руководитель: Кандидат технических наук, старший научный сотрудник
Владимир Юрьевич СКИБА

Официальные оппоненты: Доктор технических наук, профессор
Владимир Павлович Просихин

Кандидат технических наук, доцент
Николай Викторович Медведев

Ведущая организация Всероссийский научно – исследовательский институт проблем вычислительной техники и информатизации

Защита состоится 21 ноября на заседании диссертационного совета 212.229.27 в Санкт-Петербургском Государственном Техническом Университете по адресу 195251, Санкт-Петербург, ул. Политехническая, 29

С диссертационной работой можно ознакомится в Фундаментальной библиотеке Санкт-Петербургского Государственного Технического Университета

Автореферат разослан 18 октября 2002 г.

Ученый секретарь диссертационного совета 212.229.22 кандидат технических наук, профессор Платонов В. В.

АКТУАЛЬНОСТЬ. Информационная безопасность в последнее время становится все более значимой и важной сферой национальной безопасности Российской Федерации. Это обусловлено тем, что информационные системы и ресурсы стали активно использоваться в промышленности, экономике, и других сферах деятельности. В утвержденной Президентом Российской Федерации Доктрине информационной безопасности Российской Федерации выделяются четыре вида угроза информационной безопасности Российской Федерации:

– угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России.

– угрозы информационному обеспечению государственной политики Российской Федерации;

– угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных и информационных ресурсов;

– угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Данная работа посвящена совершенствованию научно-методической базы обеспечения информационной безопасности по предотвращению угроз четвертого вида.

В последнее время автоматизированные системы различного назначения создаются с использованием методов распределенной обработки информации типа Extranet и Intranet. Сложная организация сетей и использование в них как отечественных операционных систем, так и многочисленных вариантов платформ UNIX, MS-DOS, Windows, Macintosh System, NetWare, а также множество вариантов сетевых протоколов TCP/IP, VMS, MVS и т.д., приводит к значительному упрощению несанкционированного доступа (НСД) к информации.

В то же время необходимо отметить, что решение проблемы обеспечения безопасности распределенной обработки информации существенно усложняется при интеграции разнородных локальных вычислительных сетей (ЛВС) в единую систему. Это связано со сложностью решения проблемы централизованного управления доступом к разнородным ресурса АС, ошибками при проектировании сервисов TCP/IP, конфигурировании хостов, а также известными недостатками сервисов TCP/IP, широко используемых при организации удаленного доступа: SMTP, telnet, FTP, DNS, gopher, WAIS, WWW, NFS,NIS, Xwindows, r-сервисов. При этом под безопасностью информации понимается такое состояние данных, при котором невозможно их случайное или преднамеренное раскрытие, изменение или уничтожение. В этих условиях обеспечить безопасность информации возможно только при условии принятия специальных мер, и, прежде всего, осуществления контроля доступа к информационно-вычислительным ресурсам и шифрования передаваемой по линии связи информации. Однако большинство находящихся сейчас в эксплуатации операционных систем, как автономных, так и сетевых, были разработаны без учета требований по защите информации. Поэтому они оказались либо вообще незащищенными, либо средства защиты и контроля доступа в них играют роль дополнений к исходной системе. Данный вывод подтверждается многочисленными фактами успешной реализацией НСД к ресурсам интегрированных зарубежных ИВС.

Самый перспективный в этих условиях метод обеспечения безопасности распределенной обработки информации является использование межсетевых экранов.

Межсетевой экран представляет собой локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и / или выходящей из АС. Межсетевой экран обеспечивает защиту АС посредством фильтрации информации, то есть ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС на основе заданных правил, проводя, таким образом, разграничение доступа субъектов из одной ЛС к объектам другой АС. Каждое правило запрещает или разрешает передачу информации определенного вида между субъектами и объектами. Как следствие, субъекты из одной АС получают доступ только к разрешенным информационным объектам из другой АС. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола».

Следовательно, научные исследования методов, моделей и алгоритмов обоснования требований к средствам защиты информации и, в частности, к межсетевым экранам для распределенных автоматизированных систем с учетом современных методов обработки информации типа Extranet и Intranet являются **АКТУАЛЬНЫМИ** и **СВОЕВРЕМЕННЫМИ**.

Данный вывод подтверждается и анализом существующих научно-технических публикаций, посвященных обеспечению безопасности распределенной обработки информации в распределенных ИВС.

Наиболее полные теоретические исследования проблем обеспечения безопасности информации выполнены в работах Герасименко В.А. (МИФИ) и Ухлинова Л.М. В этих работах разработаны концепция защиты информации, определяющая задачи и методологию обеспечения безопасности информации в автоматизированных системах обработки данных, принципы реализации управляемых процессов обеспечения безопасности информации, а также обоснована необходимость создания отдельной подсистемы управления безопасностью информации в виде иерархической системы автоматизированных рабочих мест (АРМ) безопасности на объектах АСУ ВКС. Кроме работ Герасименко В.А. и Ухлинова Л.М, к направлению теоретических исследований можно отнести работу Быстрова И.И., в которой рассмотрены теоретические аспекты организации криптографической защиты информации, а также работы Шуракова В.В., Хоффмана Л.Дж., посвященные рассмотрению принципов построения систем защиты, методов и мероприятий по обеспечению сохранности информации в системах ее обработки. Однако разработанные методы и алгоритмы позволяют обеспечить безопасность информации только в замкнутых автоматизированных системах, не использующих для передачи информации сети общего пользования.

Кроме того, теоретические исследования методов контроля доступа к ресурсам ИВС безусловно имеют важное значение для определения общей стратегии защиты информации в создаваемой системе. Однако теоретическое описание методов контроля доступа не всегда позволяет сформулировать требования к их реализации в виде программно-аппаратных средств. Данное обстоятельство несколько ограничивает возможность использования научных работ этой группы на этапе обоснования характеристик межсетевых экранов при их проектировании.

Подавляющее большинство научных работ в области обеспечения безопасности информации содержит описание СЗИ безотносительно к условиям их применения. Наиболее полно СЗИ рассмотрены в книге одного из участников разработки международного Проекта COST-11 «Механизмы защиты вычислительных сетей» С.Мафтика. Однако авторы Проекта после его завершения вынуждены были признать, что ряд научных направлений требует более глубокой проработки. Одним из таких направлений является разработка средств фильтрации потоков и установления защищенных соединений. К этому же классу работ

могут быть отнесены диссертации Тимофеева Ю.А. (НИИ «Квант»), Казарина О.В. и Скибы В.Ю. Работы данных авторов рассматривают отдельные аспекты защиты информации в АСУ без учета необходимости решения задач управления процессами обеспечения безопасности распределенной обработки информации.

Таким образом, можно сделать вывод об отсутствии в настоящее время методов, моделей и алгоритмов обоснования требований к МЭ, применение которых позволяет повысить эффективность защиты за счет реализации научно-обоснованного управления правилами фильтрации и установления защищенных соединений при использовании современных методов распределенной обработки информации.

Данный вывод обусловил необходимость постановки и решения **НАУЧНОЙ ЗАДАЧИ** по разработке комплекса инженерно-технических методик обоснования требований к межсетевым экранам.

ЦЕЛЬЮ данной работы является уменьшение вероятности НСД при распределенной обработке информации на основе Intranet- и Extranet-технологий в глобальных корпоративных вычислительных сетях за счет применения межсетевых экранов.

ОБЪЕКТОМ ИССЛЕДОВАНИЙ данной работы являются методы распределенной обработки информации на основе Intranet- и Extranet технологий, а **ПРЕДМЕТОМ** – методы обеспечения сетевой безопасности в глобальных корпоративных вычислительных сетях при межсетевом информационном взаимодействии.

ОСНОВНЫМИ РЕЗУЛЬТАТАМИ исследований являются:

1. Методика структурно-функционального формирования межсетевого экрана на основе профиля разграничения доступа.

2. Базовая модель удаленного управления межсетевым экраном в распределенной автоматизированной системе.

3. Методика обоснования правил фильтрации и управления потоками информации.

4. Методика обоснования характеристик протокола установления защищенных соединений.

5. Практические рекомендации по созданию унифицированной технологии построения защищенной виртуальной сети на основе типовой структуры межсетевого экрана.

НАУЧНАЯ НОВИЗНА диссертации заключается в том, что предложено использовать метод структурно-функционального формирования на основе профиля разграничения доступа при межсетевом взаимодействии при формировании структуры межсетевых экранов с последующим обоснованием характеристик экрана на основе метода двухэтапной вариантной оптимизации.

НАУЧНАЯ ЗНАЧИМОСТЬ работы состоит в развитии теории обеспечения информационной безопасности в части разработки методик обоснования структур и характеристик межсетевых экранов для распределенных автоматизированных систем.

ПРАКТИЧЕСКАЯ ЗНАЧИМОСТЬ диссертации заключается в том, что разработанные методики, модели и алгоритмы позволяют уменьшить вероятность НСД в автоматизированных системах за счет учета на этапе обоснования требований к межсетевым экранам особенностей технологий распределенной обработки информации в глобальных корпоративных вычислительных сетях.

РЕАЛИЗАЦИЯ РЕЗУЛЬТАТОВ РАБОТЫ. Основные результаты работы реализованы при обосновании требований к системам защиты информации перспективных

средств автоматизации деятельности региональных подразделений Центрального банка Российской Федерации и в учебном процессе в Московском государственном техническом университете им. Н.Э. Баумана, что подтверждено соответствующими актами. Результаты работы использовались при выполнении плановых работ, на которые получены положительные отзывы Заказчика.

АПРОБАЦИЯ И ПУБЛИКАЦИЯ РЕЗУЛЬТАТОВ РАБОТЫ. Научные результаты, полученные в диссертационной работе докладывались на межведомственных и международных научно-технических конференциях, опубликованы в 10 статьях.

СТРУКТУРА И ОБЪЕМ ДИССЕРТАЦИИ. Диссертационная работа состоит из введения, четырех разделов, заключения и списка литературы. Работа изложена на 148 листах машинописного текста (включая 28 рисунков, 9 таблиц и список литературы из 62 наименований).

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ.

ПЕРВЫЙ РАЗДЕЛ содержит обоснование роли и места межсетевых экранов для обеспечения безопасности распределенной обработки информации на основе Intranet- и Extranet-технологий, анализ современных методов защиты информации, методов, моделей, алгоритмов и существующих программно-аппаратных средств защиты информации, а также методов обоснования требования к ним. На основе выводов, сделанных в результате анализа, сформулирована решаемая в диссертации научная задача.

Дано:

1. структуры S и S_i распределенной автоматизированной системы и локальной вычислительной сети объекта, входящей в состав автоматизированной системы соответственно;

2. множество J вариантов информационно-логических связей между локальными вычислительными сетями объектов, входящих в состав распределенной автоматизированной системы;

3. множество G стратегий нарушения безопасности информации в глобальных корпоративных вычислительных сетях;

4. система W показателей эффективности предотвращения несанкционированного доступа к ресурсам распределенной автоматизированной системе.

Требуется:

Разработать комплекс P методик обоснования требований к межсетевым экранам для распределенных автоматизированных систем, которые на основе учета взаимосвязи

$$W = F(S, S_i, J, G)$$

позволят обеспечить выполнение условия

$$R_{НСД}(P, W^*) \le R^*_{НСД},$$

где W^* – характеристики эффективности межсетевого экрана в заданных условиях применения с выбранным составом операций над защищаемыми ресурсами;

$R^*_{НСД}$, $R_{НСД}$ – требуемая и реально полученная вероятности несанкционированного доступа к ресурсам распределенной автоматизированной системы.

ВТОРОЙ РАЗДЕЛ посвящен разработке комплекса моделей и прикладных методик обоснования структуры МЭ. С учетом принятой модели нарушителя (Табл. 1) разработана вероятностная модель возможных исходов при реализации обобщенных функций

обеспечения безопасности распределенной обработки информации (Рис. 1, Табл. 2), которая используется в разработанных методиках и на защиту не выносится. Модель представляет собой дерево независимых событий, связанных с возникновением и предотвращением попыток НСД к защищаемым ресурсам.

Табл. 1.

Тип	Содержание попытки НСД	Класс нарушителей			
		Санк. польз.		Злоумышл.	
		Внутр.	Внеш.	Внутр.	Внеш.
1.	Несанкционированная модификация правил фильтрации информационных потоков	1.1	1.2	1.3	1.4
2.	Установка несанкционированного сеанса распределенной обработки данных	2.1, 2.2	2.3, 2.4	2.5, 2.6	2.7, 2.8
3.	Несанкционированное получение параметров защищенного сеанса распределенной обработки данных	3.1	3.2	3.3	3.4
4.	Несанкционированная передача информационных потоков	4.1 – 4.4	4.5 – 4.8	4.9 – 4.12	4.13 – 4.16
5.	Несанкционированное получение информационных потоков	5.1	5.2	5.3	5.4
6.	Несанкционированная подмена информационных потоков	6.1, 6.2	6.3, 6.4	6.5, 6.6	6.7, 6.8

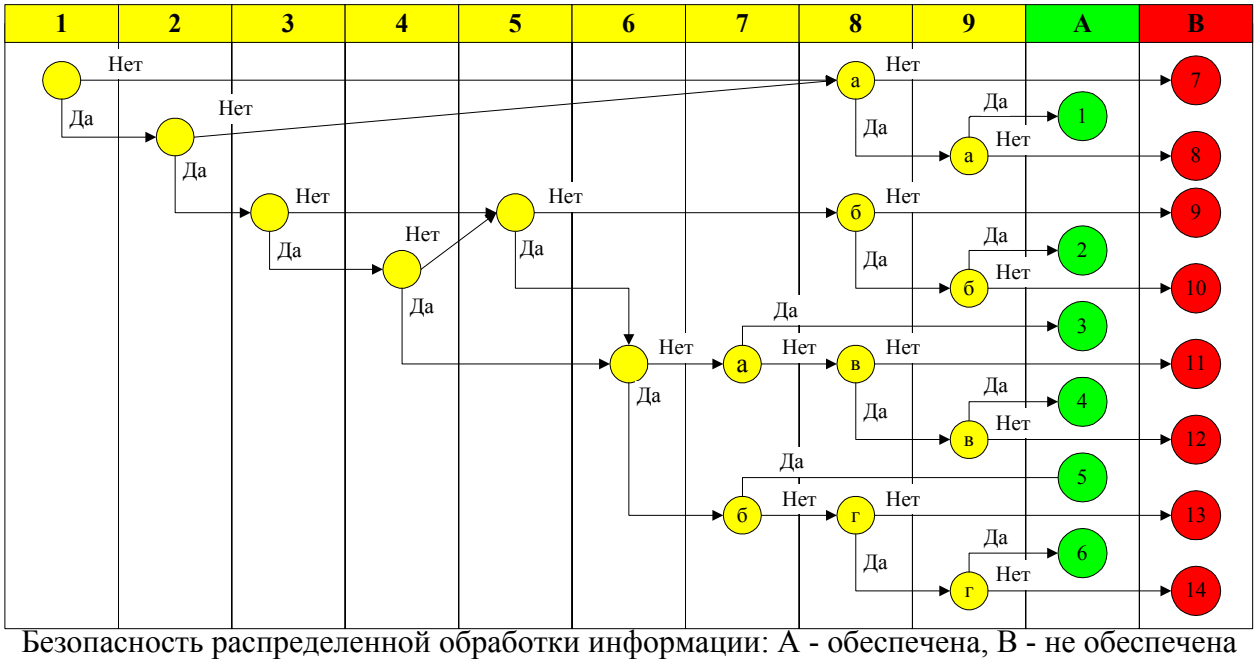

Рис. 1. Вероятностная модель обеспечения безопасности распределенной обработки информации

На основе рассмотренных моделей разработана методика обоснования требований к МЭ. Первый этап методики посвящен предварительному обследованию автоматизированной системы и необходимости применения в ней МЭ, в процессе которого составляются краткие характеристики системы с точки зрения обеспечения безопасности распределенной обработки информации. На этапе выполняется анализ состава и содержания

конфиденциальной информации, определяются и описываются объекты защиты и производится оценка уязвимости информации и потенциальных угроз осуществления НСД.

Табл. 2.

№ п/п	Функции межсетевого экрана	Класс нарушителя
1.	Предотвращение НСД на уровне формирования правил фильтрации	администратор
2.	Предотвращение попыток НСД первого типа	1.1 – 1.4
3.	Предотвращение попыток НСД 2 типа	2.2, 2.4, 2.6 и 2.8
4.	Предотвращение попыток НСД 3 типа	3.1 – 3.4
5.	Предотвращение попыток НСД 4 типа	4.4, 4.8, 4.12 и 4.16
6.	Предотвращение попыток НСД 5 типа	5.1 – 5.4
7.	Предотвращение попыток НСД 6 типа	а) 6.1, 6.3, 6.5 и 6.7; б) 6.2, 6.4, 6.6 и 6.8
8.	Обнаружение попыток НСД на уровне мониторинга и аудита распределенной обработки информации	а) 1.1 – 1.4, 2.1, 2.3, 2.5, 2.7, 4.1, 4.5, 4.9, 4.13; б) 2.2, 2.4, 2.6, 2.8, 3.1 – 3.4, 4.2 – 4.4, 4.6 – 4.8, 4.10- 4.12, 4.14 – 4.16;
9.	Локализация и ликвидация попыток НСД	в) 6.1, 6.3, 6.5 и 6.6; г) 6.2, 6.4, 6.6 и 6.8.

Вторым этапом является формулирование концептуальных положений по построению МЭ на основе обоснования требований по обеспечению безопасности распределенной обработки информации и функций и задач МЭ, а также определение принципа контроля доступа. Обоснование требований учитывает множество факторов: от целевого назначения системы до характеристик обрабатываемых данных и режимов эксплуатации технических средств. Обоснование функций и задач МЭ возможно на основе вероятностной модели решения обобщенных функций обеспечения безопасности распределенной обработки информации.

Следующим этапом методической схемы является синтез структуры МЭ, который можно разделить на следующие составляющие:

– структурно-функциональное формирование МЭ (определение оптимального состава и взаимосвязей элементов МЭ, оптимальное разбиение множества управляемых объектов на отдельные подмножества, обладающие заданными характеристиками связей и т.д.);

– синтез системы управления МЭ:

  – выбор принципов организации управления МЭ (согласование целей элементов МЭ, распределением прав и ответственности, созданием контуров принятия решений по фильтрации потоков информации и т.д.);

  – оптимальное распределение выполняемых функций между администратором безопасности и программно-аппаратными средствами МЭ;

  – выбор организационной иерархии МЭ.

Следующий этап – анализ характеристик и определение эффективности МЭ – заключается в обосновании системы показателей эффективности, характеризующих потенциальные и динамические свойства МЭ. При определении эффективности МЭ

необходимо провести оценку его характеристик и оценку защищенности ресурсов ИВС в условиях решения выбранных функций и задач обеспечения безопасности распределенной обработки информации, а также сравнить полученные оценки защищенности с требуемыми.

В случае неудовлетворительных характеристик МЭ, определяются причины и осуществляется выбор рационального варианта модификации структуры МЭ.

Последним этапом методической схемы обоснования структуры МЭ является принятие решения на разработку и реализацию МЭ с выбранной структурой.

Научная новизна методики заключается в том, что обоснование состава и взаимосвязи компонентов структуры межсетевого экрана основывается на логико-вероятностной модели предотвращения НСД к защищаемым ресурсам, научная значимость – в развитии принципов формализации процесса обоснования структур межсетевого экрана в части конкретизации условий завершения этапов проектирования, а практическая значимость заключается в том, что обеспечивается возможность прогнозирования уровня защищенности обрабатываемой в ИВС информации с учетом заданных требований к характеристикам реализации функций обеспечения безопасности распределенной обработки информации.

Структурно-функциональное формирование (СФФ) МЭ представляет собой расширенное (относительно формализованного) описание структуры МЭ и процессов ее функционирования. Под структурно-функциональным описанием МЭ понимается описание МЭ и процессов его функционирования, которое отвечает следующей совокупности условий:

1. Условие полноты, т.е. отображения всех существенно значимых элементов и атрибутов МЭ, а также их взаимосвязи.

2. Условие адекватности, т.е. обеспечения возможности воспроизведения в процессе формирования всех существенно значимых характеристик процессов функционирования МЭ.

3. Условие стандартности и унифицированности внутренней структуры элементов МЭ и взаимодействия между ними.

4. Условие модульности, т.е. автономной организации элементов, позволяющей стандартными способами объединять элементы в сложные структуры и заменять любой элемент и их совокупности.

5. Условие гибкости, т.е. практически неограниченной возможности расширения и реорганизации структуры одних компонент МЭ без изменения (или без существенного изменения) других компонент.

6. Условие прозрачности, т.е простоты изучения структурных элементов МЭ, любой их совокупности и взаимосвязей между элементами и их совокупностями.

Комплексный характер и многоплановость процесса СФФ МЭ обусловливает существенные трудности при построении и реализации комплексного критерия эффективности МЭ, в достаточной степени адекватного процессу обеспечения безопасности распределенной обработки информации. Решением этой проблемы является использование аппроксимационной схемы многоступенчатой оптимизации при соблюдении ряда условий, из которых наиболее существенным является вариантность разработки. В этом случае процесс СФФ МЭ сводится к последовательной оптимизации по иерархии подсистем, конечных целей и задач МЭ. Суть вариантного подхода при этом заключается в том, что рассматриваются все возможные структуры МЭ, связанные с выбором наилучшего проектного решения, и для каждой структуры решается задача поиска оптимального решения.

Формально процедура принятия решения по синтезу структуры МЭ представляет собой функциональное отображение, формирующее решение для последовательно расширяемого набора исходных данных (непосредственно или интерактивно) в процессе эволюционного поиска.

При СФФ МЭ рассматривается трехуровневое дерево критериев и ограничений, формируемых при выборе конкретного варианта МЭ. Это дерево связывает первый уровень – МЭ в целом – со вторым (промежуточным) уровнем, на котором располагаются различные подсистемы МЭ. В свою очередь, второй уровень связан с третьим (нижним), охватывающим отдельные элементы – программно-аппаратные средства, входящие в различные подсистемы МЭ.

Процесс СФФ МЭ проводится в два цикла. На первом цикле формируется множество вариантов МЭ и осуществляется локальная оптимизация, в рамках которой выбираются состав и структура подсистем (локально оптимальные или близкие к оптимальным варианты). Для конкретного задания функции оценки на этом этапе используются методы теории нечетких многокритериальных задач оптимизации, позволяющие определить множество Парето-оптимальных структур МЭ.

Пусть A – множество допустимых структур МЭ. Обозначим через z_1, z_2, ..., z_n целевые функции. Пусть Ω – множество мер неопределенности, адекватно отражающих неполноту информации (отсутствие сведений) об условиях функционирования МЭ. На высоких уровнях абстракции множеством Ω охватываются структурные, параметрические и режимно-эксплуатационные меры неопределенности. Множество допустимых исходов, которые могут быть получены при сочетании элементов множества действий с элементами множества мер неопределенности, может быть описано декартовым произведением A×Ω. Целевые функции при этом получают смысл отображений:

$$z_i : A \times \Omega \to R^{(1)}, i \in [1, n], Z : A \times \Omega \to R^n .$$

Рациональный принцип принятия решений S в этом случае определяется следующими условиями:

1. S (A, Ω, Z) ⊂ A, т.е. решениями могут быть лишь допустимые структуры МЭ;

2. a ∈ S (A, Ω, Z) и b ∈ A при Z (a, ω) = Z (b, ω); ∀ ω ∈ Ω ⇒ b ∈ S (A, Ω, Z), две структуры, имеющие одинаковые векторные оценки, либо обе являются, либо обе не являются решениями;

3. S (A, Ω, Z) ⊂ eff (A, Ω, Z), где множество eff (A, Ω, Z) – эффективная граница образа множества A, полученного с помощью отображения Z, и является множеством всех допустимых векторных оценок. Из этого условия следует, что лишь те структуры МЭ, которым соответствуют эффективные векторные оценки (оптимальные по Парето), представляют собой потенциально возможные решения. Определение вариантов структур МЭ, оптимальных по Парето, представляет собой классическую задачу векторной оптимизации, состоящей в определении множества:

$$\left\{ a \in A \middle| Z(a) \in eff(A, \Omega, Z) \right\};$$

4. S (A, Ω, Z) ≠ ∅, т.е. должно быть найдено, по крайней мере, одно решение;

5. если (A, Ω, Z) и (B, Ω, Z) – две ситуации принятия решений, то

$$S(A,\Omega,Z)\cap B=\begin{cases}\varnothing\\ S(B,\Omega,Z)\end{cases},$$

т.е. лучшие структуры для множества А остаются лучшими структурами для сокращенного множества В, если эти структуры нельзя исключить из рассмотрения.

На втором цикле осуществляется синтез рационального МЭ, представляющий собой формирование программно-аппаратных элементов с выбранными ранее структурами. При этом используются методы и подходы, аналогичные используемым на первом цикле, только показатели эффективности являются четкими.

Для повышения оперативности СФФ при обосновании структуры подсистем МЭ в качестве критериев (целевых функций) используются только наиболее значимые критерии эффективности обеспечения безопасности распределенной обработки информации. При обосновании состава элементов подсистем МЭ обязательным условием является использование полного множества обоснованных критериев эффективности МЭ.

Первый этап является постановочный. На данном этапе на основе анализа исходных данных и финансово-ресурсных ограничений формулируется конкретная постановка задачи СФФ и определяются критерии эффективности МЭ.

Следующий этап – структурный синтез МЭ, целью которого является формирование и локальная оптимизация структуры МЭ. Первоочередные задачи данного этапа – определение функций и задач МЭ на основе вероятностной модели исходов и обоснование вариантов структуры МЭ (выбор состава функциональных подсистем и их взаимодействия). Для каждого варианта структуры МЭ на основании введенных критериев определяются нечеткие оценки их эффективности. После этого с использованием методов многокритериальной оптимизации определяется подмножество Парето-оптимальных вариантов структур МЭ. Если в результате получилось пустое подмножество, то осуществляется возврат на постановочный этап СФФ МЭ.

Следующий этап – оптимизационный синтез МЭ, целью которого является выбор технического решения, удовлетворяющего поставленной задачи СФФ МЭ. На данном этапе на основе анализа методов, алгоритмов и программно-аппаратных средств обеспечения безопасности распределенной обработки информации определяются варианты состава элементов функциональных подсистем для каждой Парето-оптимальной структуры МЭ. Для каждого варианта на основе введенного векторного критерия определяются количественные оценки, после чего выбирается наилучший вариант. Следующая задача – проверка выполнения всех требований по обеспечению безопасности распределенной обработки информации при использовании МЭ с выбранной структурой. При неудовлетворении выполняется уточнение ограничений, допущений и исходных данных и осуществляется возврат на постановочный этап.

Последним этапом СФФ МЭ является принятие решения на разработку и реализацию МЭ с выбранной структурой программно-аппаратных средств.

Научная новизна данной методики заключается в использовании для выбора вариантов межсетевого экрана трехуровневого дерева критериев и ограничений, причем на первом этапе для задания функций оценок используются методы решения нечетких многокритериальных задач, а на втором – методы синтеза структуры по полному множеству однозначно определенных границ эффективности установления защищенных соединений и фильтрации потоков в заданных условиях реализации системы.

Практическая значимость обусловлена тем, что она позволяет использовать типовые решения по установлению защищенных соединений и управлению правилами фильтрации

информационных потоков при проектировании конкретных межсетевых экранов.

Автором модифицирована модель адаптивного управления безопасностью информации на основе эталонного поведения системы обеспечения безопасности информации за счет учета особенностей распределенной обработки информации с использованием Extranet- и Intranet-технологий. При этом выделение задач нормативного и оперативного управления элементами и параметрами МЭ позволяет более эффективно обеспечить безопасность распределенной обработки информации в условиях неопределенности места и времени попыток НСД.

Цель управления заключается в решении задачи:

$$U^*(t+\tau) = \arg\max_{U(t)\in\Delta} R^t\left[X(Q(t), U(t)), S(t+\tau)\right]$$

где τ – упреждение прогноза состояния безопасности распределенной обработки информации;

$U^*(t+\tau)$ – стратегия управления с учетом упреждения прогноза;

$R^t(.)$ – критерий эффективности в момент времени t с учетом упреждения прогноза;

$S(t+\tau)$ – прогнозируемое состояние с учетом упреждения прогноза;

Δ – ограничения на выбор стратегии управления.

Для упрощения моделирования в условиях неопределенности ряда характеристик распределенной обработки информации в модели используются элементы программного управления (планирования нормативного – базовые профили фильтрации потоков и оперативного управления – периодичность регенерации ключевых параметров и аудита межсетевого взаимодействия).

Т.о. сущность модели заключается в иерархическом представлении функций управления с элементами адаптации к условиям применения:

$$W = W <W_{по}, W_{пн}, W_о, W_н>,$$

где $W_{по}$ – оператор планирования оперативного управления МЭ: $\pi_о = W_{по}$ (X, S);

$W_о$ – оператор оперативного управления МЭ: $U_о = W_о$ (X, S, $\pi_о$);

$W_{пн}$ – оператор планирования нормативного управления МЭ: $\pi_н = W_{пн}$ (X, S, $U_о$);

$W_н$ - оператор нормативного управления МЭ: $U_н = W_н$ (X,S, $\pi_н$);

Научная новизна разработанной модели заключается в применении для управления функционированием межсетевого экрана методов адаптивного управления с эталонной моделью распределенной обработки информации. Научная значимость состоит в модификации модели адаптивного управления процессами обеспечения безопасности на основе эталонного поведения системы обеспечения безопасности информации за счет учета особенностей распределенной обработки информации с использованием Extranet- и Intranet-технологий. Практическая значимость предложенной модели обусловлена тем, что она позволяет реализовать удаленное управление системой территориально-распределенных межсетевых экранов и контролировать безопасность распределенной обработки информации.

В третьем разделе на основе анализа общих принципов обоснования требований к системам защиты информации уточнен состав системы показателей эффективности обеспечения безопасности распределенной обработки информации. Показано, что для определения значимости показателей целесообразно использовать их декомпозицию на функциональные, оперативные, экономические показатели, а также на показатели надежности и критичности. Разработан обобщенный алгоритм формирования дерева показателей для различных условий реализации МЭ.

1. Проводится анализ нормативно-технической документации по оценке защищенности информации от НСД, существующей номенклатуры показателей эффективности обеспечения безопасности распределенной обработки информации, разработанных критериев и методик оценки, а также методик контроля значений показателей эффективности на всех этапах жизненного цикла МЭ.

2. Выделяется доминирующий фактор (или доминирующие факторы) обеспечения безопасности распределенной обработки информации в данных условиях функционирования в зависимости от структуры ИВС и специфики обрабатываемой информации. Значению каждой характеристик ставится в соответствие определенный рейтинг создаваемой МЭ (высокий, средний, низкий). Каждому уровню рейтинга соответствует свой уровень сложности МЭ и ее определенные функции. Нормативное значение характеристик(и) МЭ задается в числовом выражении.

3. Определяются критерии оценки для каждой характеристики: функциональность – вероятность НСД к ресурсам, обеспечиваемый уровень и класс защищенности и т.д.; надежность – надежность работы МЭ в течении заданного времени, вероятности компрометации и восстановления ключевых параметров и т.д.; оперативность – время установления защищенного сеанса, пропускная способность, время идентификации и аутентификации пользователей и т.д.; критичность – аппаратная сложность, диагностируемость, тестируемость, взаимозаменяемость и т.д.; экономичность – стоимость разработки и эксплуатации МЭ, загрузка ИВС служебными сообщениями и т.д. На этапе формирования требований к МЭ каждый выбранный критерий оценивается весовым коэффициентом K_{ij}, где i – порядковый номер показателя эффективности, j – порядковый номер метрики.

4. Выбираются метрики для каждого критерия со своими весовыми коэффициентами M_{nk},, где n – порядковый номер критерия, а k – порядковый номер метрики.

5. Ранжируется выбранная номенклатура показателей эффективности по рейтинговым уровням эффективности МЭ (высокому, среднему, низкому) в соответствии с суммарными значениями весовых коэффициентов критериев и метрик. Производится сверка удовлетворения требований к МЭ по выбранной номенклатуре показателей эффективности и установленному заказчиком уровню.

6. Подготовка контрольного варианта состава показателей эффективности для конкретного компонента МЭ.

С учетом уточненного состава системы показателей разработаны методики обоснования характеристик протокола установления защищенных соединений и правил фильтрации информационных потоков при распределенной обработке информации.

Методика обоснования правил фильтрации информационных потоков основывается на анализе требований по обеспечению безопасности распределенной обработки информации в соответствии с руководящими документами Гостехкомиссии России с учетом специфики используемых технологий и стандартных протоколов передачи информации.

При этом основными факторами формирования правил фильтрации являются:

– уровни взаимодействия ЭМ ВОС;

– используемые сетевые протоколы передачи информации;

– структуры пакетов выбранных сетевых протоколов;

– используемая система адресации взаимодействующих абонентов и портов сетевого оборудования;

– структура сегментации защищаемой ЛВС;

– временные ограничения на работу пользователей в системе.

Научная новизна методики заключается в формировании правил фильтрации на основе анализа уровней взаимодействия в соответствии с ЭМ ВОС и сетевых протоколов, используемых при распределенной обработке информации. Научная значимость состоит в разработке методического аппарата обоснования правил фильтрации и создания типовых (базовых) профилей управления потоками при распределенной обработке информации на основе Intranet и Extranet технологий. Практическая значимость обусловлена тем, что методика позволяет генерировать структуру профиля фильтрации с учетом специфики распределенной обработки информации в системе.

Исходными данными обоснования состава и характеристик операций криптографического протокола установления защищенных соединений являются принципы построения и функционирования АС, а также финансовые и ресурсные ограничения на разработку МЭ. На основании этих данных и требуемого уровня защищенности информации определяется целесообразность введения криптографических протоколов (размер ключа, схема, ит.д.) в МЭ.

Обоснование характеристик протокола основывается на анализе условий распределенной обработки информации и учитывает всю совокупность, влияющих на безопасность передаваемых сообщений. Методика обоснования характеристик протокола представляет собой последовательность этапов, причем результат каждого этапа имеет принципиальное значение для принятия решений по составу и содержанию включаемых в протокол процедур обработки сообщений.

Исходными данными для обоснования состава и характеристик операций протокола являются специфические особенности АС и реализованных методов обработки информации, методы шифрования с требуемой криптостойкостью, структура и объем передаваемых данных, а также принципы формирования и применения ключевой информации в АС, определенные на ранних этапах выбора криптосистем.

На основе анализа исходных данных и формального описания криптопротокола выполняется первый этап методики, который объединяет выбор и обоснование типа криптосистемы, используемой в протоколе, и применяемой ключевой схемы.

Если выбор криптосистемы из множества известных и допущенных к использованию в АС влияет в основном на принципы реализации процедур шифрования (дешифрования) данных, то от обоснованности выбора ключевой схемы зависят основные функциональные характеристики протокола, например информационная избыточность сообщений, объем ключевой информации, необходимой абонентам, периодичность смены ключей, число служебных сообщений протокола и, следовательно, время установки защищенных соединений между абонентами.

На втором этапе выполняется выявление криптографических ограничений и допущений, связанных со свойствами выбранной криптосистемы. Поскольку все криптосистемы основаны на какой-либо математической задаче, имеющей прямое решение и очень сложное обратное решение, то обычно все допущения и ограничения связаны с

выбором параметров криптосистемы. Например, для метода RSA существуют ограничения на размеры модуля n, а для алгоритма DES – ограничения на методы генерации ключей и использования s-блоков. Кроме того, на этом же этапе выполняется непосредственная разработка структуры передаваемых сообщений, выявление всех допущений, связанных с последовательностью передачи и семантикой служебных сообщений.

Здесь существенное значение имеют условия применения протокола, анализ которых позволяет уточнить цель каждого допущения, выявить наиболее критичные элементы протокола и максимально упростить модификацию протокола, которая выполняется при невозможности реализации какого-либо допущения на практике.

Особое внимание на этом этапе уделяется исследованию возможности снижения стойкости используемых криптопреобразований за счет специфики протокола. Снижение стойкости может произойти, например, при шифровании одних и тех же сообщений с помощью разных ключей при условии, что содержимое этих сообщений известно нарушителю. Если обозначить через $E_j(M)$ сообщение M, зашифрованное с помощью ключа j, то при обосновании состава и характеристик операций криптографических протоколов необходимо анализировать влияние на их безопасность следующих совокупностей зашифрованных сообщений, которые, по предположению, доступны нарушителю:

1. Совокупность $\{E_j(M)\}$, где для шифрования одного и того же сообщения M используются различные ключи, особенно если они связаны между собой какой-либо зависимостью.

2. Совокупность $\{E(M_j)\}$, где для шифрования сообщений M_j, имеющих какую-либо связь друг с другом, используется один и тот же ключ.

3. Совокупность $\{E_j(M_j)\}$, где для шифрования известного множества сообщений M_j используются различные ключи. При этом особый интерес представляет случай, когда ключи также имеют некоторую зависимость друг от друга.

Третий этап посвящен разработке состава сообщений протокола, характеристик операций над сообщениями (правил их передачи), и оценке его безопасности. Следует отметить, что задача оценки безопасности криптографических протоколов является достаточно сложной научной проблемой, решение выходит за пределы данной работы. Если по результатам оценки безопасности криптопротокол не удовлетворяет предъявленным к нему требованиям (является небезопасным), то после уточнения ограничений, принятых допущений и исходных данных процесс обоснования начинается снова с первого этапа.

Четвертый этап является завершающим этапом методики проектирования криптографических протоколов, после которого следует непосредственная реализация разработанного протокола. На этом этапе проводится исследование влияния на безопасность протокола нарушения каждого из принятых допущений и ограничений. Основной подход, используемый в этих исследованиях, заключается в применении математического моделирования работы протокола с учетом существующих стратегий поведения нарушителя. Результаты исследований, проводимых на четвертом этапе, могут показать ряд ограничений, влияние которых на безопасность протокола пренебрежимо мало. В этом случае выполняется коррекция протокола за счет снятия лишних ограничений.

Научная значимость заключается в разработке математического аппарата анализа слабых мест процедуры установления защищенного соединения с использованием стандартных протоколов сетей общего пользования и своевременного учета всех потенциальных возможностей нарушения безопасности распределенной обработки информации. Практическая значимость методики обусловлена тем, что она позволяет использовать типовые решения по выбору криптографических схем и схем управления ключевой информацией для установления защищенных соединений при использовании

Intranet- и Extranet-технологий обработки информации.

В четвертом разделе на основе разработанного комплекса прикладных методик обоснованы практические рекомендации по структуре типового МЭ, типовым схемам обеспечения безопасности информации для Extranet- и Intranet-технологий. Типовая структура межсетевого экрана представляет собой совокупность функциональных подсистем объединяемых на основе программно-аппаратного экранирующего фильтрующего маршрутизатора с защищенной операционной средой.

Основными подсистемами являются:

– подсистема сетевых адаптеров в составе не менее трех сетевых адаптеров;

– подсистема конфигурирования сетевых адаптеров;

– подсистема фильтрации потоков;

– подсистема установления защищенных соединений;

– подсистема сжатия информационных потоков для защищенных соединений;

– подсистема аутентификации администратора безопасности;

– подсистемы управления и поддержки принятия решений;

– подсистема регистрации и учета выполняемых операций межсетевого взаимодействия;

– подсистема обеспечения целостности программно-информационных компонент МЭ;

– подсистема восстановления МЭ.

Реализация межсетевого экрана на основе обоснованной типовой структуры позволяет обеспечить безопасность распределенной обработки информации как с использованием Extranet-технологии, так и Intranet-технологии.

В разделе также проведен анализ результатов экспериментальных исследований эффективности применения обоснованных автором практических рекомендаций по обеспечению безопасности распределенной обработки информации.

На первом этапе проводилась оценка характеристик обеспечения безопасности распределенной обработки информации в соответствии с вероятностной моделью исходов в условиях воздействия различного рода попыток НСД. При этом в качестве варьируемых параметров были выбраны интенсивность попыток НСД к ресурсам ЛВС (количество попыток НСД в сутки); количество в ЛВС контролируемых ресурсов, пользователей, рабочих станций, межсетевых каналов связи, установленных сеансов межсетевого взаимодействия, а также относительная полнота моделей угроз.

На втором этапе оценивался эффект от применения МЭ при распределенной обработки информации при различных режимах распределенной обработки информации и вклад подсистемы обеспечения сетевой безопасности на основе МЭ в общую эффективность обеспечения безопасности информации в ИВС. Оценка производилась экспертно-расчетным путем на основе тестирования программного комплекса ЛВС с учетом известных моделей осуществления НСД к ресурсам ЛВС в условиях ее интеграции с распределенной (гибридной) ИВС общего пользования.

Анализ экспериментальных исследований показал, что применение типового МЭ, структура и характеристики которого были обоснованы с использованием разработанного комплекса прикладных методик, позволяет повысить вероятности предотвращения НСД к информации при использовании:

– Web-сервера – на 15%;

– доступа к ресурсам сети Интернет – на 41%;

– удаленного доступа пользователей к центральной базе данных – на 33%;

– корпоративной обработки информации с использованием сетей общего пользования – на 27%;

– при интегральном использовании всех режимов распределенной обработки информации – на 34%.

При этом суммарный вклад подсистемы обеспечения сетевой безопасности на основе использования МЭ в обеспечение безопасности распределенной обработки информации составляет около 23%.

ЗАКЛЮЧЕНИЕ

В диссертационной работа поставлена и решена научная задача разработка комплекса прикладных инженерно-технических методик обоснования требований к межсетевым экранам, обеспечивающих уменьшение вероятности НСД к информации при ее распределенной обработки в автоматизированных системах с использованием Intranet- и Extranet-технологий.

Полученные в процессе исследований результаты позволяют обосновать структуру и характеристики средств обеспечения безопасности распределенной обработки информации на основе применения метода двухэтапной вариантной оптимизации.

При этом разработаны:

1. Методика структурно-функционального формирования межсетевого экрана на основе профиля разграничения доступа.
2. Базовая модель удаленного управления межсетевым экраном в распределенной автоматизированной системе.
3. Методика обоснования правил фильтрации и управления потоками информации.
4. Методика обоснования характеристик протокола установления защищенных соединений.

А так же сформулированы практические рекомендации по созданию унифицированной технологии построения защищенной виртуальной сети на основе типовой структуры межсетевого экрана.

Оценка практических результатов работы показала, что решение поставленной задачи позволяет повысить вероятностно-временные характеристики обеспечения безопасность распределенной обработки информации от 15% до 40% в зависимости от используемых технологий и методов обработки, причем суммарный вклад МЭ, с обоснованной структурой и характеристиками, в обеспечение безопасности распределенной обработки информации составляет около 23%.

Достоверность полученных результатов обеспечивалась обоснованным выбором исходных данных, основных допущений и ограничений, использованных при проведении экспериментов, а также применением современного, апробированного математического аппарата моделирования сложных технических систем.

Таким образом, все поставленные в работе частные задачи решены в полном объеме и цель диссертационной работы достигнута

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИОННОЙ РАБОТЫ

1. Скиба В.Ю., Сычев А.М. Методическая схема обоснования структуры межсетевого экрана // Межрегиональная конференция «Информационная безопасность регионов

России» («ИБРР-99»), г. С. Петербург, 13-15 октября 1999 г.: Тезисы конференции. Часть 1 – СПб., с. 77 – 78.

2. Скиба В.Ю., Сычев А.М. О проблеме обеспечения собственной безопасность межсетевых экранов // Межрегиональная конференция «Информационная безопасность регионов России» («ИБРР-99»), г. С. Петербург, 13-15 октября 1999 г.: Тезисы конференции. Часть 1 – СПб., с. 77 – 78.
3. Скиба В.Ю., Сычев А.М. Структурно-функциональное формирование межсетевого экрана // Тезисы конференции «Информационная безопасность», г. Москва, МИФИ, 20-21 января 2000 г.
4. Сычев А.М. Анализ возможных исходов при реализации обобщенных функций обеспечения безопасности распределенной обработки информации // Сборник трудов научно-практической конференции «Информационная безопасность», г. Таганрог, 6 – 8 июня 2001 г.
5. Сычев А.М. Использование межсетевого экрана Checkpoint Firewall-1 в схеме защиты сегмента сети Главного управления безопасности и защиты информации Банка России (опыт внедрения) // Методы и технические средства обеспечения безопасности информации: тезисы докладов. г. С. Петербург, СПбГТУ, 2001 г.
6. Сычев А.М. Основные подсистемы, составляющие типовую структуру межсетевого экрана // Методы и технические средства обеспечения безопасности информации: тезисы докладов. г. С. Петербург, СПбГТУ, 2001 г.
7. Сычев А.М. Подсистемы типовой структуру межсетевого экрана //II Межрегиональная конференция «Информационная безопасность регионов России» г. С. Петербург, 2001 г.
8. Сычев А.М. Анализ подсистем обобщенной структуры межсетевого экрана //II Межрегиональная конференция «Информационная безопасность регионов России» г. С. Петербург, 2001 г.
9. Сычев А.М. Опыт внедрения CheckPoint Firewall-1 в ГУБ БР //II Межрегиональная конференция «Информационная безопасность регионов России» г. С. Петербург, 2001 г.
10. Сычев А.М. Оценка эффективности защиты информации в распределенной автоматизированной системе при межсетевом взаимодействии // Проблемы информационной безопасности. Компьютерные системы № 3 г. С. Петербург, 2001 г.