На правах рукописи

УДК 004.056.53

Гхаиад Иссам

МЕТОДИКА ПРОЕКТИРОВАНИЯ И АДМИНИСТРИРОВАНИЯ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ ЗАЩИТЫ ДОСТУПА К ДАННЫМ

Специальность 05.13.17 - Теоретические основы информатики

АВТОРЕФЕРАТ

диссертации на соискание учёной степени

кандидата технических наук

Москва 2007

Работа выполнена в Московском государственном техническом университете им. Н.Э. Баумана.

Научный руководитель:	- доктор технических наук, профессор В. М. Черненький
Официальные оппоненты:	- доктор технических наук, профессор С. В. Дворянкин
	- кандидат технических наук, старший научный сотрудник С. П. Остриков
Ведущая организация:	ОАО, "Научно-исследовательский институт средств автоматизации"

Защита диссертации состоится в « __ » января 2008 года в ___ часов на заседании специализированного совета Д. 212.141.10 в Московском государственном техническом университете им. Н.Э. Баумана по адресу:
105005, г. Москва, 2-я Бауманская ул., д. 5.

С диссертацией можно ознакомиться в библиотеке Московского государственного технического университета им. Н.Э. Баумана.

Отзыв на автореферат, заверенный печатью организации, просим присылать по адресу:

105005, г. Москва, 2-я Бауманская ул., д. 5, МГТУ Н.Э. Баумана,
Учёному секретарю диссертационного совета Д. 212.141.10.

Автореферат разослан « __ » декабря 2007 года.

Ученый секретарь
диссертационного совета
кандидат технических наук, доцент _____ С. Р. Иванов

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Проблемы защиты информации в настоящее время занимают одно из ведущих мест в перечне важнейших проблем в областях развития и применения информационных технологий. Обзор литературы показал наличие широкого спектра требований к обеспечению защиты данных. Они касаются обеспечения конфиденциальности, целостности, авторизации, разграничения доступа, стоимости и других аспектов понятия защиты информации. Вместе с тем анализ показал, что многие из этих требований тесно связаны с решением проблемы защиты доступа к данным в целом. Так, например, обеспеченность защиты данных решает проблемы конфиденциальности, целостности, стоимости и др. Отмечается, что политика управления доступом является основным механизмом защиты, непосредственно обеспечивающим конфиденциальность и целостность обрабатываемой информации. Для решения проблемы доступа к данным используются разнообразные подходы: использование математических методов криптографии, применение паролей различных типов, организационные меры, биометрические методы и др. В то же время в целом ряде источников отмечается необходимость выполнения по крайней мере двух принципов организации защиты данных:

- принцип многоуровневой защиты - предписывает не полагаться на один защитный рубеж, каким бы надёжным он ни казался. Эшелонированная оборона способна, по крайней мере, задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий;
- принцип разнообразия защитных средств - рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками преодоления системы защиты информации.

Вместе с тем, обзор литературы показал явную недостаточность подходов к организации комплексной системы защиты доступа к данным, отсутствие теоретических разработок по проектированию и сопровождению системы защиты в целом. При всем многообразии методов и подходов к защите данных практически отсутствуют методы оптимального распределения защиты по элементам данных, что позволило бы широко использовать уже разработанные методы защиты, объединив их в оптимальный комплекс при защите каждого данного. Это дало бы возможность гибко организовать защиту для каждого типа данных, обеспечить повышенную защищенность и при необходимости существенно снизить стоимость системы защиты. Таким образом, тема диссертационной работы, посвященной разработке нового метода организации защиты доступа к данным, опирающегося на сформулированные выше принципы, актуальна.

Целью исследования является разработка методики проектирования и администрирования распределенной защиты доступа к данным.

Решаемые задачи. Для достижения указанной цели необходимо решить следующие задачи:

1. Произвести анализ методов защиты доступа к данным и политики их реализации
2. Определить объекты защиты;
3. Сформировать модели объекта защиты и его параметров;
4. Формализовать операции преобразования входных и выходных параметров моделей;
5. Определить способ задания параметров моделей;
6. Разработать способ распределения методов защиты по объектам защиты;
7. Определить критерии качества распределения методов защиты;
8. Разработать методику проектирования защиты данных;
9. Разработать методику администрирования защиты данных.

Предметом исследования являются методы обеспечения безопасности доступа к данным для решения задач администратора системы безопасности в целом.

Методы исследований. Для решения поставленных задач в работе используются методы теории алгебр, системного анализа, теории вероятности, математической статики, теории графов, теории нечётких множеств, аппарат лингвистических переменных, программирование.

Научная новизна. В диссертации получены следующие результаты, характеризующиеся научной новизной:

1. Метод распределенной защиты, определяющий путь доступа к данным и обеспечивающий защиту доступа к этим данным на каждом шаге пути доступа.

2. Способ оценки качества распределения методов защиты по всей совокупности мегаданных.

Практическая ценность работы заключается в разработке:

1. Методики проектирования распределенной защиты доступа к данным;

2. Методики администрирования процесса сопровождения и эксплуатации системы защиты доступа к данным;

3. Комплекса программных средств поддержки методики проектирования и эксплуатации распределенной защиты доступа к данным.

Внедрение результатов работы.

1. Теоретические положения диссертации использованы при разработке программных систем компании НПО “Эшелон”.

2. Методика проектирования и администрирования распределенной системы защиты доступа к данным использована в Российском Государственном Военно-Историческом архиве.

3. Результаты работы использованы в учебном курсе “Защита информации” кафедры ИУ-5 МГТУ им. Н.Э. Баумана.

4. Теоретические положение и методика проектирования и администрирования распределенной системы защиты доступа к данным использованы в НИР НИИИСУ МГТУ им. Н.Э. Баумана.

Апробация работы. Содержание отдельных разделов и диссертации в целом было доложено:

1. На семинарах и заседаниях кафедры “Системы обработки информации и управления” МГТУ им. Н.Э. Баумана;

2. На международной научно-технической конференции “По вопросам обучения с применением технологий e-learning”, Москва, октября 2007.

Публикации. По теме диссертации опубликовано две статьи и тезисы доклада.

Структура и объём работы. Диссертация состоит из введения, четырех глав, заключения, списка литературы и приложений, содержащих листинг разработанных программ. Объём диссертации составляет 142 страницы, в том числе 133 страниц текста. Работа включает 39 рисунка и 34 таблицы. Список литературы содержит 53 наименования.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы диссертации, ее практическое значение, формулируются основные цели исследования, основные положения, изложена структура диссертации.

В первой главе проведен аналитический обзор методов защиты в информационных системах, который показал, что в большинстве случаев предлагается защитить все данные теми или иными организационными или математическими методами. При всем многообразии методов и подходов к защите данных практически отсутствуют методы оптимального распределения защиты по элементам данных, что позволило бы широко использовать уже разработанные методы защиты, объединив их в оптимальный комплекс при защите каждого данного. Это дало бы возможность гибко организовать защиту для каждого типа данных, обеспечить повышенную защищенность и при необходимости существенно снизить стоимость системы защиты. В главе сформулированы задачи исследования.

Во второй главе разрабатывается метод распределенной защиты, когда защищаются не только сами данные, но весь путь доступа к информации с применением разнообразных методов защиты на каждом шаге этого пути. Данное совместно с описанием пути доступа к нему называется мегаданным.

Базовые понятия метода распределенной защиты

Рассмотрим связь двух отношений A и B. Взаимосвязь этих отношений представлена на рис. 1 в виде направленного графа (в дальнейшем будем называть его *цепочкой*). Будем называть вершину A *исходной*, а вершину B *искомой* информацией, а саму цепочку - базовой.

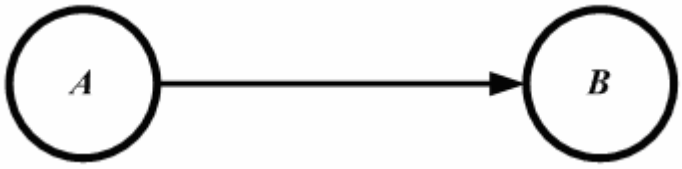


Рис. 1. Базовая цепочка

Для дальнейшего рассмотрения будем капсулу $K(A)$ вершины A характеризовать как:

$$K(A) = \langle M(A), R(A), S(A), P(A) \rangle,$$

где:

$M(A)$ – метод защиты;

$R(A)$ – способ его реализации;

$S(A)$ – стоимость реализации метода;

$P(A)$ – вероятность несанкционированного преодоления защиты, обеспеченной методом $M(A)$.

Будем называть $P(A)$ *мерой опасности вершины.*

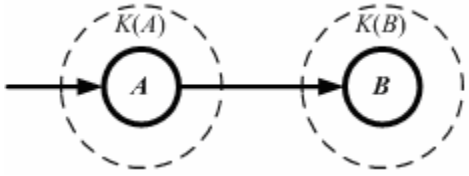


Рис. 2. Капсулирование цепочки

В предположении, что $M(A)$ и $M(B)$, соответствующие капсулам $K(A)$ и $K(B)$, независимы и не связаны между собой, *меру опасности цепочки*, приведенной на рис. 2, можно вычислить, как:

$$P(A,B)=P(A)\times P(B),$$

Добавим в состав цепочки *ключевые* вершины. На рис. 3 приведен пример цепочки, содержащей исходную вершину A, искомую вершину B и две ключевые вершины C и D.

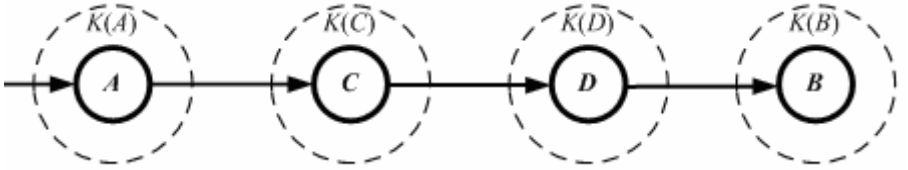


Рис. 3. Цепочка с ключевыми вершинами

Мера опасности получения информации в A и B одновременно по цепочке A,C,D,B равна:

$$P(A,C,D,B)=P(A)\times P(C)\times P(D)\times P(B)\,,$$

Учет коррелированности методов защиты в цепочке

Для оценки коррелированности методов $M(A)$ и $M(B)$ введем понятие *показателя связности* $W(A,B)$, принимающего значение на $[0,1]$. Этот показатель определяет связность метода защиты вершины B с методом защиты вершины A и показывает, насколько упрощается преодоление защиты вершины B, если вершина A уже преодолена. Будем предполагать, что большее значение показателя связности соответствует большей степени коррелированности. Так, значение $W=0$ соответствует полному отсутствию связности методов, в то время как значение $W=1$ соответствует полному сходству методов.

Введем понятие *действительной меры опасности* $P(A)_{\text{ДЕЙСТ}}$ преодоления капсулы $K(A)$ после преодоления капсулы $K(A_1)$ в виде:

$$P(A)_{\text{ДЕЙСТ}}=P(A)^{(1-W(A_1,A))},$$

Такое определение меры опасности для двух связанных вершин позволяет получить теоретически корректные значения в двух крайних точках: $W=0$ и $W=1$ (рис. 4). Так, при $W=0$ мера опасности вершины: $P(A)_{\text{ДЕЙСТ}}=P(A)$. При значении $W=1$ мы имеем эквивалентные (полносвязанные) методы защиты вершин A и A_1, и при преодолении защиты вершины A_1 мы получаем автома-

тически прямой доступ к вершине A: она оказывается полностью незащищенной с мерой опасности, равной 1.

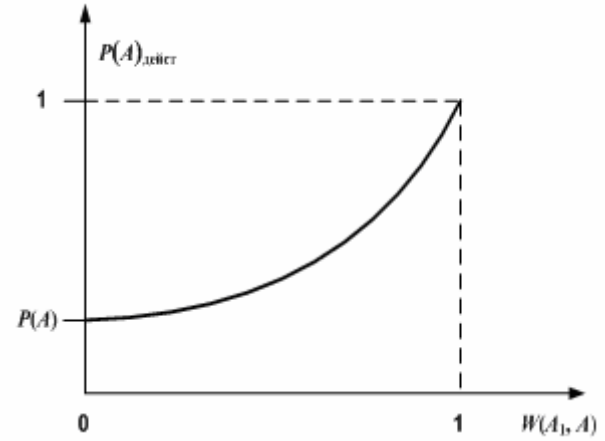


Рис. 4. Влияние показателя связности на меру опасности

Аналогичные рассуждения можно провести для цепочки. Рассмотрим цепочку, изображенную на рис. 2. Меру опасности цепочки равна:

$$P(A,B)=P(A)\times P(B)_{\text{ДЕЙСТ}};$$

Таким образом: $P(A,B)=P(A)\times P(B)^{(1-W(A,B))}$,

Рассмотрим цепочку из 3-х вершин, приведенную на рис. 5. Здесь показаны информационные вершины A, B, C капсулы $K(A), K(B), K(C)$, а также меры связности методов защиты в капсулах $W(A, B), W(B, C), W(A, C)$. Если преодолены капсулы $K(A)$ и $K(B)$, то можно преодолеть капсулу $K(C)$, используя опыт преодоления метода $M(A)$ капсулы $K(A)$, или используя опыт преодоления метода $M(B)$ капсулы $K(B)$.

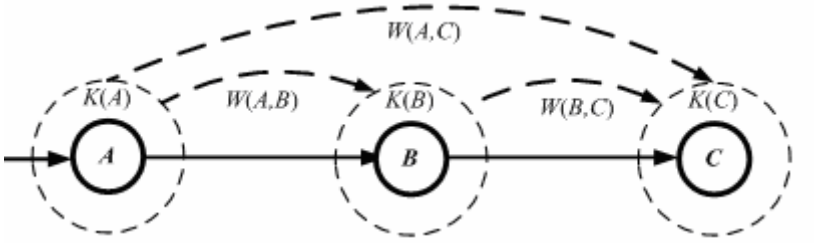


Рис. 5. Пример цепочки из 3-х вершин

Для вершины C введем понятие *эквивалентного показателя связности* $W(C)_{\text{ЭКВ}}$ в виде следующей свертки:

$$W(C)_{\text{ЭКВ}}=1-((1-W(A, C))\times(1-W(B, C))),$$

Вывод этой формулы представляет собой вероятностную интерпретацию введенных ранее понятий: поскольку W - есть показатель *связности*, значение которой лежит в интервале $(0, 1)$, то выражение $(1-W)$ можно рассматривать, как показатель *несвязности*.

Произведение показателей несвязности $(1-W(A, C))\times(1-W(B, C))$ можно интерпретировать как показатель *одновременной* несвязности по обоим показателям.

Тогда $W_{\text{ЭКВ}}$, являющееся дополнением одновременной несвязности до 1, можно интерпретировать, как показатель *любого* варианта связности.

Выполним краткое исследование свойств предлагаемой свертки:

а) пусть любой из показателей связности ($W(B,C)$или $W(A,C)$) равна 1. Тогда $W_{\text{ЭКВ}}=1$. Этот результат соответствует представлению о том, что эквивалентная связность тоже равна 1.

б) пусть один из показателей связности, например $W(A, C)$, равен 0. Тогда $W_{\text{ЭКВ}}=W(B, C)$. Этот результат соответствует представлению о том, что если метод $M(C)$ независим от $M(A)$ то его зависимости определяются лишь зависимостью от $M(B)$.

в) пусть оба показателя связности равны 0. Тогда $W_{\text{ЭКВ}}=0$. Этот результат соответствует представлению о том, что если метод $M(C)$ независим от $M(A)$ и $M(B)$, то он должен рассматриваться как совершенно независимый.

Таким образом действительная мера опасности вершины C равна:

$$P(C)_{\text{ДЕЙСТ}}=P(C)^{(1-W(C)_{\text{ЭКВ}})};$$

Подставляя, получим:

$$P(C)_{\text{ДЕЙСТ}}=P(C)^{(1-W(A,C))\times(1-W(B,C))},$$

В терминах введенных понятий (рис. 5) мера опасности цепочки (A, B) равна: $P(A, B)=P(A)\times P(B)_{\text{ДЕЙСТ}}$, где $P(B)_{\text{ДЕЙСТ}}=P(B)^{(1-W(A,B))}$.

Мера опасности цепочки (A, B, C) равна:

$$P(A, B, C)=P(A, B)\times P(C)_{\text{ДЕЙСТ}},$$

Подставляя, получим:

$$P(A, B, C)=P(A)\times P(B)_{\text{ДЕЙСТ}}\times P(C)_{\text{ДЕЙСТ}};$$

Подставляя, получим:

$$P(A, B, C)=P(A)\times P(B)^{(1-W(A,B))}\times P(C)^{(1-W(A,C))\times(1-W(B,C))},$$

Транзитивный эквивалентный показатель связности

На рис. 6 изображена вершина Z, которая связана по методу защиты с вершинами $X_1,...,X_n$, входящими в состав одной цепочки. Рассуждая аналогично вышеизложенному, *эквивалентный показателя связности* для вершины Z равен:

$$W(Z)_{\text{ЭКВ}}=1-\prod_{i=1}^{n}(1-W(X_i, Z)),$$

Таким образом, мера опасности вершины $K(Z)$ равна

$$P(Z)_{\text{ДЕЙСТ}}=P(Z)^{\prod_{i=1}^{n}(1-W(X_i, Z))},$$

Если вершины $X_1,...,X_n, Z$ входят в состав *одной цепочки* и $X_1,...,X_n$ предшествуют Z, то величину $W(Z)_{\text{ЭКВ}}$ назовем *транзитивным эквивалентным показателем связности* и обозначать как:

$$W(Z)_{\text{ЭКВ, ТРАНЗ}}=1-((1-W(X_1, Z))\times(1-W(X_2, Z))\times...\times(1-W(X_n, Z))),$$

Утверждение А: *Использование в одной цепочке одинаковых методов защиты не увеличивает меру защищенности цепочки.* Утверждение доказано в диссертации.

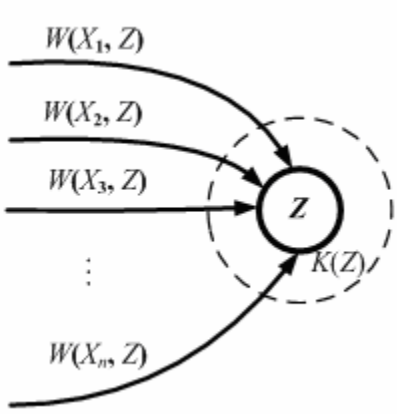


Рис. 6. Общий случай связности вершины цепочки

Отношение ситуативного замыкания

Пусть система включает n цепочек: $Q_1, Q_2, , ..., Q_n$. Пусть оказался преодоленным метод $M(Z)$ вершины Z в одной из цепочек (рис. 7). Если мы к отношению транзитивного замыкания на какой-либо цепочке добавим связи от вершины Z ко всем вершинам этой цепочки, то полученное отношение назовем *отношением ситуативного замыкания*.

Утверждение Б: *Если какая-либо вершина произвольной цепочки в результате некоторого отношения ситуативного замыкания оказывается связанной с вершинами, защищенными эквивалентными методами, то мера опасности вершины определяется связью только с одним из этих методов.* Утверждение доказано в диссертации.

Теорема: *В случае вскрытия метода $M(Z)$ вершины Z в системе защиты, расчет меры опасности каждой цепочки может быть произведен по схеме расчета транзитивного эквивалентного показателя связности путем помещения в начало цепочки дополнительной вершины с методом защиты $M(Z)$ и исключением при этом из цепочки вершины с методом защиты, эквивалентным $M(Z)$, если такая имеется. Мера опасности вновь введенной вершины полагается равной* 1. Теорема доказана в диссертации.

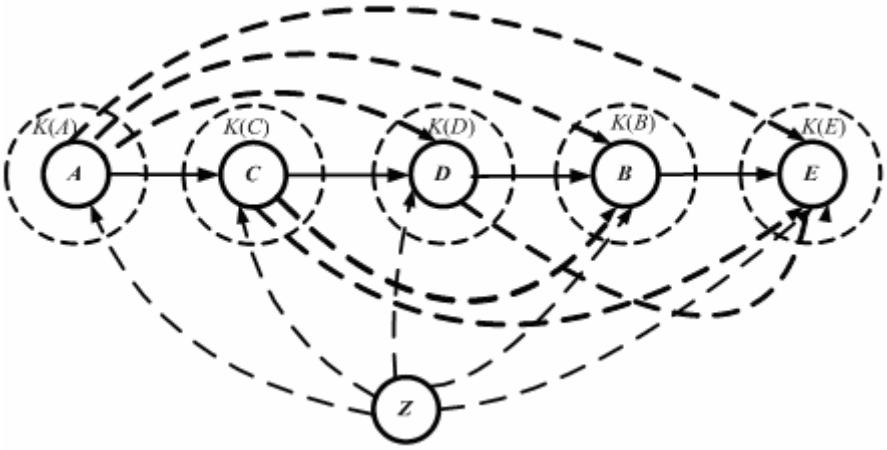


Рис. 7. Отношение ситуативного замыкания

Оценка распределения методов по совокупности цепочек

Рассмотрим цепочку $Q=\langle A_1, A_2, ... A_i, ..., A_k \rangle$, и методы защиты вершин теми же индексами $M_1, M_2, ..., M_i, ..., M_k$. Оценкой влияния метода в системе защиты заданной цепочки будем считать *уменьшение меры опасности, сопровождаемое включением данного метода по сравнению с его отсутствием.* Пусть мы оцениваем влияние метода M_i в цепочке Q. Тогда:

$$P(Q)=P(A_1)_{\text{ДЕЙСТ}} \times P(A_2)_{\text{ДЕЙСТ}} \times ... \times P(A_i)_{\text{ДЕЙСТ}} \times ... \times P(A_k)_{\text{ДЕЙСТ}},$$

Если исключить метод M_i из защиты цепочки Q, то получим новую меру опасности цепочки Q:

$$P(Q/M_i) = P(A_1)_{\text{ДЕЙСТ}} \times P(A_2)_{\text{ДЕЙСТ}} \times ... \times P(A_{i-1})_{\text{ДЕЙСТ}} \times$$
$$P^1(A_{i+1})_{\text{ДЕЙСТ}} \times ... \times P^1(A_k)_{\text{ДЕЙСТ}},$$

Разницу между полученными мерами опасности цепочки назовем *мерой влияния метода M_i в цепочке Q* и обозначим как $\Delta(M_i, Q)$.

$$\Delta(M_i, Q)=P(Q/M_i)-P(Q),$$

Выполняя подобные действия для всех методов цепочки Q, получим меры влияния методов $M_1, M_2, ..., M_i, ..., M_k$ в цепочке Q:

$$\Delta(M_1, Q), \Delta(M_2, Q), ..., \Delta(M_i, Q), ..., \Delta(M_k, Q),$$

Пусть в системе защиты в целом используется m методов. Определим пространство с координатами $M_1, M_2, ..., M_m$. Значением осей координат определим меры влияния методов. Назовем такое пространство *пространством мер влияния методов*.

Тогда каждой цепочке Q в этом пространстве можно поставить в соответствие вектор $\vec{\Delta}(Q)$ - *вектором мер влияния методов* на защиту цепочки Q:

$$\vec{\Delta}(Q)=\langle \Delta(M_1, Q), \Delta(M_2, Q), ..., \Delta(M_m, Q) \rangle,$$

Если какой-либо метод не используется в защите данной цепочки, то его мера влияния полагается равной 0. Произведем нормализацию полученных векторов. Для этого вычислим норму N вектора $\vec{\Delta}(Q)$:

$$N(\vec{\Delta}(Q)) = \sqrt{\sum_{i=1}^{m} (\Delta(M_i, Q))^2},$$

Каждую меру влияния разделим на норму:

$$K(M_i, Q) = (\Delta(M_i, Q)) / N(\vec{\Delta}(Q)),$$

Величину $K(M_i, Q)$ назовем *коэффициентом влияния* метода M_i в цепочке Q. Нормализованные таким образом вектора мер влияния назовем *векторами коэффициентов влияния*.

Поскольку норма этих векторов равна 1, то мы получаем возможность сравнивать влияние метода на любую цепочку. Вычислим по каждому методу среднеарифметическую величину:

$$r(M_i) = \left(\sum_{\forall Q} k(M_i, Q) \right) / n,$$

где n – количество цепочек в системе защиты.

Величину $r(M_i)$ назовем *средневзвешенным коэффициентом влияния* метода M_i в системе защиты. *Предлагается в качестве интегрального критерия распределения методов защиты по всем цепочкам системы принять величину*:

$$K = \max_{\forall i}(r(M_i)),$$

Выбор величины K в качестве интегрального критерия позволяет определить метод, влияние которого наибольшее во всей системе защиты. При таком взгляде самым оптимальным распределением методов было бы такое, когда влияние всех методов было бы одинаковым.

Таким образом, *стратегия распределения сводится к минимизации критерия* K. Если мы имеем V вариантов распределения методов защиты по системе в целом, то наилучшим вариантом $V_{\text{ОПТ}}$ будет тот, который соответствует минимальному K:

$$V_{\text{ОПТ}} = \min_{\forall v \in V}\left\{\max_{\forall i}(r_v(Mi))\right\},$$

где r_v - средневзвешенные коэффициенты влияния методов защиты в v - том варианте распределения.

Использование понятия нечеткой лингвистической переменной для определения параметров методов защиты

В соответствии с результатами, полученными в главе 2, необходимо определить значения следующих величин:

- показатель связности методов защиты W;
- показатель мер опасности методов защиты P;
- показатель стоимости методов защиты S;
- показатель допустимой опасности мегаданных B.

Определим лингвистическую переменную, принимающую одно из возможных значений (“очень очень”, “очень”, “не очень”, “не очень очень”). Такой подход допустим, если учитывать ранее обоснованные требования настоящей методики. Для данных показателей, учитывающих различные параметры защиты, определены терм-множества соответствующих лингвистических переменных и функции принадлежности, построенные на основе экспертных оценок, а также составлены решений для определения уровня значения показателя (“очень очень”, “очень”, “не очень”, “не очень очень”) по наличию и совокупности их функциональных параметров.

Используемые идентичные лингвистические оценки одних и тех же функциональных параметров выбора комплекса методов защиты отличаются своим семантическим содержанием в силу отсутствия унифицированной шкалы измерения даже у специалистов одной предметной области.

Получаем таким образом значение показателей в качестве базовых лингвистических критериев лингвистической переменной в соответствие с допустимой опасности.

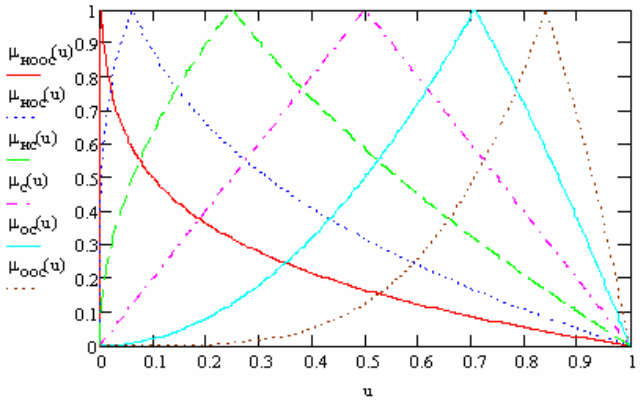
В таблице 1 показаны правила расчета функций принадлежности, соответствующих определенным значениям показателя связности W.

Таблица 1

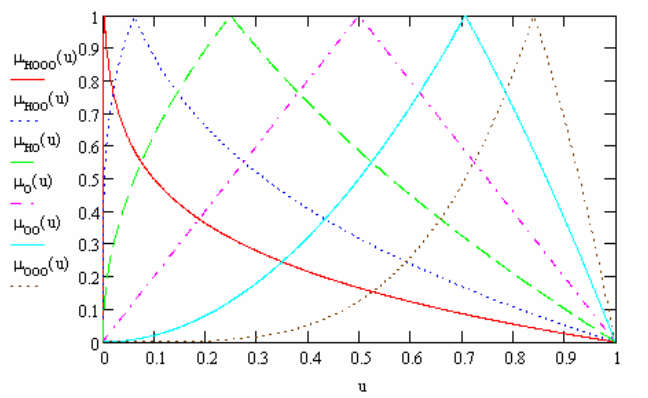
Правила расчета ФП значениям показателя связности W

Квантификатор	ФП ($u \in U$)
Не очень очень связные (ноос)	$\mu_{\text{ноос}}(u) = \mu_{\text{нос}}\left(\sqrt{u}\right),\ u \in [0,1]$
Не очень связные (нос)	$\mu_{\text{нос}}(u) = \mu_{\text{нс}}\left(\sqrt{u}\right),\ u \in [0,1]$
Не связные (нс)	$\mu_{\text{нс}}(u) = \mu_{\text{с}}\left(\sqrt{u}\right),\ u \in [0,1]$
Связные (с)	u
Очень связные (ос)	$\mu_{\text{ос}}(u) = \mu_{\text{с}}\left(u^2\right),\ u \in [0,1]$
Очень очень связные (ооос)	$\mu_{\text{ооос}}(u) = \mu_{\text{ос}}\left(u^2\right),\ u \in [0,1]$

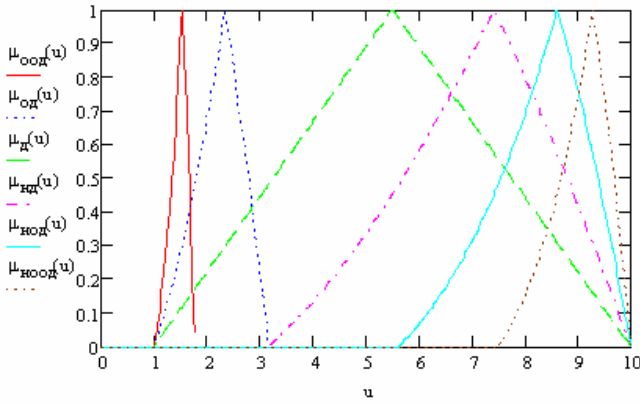
На рис. 8, приведены ФП термов ЛК показателей.



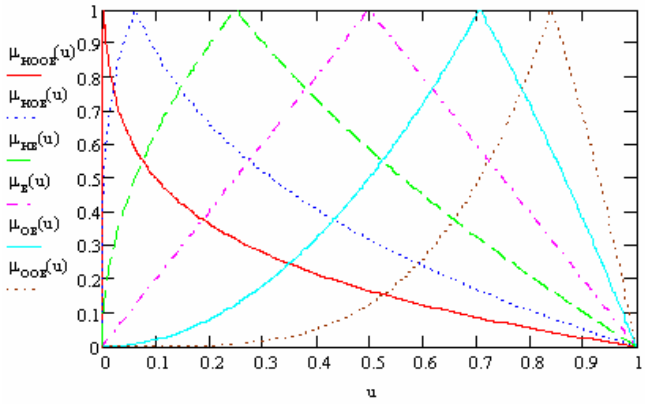
(а) ФП термов ЛП «связность W»



(б) ФП термов ЛК «опасность P»



(в) ФП термов ЛК «стоимость S»



(г) ФП термов ЛК «доп. опасность B»

Рис. 8

Методика проектирования системы защиты доступа к данным

В работе предлагается методика создания системы защиты, опирающаяся на полученные теоретические результаты. На рис. 9 приведена схема методики проектирования защиты заданной совокупности данных. Для определенности в методике необходимая совокупность данных определяется через описание бизнес-процессов предприятия. Выделенные данные рассматриваются как мега-данные и к ним прилагаются вышеизложенные методы анализа и преобразования распределений методов защиты.

В результате реализации методики получаем оптимальный вариант распределения методов защиты по цепочкам всех мегаданных. При этом мы используем понятие транзитивного эквивалентного показателя связности методов управления доступом.

Методика эксплуатации и сопровождения системы защиты доступа к данным Администратор безопасности в ходе эксплуатации информационной системы имеет возможность контролировать степень защищенности каждого данного в ходе обнаружения угроз безопасности или противоправных действий. При этом алгоритм его действий соответствует приведенной методике с той лишь разницей, что при подсчете всех характеристик используется ситуационный эквивалентный показатель связности методов защиты.

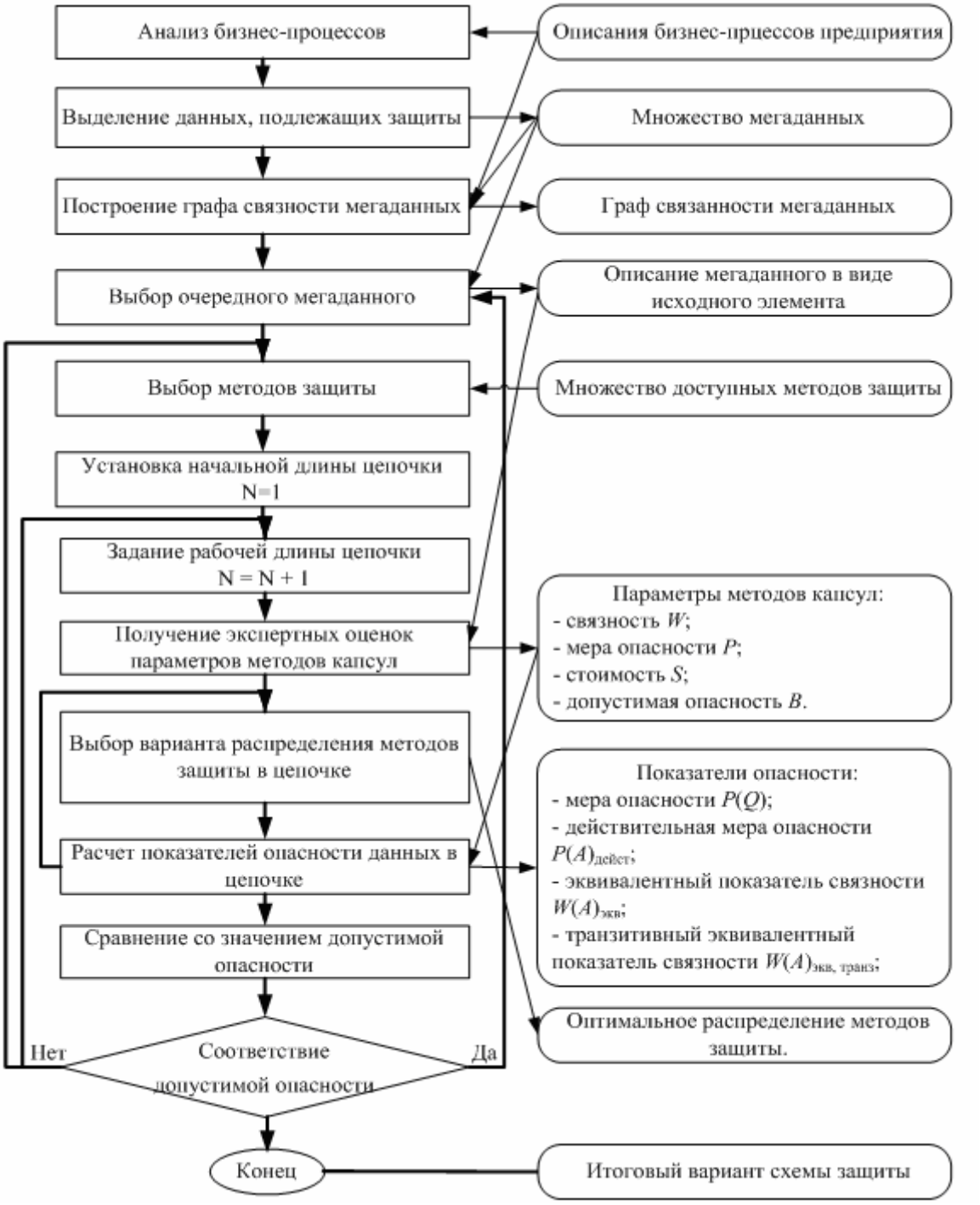


Рис. 9. Блок-схема методики проектирования системы защиты данных

В третьей главе описан комплекс алгоритмов и программ, обеспечивающий реализацию методики проектирования системы защиты данных, изложенной в главе 2. Структура комплекса приведена на рис. 10. Комплекс включает следующие алгоритмы:

1. Алгоритм выбора очередной цепочки;
2. Алгоритм формирования очередного распределения в цепочке;
3. Алгоритм расчета меры опасности цепочки;
4. Алгоритм поиска оптимального распределения методов защиты в цепочке;
5. Алгоритм расчета матрицы мер влияния методов защиты в цепочке $\Delta(M_i, Q)$;
6. Алгоритм расчета норм вектора мер влияния методов защиты в цепочке $N\left(\vec{\Delta}(Q)\right) = \sqrt{\sum_{i=1}^{m} \left(\Delta(M_i, Q)\right)^2}$;
7. Алгоритм расчета коэффициентов влияния методов защиты в цепочке $K(M_i, Q) = \left(\Delta(M_i, Q)\right) / N\left(\vec{\Delta}(Q)\right)$;
8. Алгоритм определения критериев качества распределения методов защиты в системе в целом $r(M_i) = \left(\sum_{\forall Q} k(M_i, Q) \right) / n$.

Формализованное описание задач комплекса

- Задано множество цепочек $Q = \{Q_1, ..., Q_n\}$;
- Задан состав каждой цепочки $Q_i = \left\langle A^i{}_1, A^i{}_2, ..., A^i{}_{j(i)} \right\rangle$, где $A^i{}_d$ - вершина цепочки i;
- Задано множество методов защиты вершин $M = \langle M_1, M_2, ..., M_m \rangle$;
- Заданы показатели связности методов защиты;
- Заданы меры опасности методов защиты.

Комплекс решает следующие задачи:

Задача 1. Для каждой цепочки Q_i требуется найти отображение:

$$F_i : Q_i \to M \text{, минимизирующее } P(Q_i);$$

где: $P(Q_i)$ - Мера опасности цепочки Q_i.

Задача 2. Вычислить промежуточный и интегральный критерии качества распределения методов защиты по всем цепочкам системы в целом.

Задача 3. Предоставить средства коррекции распределения методов защиты по каждой цепочке в соответствии с предпочтениями администратора.

В четвертой главе представлены результаты практического применения методики проектирования системы защиты на примере доступа к информационным ресурсам крупного архивного учреждения.

На основе результатов практического применения разработанной методики проводится проверка ее основных положений и эффективности предложенных алгоритмов по защите доступа к данным. В таблице 2 представлен перечень документов, подлежащих защите.

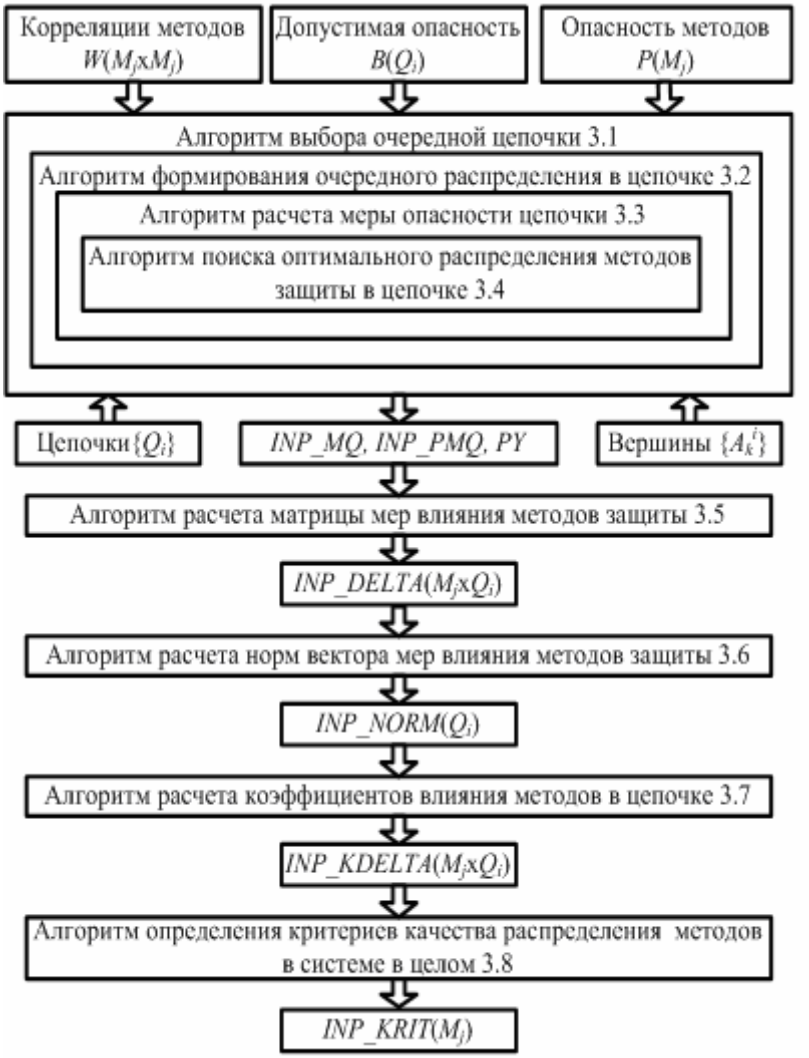


Рис. 10. Схема структуры комплекса алгоритмов поддержки методики проектирования систем защиты доступа к данным

Таблица 2

Индекс док.	Описание документа	Мегаданные
D_1	Списочный состав войсковых подразделений	Q_1
D_2	Личные данные командного состава	Q_2
D_3	Приказы, распоряжения, команды	Q_3
D_4	Подготовка и проведение военных операций	Q_4
D_5	Документы служебного пользования (данные о потерях, испытаниях оружия)	Q_5
D_6	Секретные документы (разведка, контрразведка)	Q_6
D_7	Документы особой важности (документы верховного командования, спецоперации)	Q_7

На основании анализа принятых на предприятии процессов доступа к документам (бизнес - процессов доступа), была построена схема взаимодействия мегаданных между собой и проектируемой системы защиты доступа (рис. 11).

где: БП - бюро пропусков; СД - пункт проверки служебных документов; КПП1, КПП2 - контрольно - пропускной пункт.

В соответствии с методикой получения экспертных оценок необходимых параметров (опасности методов защиты $P(M)$, цепочки Q_i и максимально допустимой опасности $B(Q)$ - таблица 4; корреляция методов $W(M \times M)$ - таблица 4), были получены оценки этих параметров.

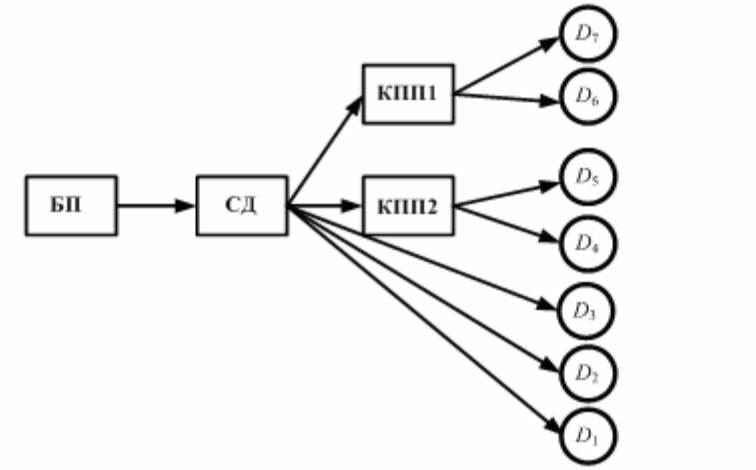


Рис. 11. Схема организации доступа к данным

Таблица 3

метод	Название метода	$P(M)$	Цеп.	$B(Q)$
M_1	Пропуск	0,4	Q_1	0,2
M_2	Паспорт	0,3	Q_2	0,15
M_3	Служебный документ	0,37	Q_3	0,1
M_4	Пароль	0,6	Q_4	0,09
M_5	Паспорт со служебным документом	0,2	Q_5	0,08
M_6	Отпечаток пальца обычный	0,04	Q_6	0,006
M_7	Отпечаток пальца инфракрасный	0,02	Q_7	0,004

Таблица 4

$W(M \times M)$	M_1	M_2	M_3	M_4	M_5	M_6	M_7
M_1	1	0,15	0,2	0,5	0,1	0,01	0,01
M_2	0,25	1	0,45	0,6	0.7	0,05	0,05
M_3	0,1	0,2	1	0,6	0.4	0,05	0,05
M_4	0,05	0,05	0,1	1	0,03	0	0
M_5	0,4	1	1	0,8	1	0,1	0,1
M_6	0,9	0,7	0,8	0,95	0,5	1	0,4
M_7	0,95	0,8	0,85	0,95	0,5	0,9	1

Расчет параметров цепочек

С помощью комплекса программ распределения и расчета параметров получен рациональный вариант распределения методов защиты по цепочкам всех мегаданных. (таблица 5).

Таблица 5

Цепочка	A_1	A_2	A_3	A_4	$P(Q)$	$B(Q)$
Q_1	M_1	M_3			0,1805	0,2
Q_2	M_1	M_2			0,1437	0,15
Q_3	M_1	M_5			0,0939	0,1
Q_4	M_1	M_5	M_4		0,0892	0,09
Q_5	M_1	M_3	M_2	M_4	0,0764	0,08
Q_6	M_1	M_5	M_6		0,0053	0,006
Q_7	M_1	M_5	M_7		0,0028	0,004

По результатам получаем критерий качества распределения методов защиты в системе в целом (рис. 12).

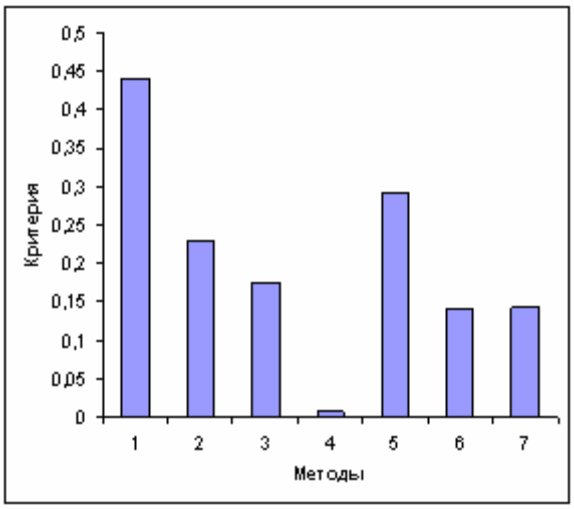


Рис. 12. Критерии качества распределения методов в системе в целом

Видно что, наибольший коэффициент влияния у первого метода M_1, в то время, как метод M_4 имеет наименьший коэффициент влияния.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

1. Разработана новая методика проектирования и администрирования распределенной системы защиты доступа к данным, позволяющей управлять как процессом проектирования системы защиты, так и ходом ее эксплуатации. Предложенная методика основывается на принципе создания системы распределенной защиты для каждого типа данных. При этом доступ к данным каждого типа определяется преодолением последовательности защищенных данных и ключевых отношений, называемых мегаданными.

2. Разработаны теоретические основы создания защиты мегаданного, а именно:

- определена формальная структура мегаданного в виде однонаправленного линейного графа, называемого цепочкой;
- введено понятие защитной капсулы, обеспечивающей защиту одной вершины цепочки, и включающей метод защиты, способ его реализации, стоимость реализации метода, меру опасности метода, допустимую меру опасности вершины, меру опасности цепочки;
- введено понятие показателя связности методов, определяющее степень коррелированности методов по подходу и реализации защиты вершины. Предложены аналитические зависимости определения влияния показателей связности методов вершин цепочки на меру опасности конкретной вершины. Доказано, что действительная мера опасности любой вершины цепочки может быть определена, как свертка транзитивного замыкания отношения связности методов по цепочке. Для многосвязных вершин введено понятие эквивалентной меры связности и получено его

математическое выражение на основе вероятностной интерпретации меры опасности;

- определено отношение ситуативного замыкания, позволяющее определить взаимодействие методов защиты между различными цепочками. Доказана теорема о построении транзитивного замыкания, эквивалентного ситуативному, позволяющая построить эффективный алгоритм оценки новой опасности для каждой цепочки в случае, когда злоумышленником преодолен какой-то метод защиты где-либо в системе.

3. Предложены показатели качества распределения методов защиты по всей совокупности цепочек на основе построения пространства нормированных векторов мер влияния методов на защиту каждой цепочки.

4. На основании полученных результатов и теоретических выводов предложены методика проектирования и администрирования распределенной системы защиты доступа к данным и методика эксплуатации и сопровождения этой системы.

5. Разработан комплекс алгоритмов, реализующий методику проектирования и администрирования распределенной системы защиты доступа к данным. Комплекс алгоритмов реализован по последовательно-вложенной схеме, что обеспечивает модульность, гибкость в реализации функций и широкий диапазон применения в ходе реализации как методики проектирования системы защиты, так и методики администрирования.

6. Эффективность предложенной в диссертации методики проектирования и администрирования распределенной системы защиты доступа к данным и работоспособность программного комплекса поддержки методики проектирования продемонстрированы на примере проектирования системы защиты доступа к информационным ресурсам крупного архивного учреждения. В результате их применения удалось получить оптимальные варианты распределения методов защиты и оперативно произвести их коррекцию с учетом пожеланий администрации и принятой в учреждении схемой допуска, получив варианты, незначительно отличающиеся от оптимальных.

7. Теоретические положение, алгоритмы, программы и методика проектирования и администрирования распределенной системы защиты доступа к данным использованы при разработке программных систем компании НПО “Эшелон”, в учебном курсе “Защита информации” кафедры ИУ-5 МГТУ им. Н.Э. Баумана, в НИР НИИИСУ МГТУ им. Н.Э. Баумана.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Гхаиад Иссам Показатели информационной безопасности предприятии //Сборник статей /Под ред. В.М. Черненького. - 2006. - № 5. - С.112-121.

2. Гхаиад Иссам, Черненький В.М. Методика администрирования защиты доступа к данным в АСУП //Вестник МГТУ. Приборостроение. - 2007.- № 4. - С. 60-69.

3. Гхаиад Иссам, Теоретические основы метода распределенной защиты данных //По вопросам обучения с применением технологий e-learning: Материалы международной конференции - Москва, 2007. - С. 125-127.