На правах рукописи

Лысенко Александр Георгиевич

ЯЗЫК ОПИСАНИЯ РИСКОВ ДЛЯ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Специальность:

05.13.19 — Методы и системы защиты информации, информационная безопасность

Автореферат диссертации на соискание ученой степени

кандидата технических наук

Санкт-Петербург — 2008

Работа выполнена в Государственном образовательном учреждении высшего профессионального образования "Санкт-Петербургский государственный политехнический университет"

Научный руководитель:

кандидат технических наук, доцент
Корт Семён Станиславович

Официальные оппоненты: Мирончиков Евгений Тимофеевич
доктор технических наук, профессор

Шишкин Владимир Михайлович
кандидат технических наук, с.н.с.

Ведущая организация:

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Защита состоится "___" _____ 2008 г. в ____ часов
на заседании диссертационного совета Д 212.229.27
ГОУ ВПО "Санкт-Петербургский государственный политехнический университет"
195251, Санкт-Петербург, ул. Политехническая, 29, корп. __, ауд. _____

С диссертацией можно ознакомиться в фундаментальной библиотеке
ГОУ ВПО "Санкт-Петербургский государственный политехнический университет"

Автореферат разослан "___" _____ 2008 г.

Ученый секретарь
диссертационного совета Платонов В.В.

Общая характеристика работы

Актуальность. В настоящее время обеспечение безопасности информационных систем является одним из приоритетных направлений развития сетевой инфраструктуры организаций. Ввиду усложнения информационных систем, увеличения числа угроз возникает потребность в оценке безопасности систем.

Согласно ГОСТ 17799 оценка безопасности – систематический анализ вероятного ущерба, наносимого бизнесу в результате нарушений информационной безопасности, с учетом возможных последствий от потери конфиденциальности, целостности или доступности информации или других активов или вероятности наступления такого нарушения с учетом существующих угроз и уязвимостей, а также внедренных мероприятий по управлению информационной безопасностью. Оценка рисков нарушения безопасности является одной из важнейших составляющих процесса управления безопасностью (ГОСТ 15408).

Модернизация информационных систем с одной стороны, является необходимым условием развития сетевой инфраструктуры, с другой – сопряжено с появлением новых угроз информационной безопасности, необходимостью в разработке и оценке влияния новых средств защиты информации на снижение риска информационной системы. Особенно остро эта проблема стоит при внесении в информационную систему мобильного сегмента, так как возникают новые угрозы, нехарактерные для фиксированного сегмента.

Для анализа безопасности необходима разработка подхода, который позволит оценить как риски информационной системы с учетом множества атрибутов, так и влияние средств защиты на снижение общего риска системы.

В диссертационной работе предлагается подход к оценке рисков нарушения безопасности с использованием языка описания рисков. Подход реализован в методике, которая позволяет производить оценку рисков нарушения безопасности системы с учетом множества атрибутов.

Диссертационная работа опирается на исследования таких отечественных и зарубежных ученых, как А.А. Грушо, А.А.Малюк, С.А. Петренко, Л. Хоффман, Ф. Кломан и др.

Целью работы является оценка рисков нарушения безопасности информационной системы с использованием языка описания рисков.

Для достижения поставленной цели в работе решались следующие задачи:

1. Разработка и реализация логического языка описания рисков нарушения безопасности для составления формальной спецификации информационной системы, угроз и средств защиты.

2. Разработка подхода к оценке рисков нарушения безопасности с использованием языка описания рисков.

3. Разработка методики оценки рисков нарушения безопасности, учитывающей множества атрибутов на базе предложенного языка, позволяющей сравнивать средства защиты, оценивать последствия реализации угроз.

Объектом исследования являются информационные системы.

Предметом исследования являются методы оценки рисков информационной безопасности.

Методы исследования. Для решения поставленных задач использовались системный анализ, методы экспертной оценки рисков, теория нечетких множеств, методы логического моделирования.

Научная новизна диссертационной работы состоит в следующем:

1. Разработан и реализован логический язык описания рисков нарушения безопасности системы, который позволяет выполнять оценку рисков нарушения безопасности с учетом множества атрибутов.

2. Предложен подход к оценке рисков нарушения безопасности, обладающий полнотой и непротиворечивостью. Подход включает оценку рисков нарушения безопасности информационных систем, обоснование выбора средств защиты, учет последствий реализации угроз с использованием языка описания рисков нарушения безопасности.

3. Разработана методика оценки рисков нарушения безопасности на основе разработанного языка, позволяющая производить оценку рисков информационных систем, оценку вклада средств защиты в снижение риска нарушения безопасности системы.

Практическая ценность работы определяется возможностью использования полученных результатов для проведения оценки рисков нарушения безопасности. Предложенная методика оценки рисков с использованием языка описания рисков нарушения безопасности и логического моделирования рисков, позволяет решать следующие задачи:

1. Составлять формальное описание информационной системы с учетом требований по безопасности, угроз и средств защиты.

2. Производить оценку рисков нарушения безопасности информационных систем с учетом различных атрибутов.

3. Учитывать последствия воздействия угроз на ресурсы информационных систем.

4. Обосновывать выбор средств защиты в информационных системах.

Практическая ценность и новизна работы подтверждаются двумя актами внедрения: от ЗАО "СПбРЦЗИ" (результаты использованы при разработке методик вычисления безопасности информационных систем), от кафедры "Информатика и информационная безопасность" ПГУПС (результаты применены в учебном процессе кафедры).

Апробация работы. Основные теоретические и практические результаты работы обсуждались на 9-й международной научно-практической конференции "Информационная безопасность - 2007", на 15-й и 16-й конференции "Методы и технические средства обеспечения безопасности информации", на 5-й Санкт-Петербургской межрегиональной конференции "Информационная безопасность регионов России".

Публикации. По теме диссертации опубликовано 10 работ.

Основные положения, выносимые на защиту.

1. Логический язык описания рисков нарушения безопасности, позволяющий сравнивать средства защиты и учитывать последствия реализации угроз.

2. Подход к оценке рисков нарушения безопасности и оценке влияния средств защиты на снижение рисков в информационной системе на основе языка описания рисков.

3. Методика оценки рисков нарушения безопасности информационной системы на основе языка описания рисков нарушения безопасности, которая позволяет оценить риски системы и влияние средств защиты на снижение риска системы.

Объем и структура. Диссертация состоит из введения, четырех глав, заключения и списка литературы.

Содержание работы

Во введении обоснована актуальность темы диссертационной работы, определены цели, задачи, объект и предмет исследования, сформулирована на-

учная новизна результатов и их практическая значимость, указаны применяемые методы, описана структура диссертации.

В первой главе проведен сравнительный анализ методов оценки рисков нарушения информационной безопасности и программных средств, реализующих методики оценки рисков нарушения безопасности. Сформулирована задача разработки подхода к оценке рисков нарушения безопасности с использованием формального описания спецификации системы и логического моделирования рисков нарушения безопасности.

Анализ различных методов оценки рисков нарушения безопасности показал, что большинство из них основывается на большом объеме предварительно собранных статистических данных, сбор которых не всегда представляется возможным. Наличие неполных или неточных данных о поведении системы в прошлом или сложность прогнозирования поведения в будущем затрудняет использование существующих методик оценки рисков нарушения безопасности и оценки влияния средств защиты на снижение риска системы. При применении новых средств защиты риск нарушения безопасности изменяется ввиду изменения вероятности воздействия угроз на ресурсы. Однако, помимо требований к средствам защиты, по отношению к системе могут быть определены различные требования по безопасности, которые также следует учитывать при оценке риска нарушения безопасности.

В настоящей работе под риском нарушения безопасности понимается вероятность нанесения ущерба информационной системе.

В модели системы защиты с полным перекрытием Клементса (рис. 1) риск R определяется по формуле:

$$R = \sum_{i=1}^{N} \{P(T_i) * W(T_i)\}, \qquad (1)$$

где $P(T_i)$ - вероятность реализации угрозы T_i, $W(T_i)$ – ущерб, нанесенный в результате реализации угрозы T_i, N – число угроз.

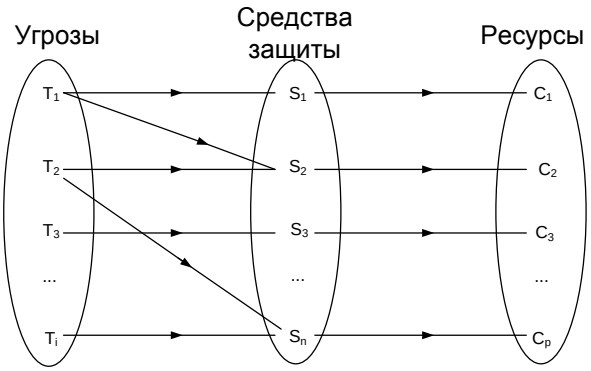

Рис. 1. Классическая модель системы защиты с полным перекрытием Клементса

В работе предлагается подход к оценке рисков нарушения безопасности, представляющий собой комбинацию метода оценки рисков нарушения безопасности, основанного на модели системы защиты с полным перекрытием, обладающей полнотой и непротиворечивостью, и экспертного метода, сочетающего в себе возможность формального описания системы и позволяющего использовать новые атрибуты. В качестве атрибутов могут выступать типы ресурсов, стоимость ресурсов, типы угроз, функции средств защиты.

В работе предлагается расширение модели Клементса путем добавления множества новых атрибутов. С учетом расширения модели, формула (1) может быть представлена в следующем виде:

$$R = F(C, T, S), \qquad (2)$$

где F – функция, задаваемая с использованием правил нечеткой логики; C – множество ресурсов, $C_j = \{c_{j1}, \ldots, c_{jx}\}$, c_{jx} – атрибут ресурса C_j (тип ресурса, стоимость ресурса); T - множество угроз, $T = \{t_{k1}, \ldots, t_{ky}\}$, t_{ky} – атрибут угрозы T_k (тип угрозы, вероятность реализации); S – множество средств защиты, $S = \{s_{m1}, \ldots, s_{mz}\}$, s_{mz} – атрибут средства защиты (тип средства защиты, список угроз, от которых защищает, список функций защиты).

Для реализации предложенного подхода к оценке рисков нарушения безопасности информационных систем с учетом множества атрибутов требуется разработка языка, который позволит задавать формальное описание системы, угроз, требований по безопасности и средств защиты.

Во второй главе приведен результат анализа языков описания безопасности информационной системы, рассмотрен логический язык описания рисков нарушения безопасности, угроз, средств защиты.

С целью выбора основы для языка были проанализированы наиболее

распространенные языки, используемые при описании безопасности систем. При этом было выделено три класса языков: языки формальной проверки спецификации системы (PVS, ACL2), языки разработки систем на базе UML и языки описания политик безопасности.

На основании анализа были сформулированы требования к языку описания рисков:

1. Иметь математический аппарат, учитывающий различные атрибуты системы при оценке рисков нарушения безопасности.
2. Поддерживать формальное описание и выводы.
3. Обладать универсальностью по отношению к информационным системам, то есть задавать описание системы на уровне субъектов и объектов.
4. Поддерживать нечеткую логику ввиду неоднозначности описания системы.
5. Позволять производить оценку рисков нарушения безопасности информационных системы.

Отправной точкой для разработки языка описания рисков послужил язык описания политик безопасности, позволяющего задать описание информационной системы в виде системы логических термов и правил при помощи языка логического программирования Prolog. С учетом сформулированных требований, на основе языка описания политик безопасности был разработан язык описания рисков нарушения безопасности.

В современной организации даже приближенная оценка стоимости информации, конкретного актива или финансовых потерь в случае нарушения безопасности является нетривиальной задачей. Поэтому при неоднозначности в описании системы целесообразно использовать нечеткую логику, при которой исходные данные задаются интервалом, характеризующим достоверность соответствующего значения.

Аппарат разработанного языка базируется на ряде задаваемых и вычисляемых переменных, таких, как вероятность воздействия угрозы, риск нарушения безопасности, термов, определяющих объекты и субъекты системы, средства защиты. На базе термов определены правила логического вывода, в соответствии с которыми производится оценка рисков нарушения безопасности.

Для поддержки нечеткой логики при оценке рисков нарушения безопасности, введены нечеткие переменные, некоторые из которых приведены в табл. 1.

Таблица.1. Примеры нечетких переменных

№	Название	Тип переменной	Описание
1	intention	Определяемая	Вероятность воздействия
2	objectCost	Определяемая	Стоимость объекта
3	valueLim	Определяемая	Предельно допустимый риск нарушения безопасности
4	risk	Вычисляемая	Риск нарушения безопасности системы
5	intruderQual	Определяемая	Квалификация нарушителя
6	userType	Определяемая	Тип пользователя

На этих переменных определяются предикаты, задающие описание системы, ее среды, описания угроз, средств защиты. На базе предикатов определяются правила логического вывода.

На логическом языке FuzzyProlog определяются термы и правила языка описания рисков нарушения безопасности, часть из которых представлена в табл. 2 и 3.

Таблица 2. Примеры термов языка

№	Терм	Аргументы
1	Определение объекта *object*	*(+objectName, +objectType, +[threat$_1$(intention),…, threat$_n$(intention), +[indirectThreat$_1$(intention),…, indirectThreat $_n$(intention)], +objectCost)* Первый аргумент – объект, второй – тип, третий – список прямых угроз, четвертый – список косвенных угроз, пятый – стоимость объекта
2	Определение типа объекта *objectType*	*(+objectType)* Аргумент – тип объекта
3	Определение пользователя *user*	*(+userName, +userType)* Первый аргумент – имя пользователя, второй – тип пользователя
4	Определение типа пользователя *userType*	*(+userType, +informationCategory)* Первый аргумент – тип пользователя, второй – категория информации
5	Определение угрозы *threat*	*(+threatName, +threatType)* Первый аргумент – название угрозы, второй – тип угрозы
6	Определение типа угрозы *threatType*	*(+threatType)* Аргумент – тип угрозы
7	Определение средства защиты *newSecurityItem*	*(+secItem, +secFunctions[])* Первый аргумент – средство защиты, второй аргумент – список функций защиты
8	Определение функции защиты *secFunction*	*(+secFunction, +objectType, +threats[])* Первый аргумент – функция защиты, второй – объект, третий – список угроз
9	Определение требования по безопасности *requirement*	*(+reqName, +objectType, +threat, +limit)* Первый аргумент – требование по безопасности, второй аргумент – тип объекта, третий – угроза, четвертый – предельно-допустимая вероятность воздействия угрозы на тип объекта

Таблица 3. Примеры правил языка

№	Правило	Аргументы

1	Вычисление риска нарушения безопасности для объекта *calcThreats* Правило выполняет оценку рисков нарушения безопасности с использованием алгоритма нечеткого логического вывода Мамдани	*(+object, -risk)* Входной аргумент – ресурс, выходной – риск объекта
2	Вычисление риска нарушения безопасности для с учетом прямых угроз объекта *calcDirectThreats*	*(+object, -riskDirectThreats)* Входной аргумент – ресурс, выходной – риск с учетом прямых угроз для объекта
3	Вычисление риска нарушения безопасности с учетом косвенных угроз для объекта *calcIndirectThreats*	*(+object, - riskInDirectThreats)* Входной аргумент – ресурс, выходной – риск с учетом косвенных угроз для объекта
4	Вычисление суммарного риска нарушения безопасности *calcAll*	*(-risk*) Выходной аргумент – риск нарушения безопасности системы
5	Выполнение требований по безопасности *acceptRequirement*	*(+secItem, +reqName)* Первый аргумент – средство защиты, второй – требование по безопасности
6	Выполнение всех требований по безопасности *acceptAllRequirements*	*(+secItem)* Аргумент – средство защиты
7	Принадлежность функции защиты средству защиты *inSecItem*	*(+secItem, +secFunction)* Первый аргумент – средство защиты, второй – функция защиты
8	Анализ рисков нарушения безопасности *riskAnalize*	*(+criticalValue)* Аргумент – критическое значение, при превышении которого предикат примет значение ЛОЖЬ

Разработанный с учетом рассмотренных требований логический язык описания рисков нарушения безопасности задается как система логических термов и правил при помощи языка логического программирования FuzzyProlog, поддерживает определение и вычисление нечетких переменных.

В качестве алгоритма нечеткого логического вывода использовался алгоритм Мамдани:

1. Этап фазификации: определяются степени истинности, т.е. значения функций принадлежности для левых частей каждого правила. Для базы правил с m правилами, определяющими зависимость риск от атрибутов информационной системы обозначим степени истинности как $A_{ik}(x_k)$, i=1..m, k=1..n, $B_i(y)$ - функция принадлежности для правой части правил.

2. Этап нечеткого вывода. Сначала определяются уровни "отсечения" для левой части каждого из правил: $\alpha_i = \min(A_{ik}(x_k))$. Далее находятся усеченные функции принадлежности: $B_i^*(y) = \min_i(\alpha_i, B_i(y))$.

3. Этап композиции. Происходит объединение полученных усеченных функций, для чего используется максимальная композиция нечетких множеств: $MF(y) = \max_i (B_i^*(y))$, где MF(y) – функция принадлежности итогового нечеткого множества.

4. Этап дефазификации (приведения к четкости) с использованием метода среднего центра: $MF(y) = \max_i (B_i^*(y))$. Выполняется определение зависимости вероятности ущерба от вероятности воздействия угроз.

Язык описания рисков нарушения безопасности информационной системы позволяет:

- составить формальное описание системы, требований к функциям и средствам защиты;
- задать отношения между множеством угроз, средств защиты, рисков нарушения безопасности;
- проверить описание на полноту и непротиворечивость;

С использованием языка появляется возможность оценить риски нарушения безопасности с учетом различных атрибутов, оценить влияние средств защиты на снижение риска системы и обосновать выбор средства защиты.

Разработанный язык описания рисков нарушения безопасности является универсальным, так как позволяет задать формальное описание системы на уровне типизированных объектов, субъектов, угроз, воздействующих на систему, требований по безопасности, функций и средств защиты.

В третьей главе на основе разработанного языка приводится методика оценки рисков нарушения безопасности информационных систем с учетом множества атрибутов угроз, ресурсов, средств защиты на основе языка описания рисков нарушения безопасности.

Для реализации подхода к оценке рисков нарушения безопасности, предложенного в главе 2, была разработана методика, состоящая из следующих основных этапов:

1. Составление спецификации информационной системы на основании предметной области (рис. 2).
   - Составление спецификации объектов и субъектов.
   - Составление спецификации угроз.
   - Составление спецификации требований по безопасности.
   - Составление спецификации функций и средств защиты.

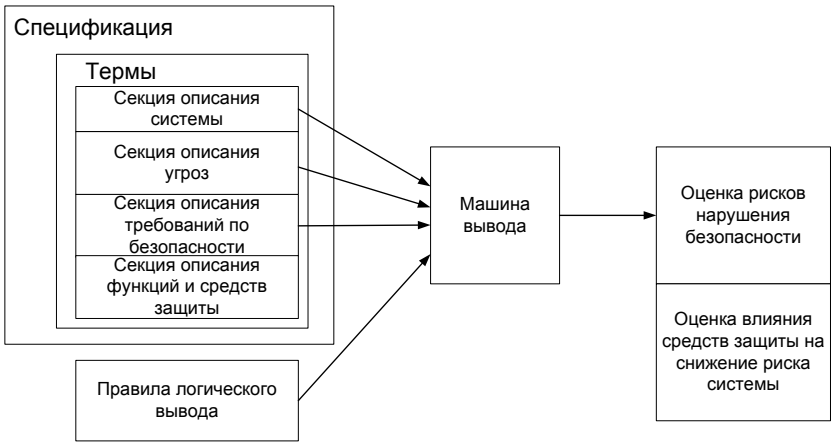

Рис. 2. Структура спецификации языка описания рисков нарушения безопасности

2. Оценка риска нарушения безопасности информационной системы

3. Оценка средств защиты информации с использованием методов нечеткой логики.

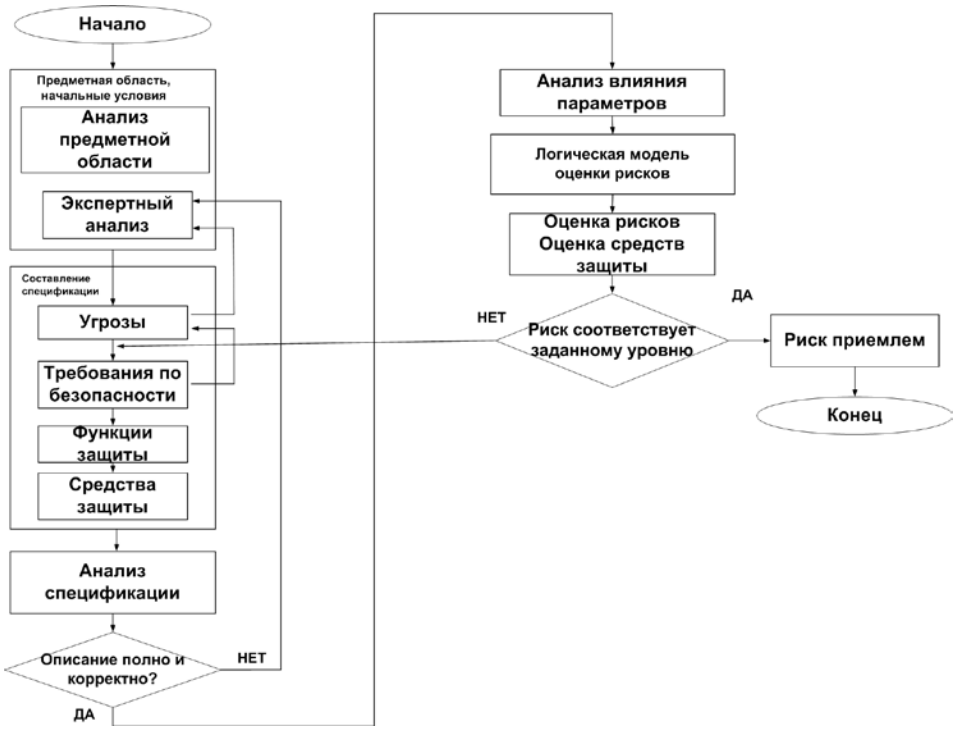

Рис. 3. Алгоритм методики оценки рисков нарушения безопасности с использованием языка описания рисков

Согласно предложенной методике для любой системы следует (рис. 3):

- составить формальное описание на уровне объектов (ресурсов), субъектов, угроз, функций защиты, требований по безопасности.

- проверить полноту и непротиворечивость спецификации
- оценить риски нарушения безопасности, оценить влияние средств защиты на снижение риска информационной системы с использованием правил логического вывода и методов нечеткой логики.

Предложенная методика позволяет проводить оценку рисков нарушения безопасности информационных систем, оценку влияния средства защиты на снижение риска системы с учетом различных атрибутов.

В четвертой главе приведен пример использования разработанной методики для оценки рисков нарушения безопасности в информационной системе с мобильным сегментом. Появление мобильного сегмента в информационной системе сопряжено с возникновением новых угроз информационной безопасности. При этом актуальной является как безопасность мобильного сегмента, так и взаимодействия мобильного и фиксированных сегментов (рис. 4) и, как следствие, требуется оценка рисков нарушения безопасности для таких систем, оценка влияния средств защиты на снижение риска нарушения безопасности.

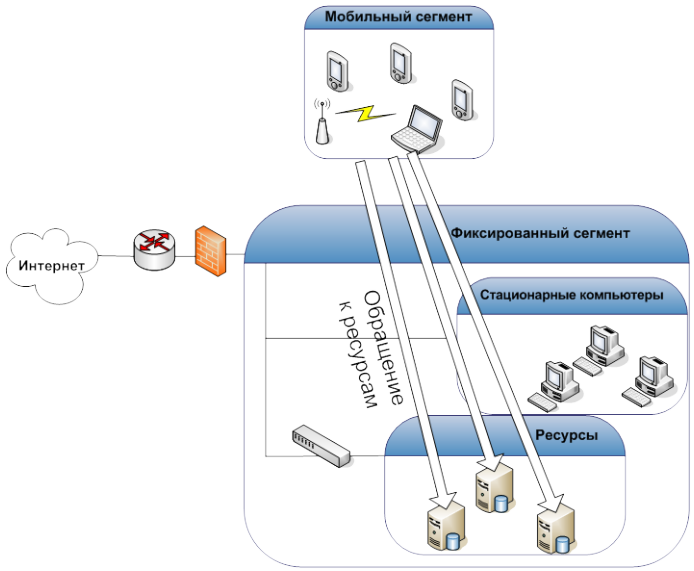

Рис. 4. Архитектура информационной системы с учетом удаленного доступа мобильных клиентов

Особенностями этой системы является то, что при удаленном обращении мобильных клиентов к ресурсам фиксированного сегмента актуальны угрозы раскрытия информации, угроза расширения прав при доступе к ресурсу и получение единовременного доступа ко всему дозволенному объему информации.

Для обеспечения защиты при осуществлении удаленного доступа мобильных клиентов к ресурсам информационной системы предлагается решение, которое позволит сократить угрозы и снизить риски нарушения безопасности. Если на стыке фиксированного и мобильного сегментов установить специализированный шлюз разграничения доступа, тогда все запросы мобильных клиентов к ресурсам фиксированного сегмента будут проходить через него, что позволит уменьшить воздействие наиболее критичных угроз (рис. 5). Так, например, конфиденциальная информация не хранится на мобильных устройствах и не передается по открытым каналам связи.

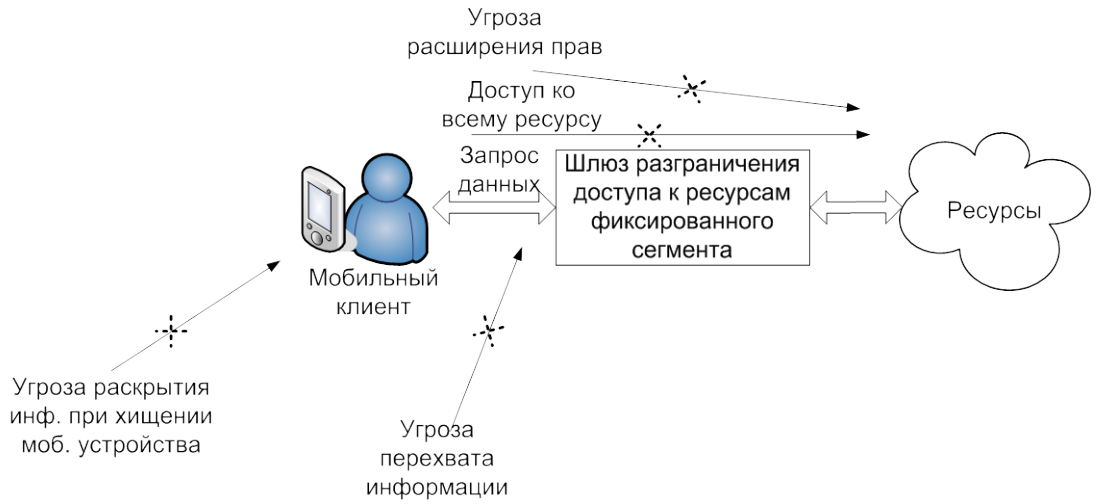

Рис. 5. Снижение воздействия угроз при обращении клиентов к ресурсам фиксированного сегмента через специализированный шлюз

С помощью языка описания рисков, информационная система, состоящая из фиксированного и мобильного сегментов, описана с использованием предикатов (табл. 4).

Таблица 4. Пример описания информационной системы

Предикаты	**Описание**
objectType(dataBase). *objectType(fileServer).* *objectType(mobleClient).* *objectType(channel).*	Определение типов объектов
object(wiredChannel, channel, [disclosure(veryLow)]). *object(wirelessChannel, channel, wireless, [disclosure(veryHigh), hearing(high)] , _, _). object(mobileClients, mobileClient, [availability(veryHigh), disclosure, substitution(veryLow), lost(medium)], _, _). object(dataBaseSecured, dataBase [oneTi-*	Определение объектов

meAccess(high), escalation(medium), substitution(veryLow)] , _, _).object(accessPoint, channel, [substitution(veryLow)], _, _).	
informationCategory(wired). *informationCategory(wireless).* *inCategory(wired, wireless).*	Определение категории информации
intruderType(internal). *intruderType(external).*	Определение типов нарушителя
threatType(confidentiality). *threatType(integrity).* *threatType(availability).* *threatType(mixed).*	Определение типов угроз
threat(disclosure, confidentiality, veryHigh). *threat(hearing, confidentiality, medium).* *threat(escalation, confidentiality, veryHigh).* *threat(oneTimeAccess, availability, low).* *threat(lost, mixed, high).*	Определение угроз
secFunction(antiDisclosure, disclosure, [wirelessChannel, mobileClients]). secFunction(antiHearing, hearing, wirelessChannel). *secFunction(antiEscalation, escalation, dataBase).* *secFunction(antiOneTimeAccess, oneTimeAccess, dataBase).* *newSecurityItem(gateway, [antiDisclosure, antiHearing, antiEscalation, antiOneTimeAccess]).*	Определение защитных мер
requirement(wirelessChannel, disclosure, veryLow).	Требование по безопасности

Согласно методике, приведенной в главе 3, была произведена оценка рисков нарушения безопасности для информационной системы с мобильным сегментом до и после внедрения специализированного шлюза, обрабатывающего запросы удаленных мобильных клиентов к ресурсам фиксированного сегмента.

Для рассматриваемого примера была определена зависимость вероятности ущерба от вероятности воздействия угроз (рис. 6, 7).

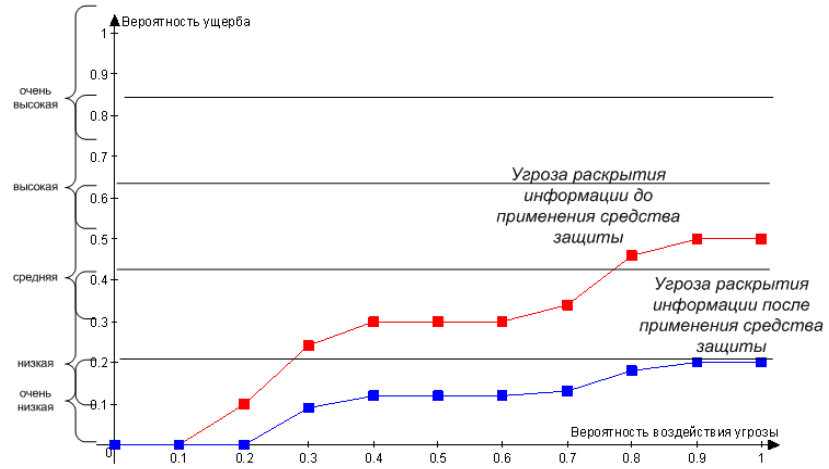

Рис. 6. Зависимость вероятности ущерба от вероятности воздействия угрозы раскрытия информации до и после применения средства защиты

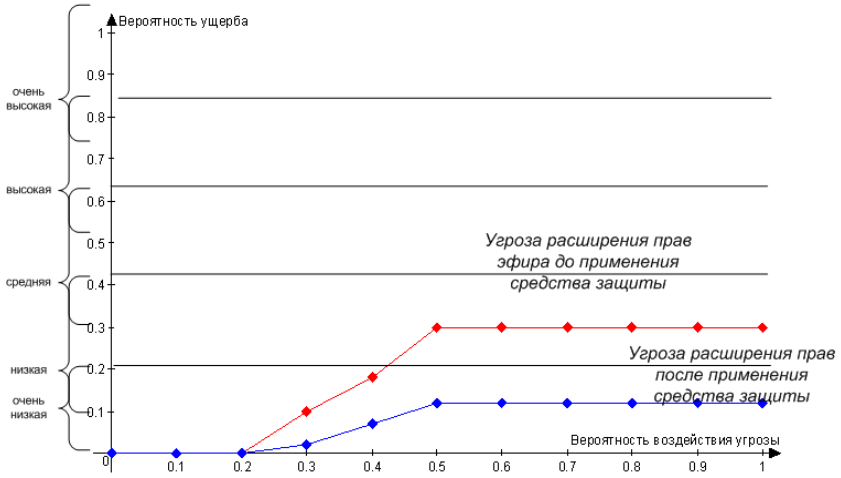

Рис. 7. Зависимость вероятности ущерба от вероятности воздействия угрозы расширения прав доступа до и после применения средства защиты

Использование специализированного шлюза разграничения доступа уменьшило вероятность воздействия основных критических угроз и тем самым снизило риск нарушения безопасности информационной системы. Воздействие угроз не может быть полностью устранено – то есть остался остаточный риск.

Для определения влияния средства защиты на снижение риска системы предложен относительный показатель Всз:

$$Всз = (\sigma - \sigma_{сз})/\sigma,$$

где σ – вероятность ущерба информационной безопасности до применения средства защиты, $\sigma_{сз}$ – вероятность ущерба информационной безопасности

при применении средства защиты. Показатель отражает нормированное значение влияния средства защиты на уменьшение вероятности воздействия угроз.

На рис. 8 приведен график зависимости показателя влияния средства защиты на снижение риска для системы в зависимости от вероятности воздействия угроз.

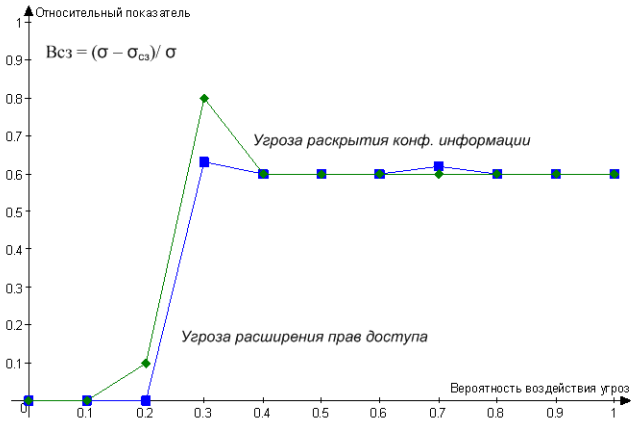

Рис. 8. Относительный показатель влияния средства защиты на снижение риска системы

Показатель отражает влияние средства защиты на снижение риска воздействия угроз. С увеличением вероятности реализации угроз, снижение риска не происходит ввиду наличия остаточного риска.

Разработанная методика оценки рисков на базе языка описания рисков позволяет:

- составить формальное описание информационной системы;
- проверить описание на полноту и непротиворечивость с использованием языка;
- оценить риски нарушения безопасности;
- оценить влияние различных средств защиты на снижение риска системы.

В заключении приведены результаты и выводы, полученные в ходе выполнения работы.

В работе получены следующие основные результаты:

1. Предложен подход к оценке рисков нарушения безопасности с использованием языка описания рисков, позволяющий оценивать риски с учетом множества атрибутов.
2. Разработан логический язык описания рисков нарушения безопасности информационных систем, позволяющий составить полную и непротиворечивую

спецификацию информационной системы, угроз и средств защиты.

3. Разработана методика оценки рисков нарушения информационной безопасности по различным атрибутам, позволяющая оценивать риски нарушения безопасности и оценить влияние средства защиты на снижение риска системы.

Основные публикации по теме диссертации

1. Лысенко А.Г. Моделирование безопасности информационных систем на основании языка описания рисков // "Проблемы информационной безопасности. Компьютерные системы". – 2008. – № 2. – С. 100-105. (из перечня ВАК РФ)

2. Лысенко А.Г. Моделирование информационной безопасности с использованием языка описания рисков // Материалы XVII общероссийской научно-технической конференции "Методы и технические средства обеспечения безопасности информации". – 2008. – С. 31.

3. Зегжда П.Д., Лысенко А.Г. Организация защищенного доступа к информации фиксированного сегмента для мобильных клиентов (тезисы доклада). Сб. материалов всероссийской межвузовской научно-технической конференции студентов и аспирантов. СПбГПУ. – 2008. – С. 85-86.

4. Зегжда П.Д., Лысенко А.Г. Вопросы безопасности гибридных корпоративных сетей высокой доступности // "Системы высокой доступности", 2007. – С. 45-50. (из перечня ВАК РФ).

5. Лысенко А.Г. Защита мобильного сегмента корпоративной сети // Материалы V Санкт-Петербургской межрегиональной конференции "Информационная безопасность регионов России" ("ИБРР-2007"): Материалы конференции. СПб: Политехника-сервис. – 2007. – Т. 1. – С. 87-88.

6. Лысенко А.Г. Расчет рисков нарушений информационной безопасности в сетях с мобильными сегментами // "Проблемы информационной безопасности. Компьютерные системы". – 2007. – № 2. – С. 100-105. (из перечня ВАК РФ).

7. Лысенко А.Г. Безопасность гибридных сетей // Материалы XVI общероссийской научно-технической конференции "Методы и технические средства обеспечения безопасности информации". – 2007. – С. 9.