Санкт-Петербургский государственный политехнический университет

На правах рукописи

04200911805

Лысенко Александр Георгиевич

МЕТОДИКА ОЦЕНКИ РИСКОВ ПРИ ПОСТРОЕНИИ СИСТЕМЫ ЗАЩИТЫ

Специальность:

05.13.19 — Методы и системы защиты информации, информационная безопасность

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель:

кандидат технических наук Корт Семён Станиславович

Санкт-Петербург — 2009

2

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 4

ГЛАВА 1. МЕТОДЫ ОЦЕНКИ РИСКОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 10

1.1. Сравнительный анализ методов оценки рисков нарушения информационной безопасности 11

1.1.1. Табличный метод 12

1.1.2. Метод анализа иерархий 13

1.1.3. Модель системы защиты с полным перекрытием Клементса 15

1.1.4. Сравнительный анализ средств оценки рисков нарушения информационной безопасности 17

1.2. Выводы 21

1.3. Расширение модели системы защиты с полным перекрытием 24

ГЛАВА 2. ЛОГИЧЕСКИЙ ЯЗЫК ОПИСАНИЯ РИСКОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 27

2.1. Требования к языку описания рисков нарушения информационной безопасности компьютерной системы 27

2.2. Структура языка описания рисков нарушения информационной безопасности 30

2.3. Выводы 55

ГЛАВА 3. МЕТОДИКА ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ С ИСПОЛЬЗОВАНИЕМ ЯЗЫКА ОПИСАНИЯ РИСКОВ 56

3.1. Этапы методики 56

3.2. Шкала оценки рисков нарушения информационной безопасности 60

3.3. Выбор функций принадлежности 61

3.4. Выводы 62

ГЛАВА 4. ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ И ОЦЕНКА РИСКОВ НА ПРИМЕРЕ КОМПЬЮТЕРНОЙ СИСТЕМЫ С

МОБИЛЬНЫМ СЕГМЕНТОМ 64

4.1. Компьютерная система с мобильным сегментом 64

4.1.1. Архитектура компьютерной системы 64

4.1.2. Модель нарушителя компьютерной системы с мобильным сегментом 66

4.1.3. Угрозы информационной системы с мобильным сегментом 67

4.2. Внесение в систему шлюза разграничения доступа 71

4.3. Составление спецификации системы на языке описания рисков и оценка рисков

ЗАКЛЮЧЕНИЕ

Представленнаявработеметодикапостроениясистемызащитынабазеразработанногологическогоязыкаописаниярисковпозволяетформализоватьописаниекомпьютернойсистемывыполнитьоценкурисковнарушенияинформационнойбезопасностиивыбратьвариантсистемызащитысогласнотребованиямполитикиинформационнойбезопасностииограничениямнариски

Вработеполученыследующиеосновныерезультаты

 Разработанамодельсвязывающаяоценкурисковнарушенияинформационнойбезопасностисдетализированнымописаниемкомпьютернойсистемынабораугрозфункцийисредствзащиты

 Разработаниреализованлогическийязыкописаниярисковпозволяющийприниматьрешенияодопустимомзначениирисканаоснованииописаниясистемыугрозисредствзащитыинформации

 Разработанаметодикаоценкирисковоснованнаянаразработанномязыкеипозволяющаяучестьстепеньопасностиугрозивлияниесредствзащитынарискинарушениябезопасностивкомпьютернойсистеме

 РазработанаметодикаанализавариантовсистемызащитыинформацииоснованнаянаязыкеописаниярисковМетодикапозволяетвыбратьсредствазащитыинформациисогласноограничениямнарискиитребованиямполитикиинформационнойбезопасностисучетоммножестваатрибутов

РазработаннаяметодикапостроениясистемызащитыбылапримененадляпостроениясистемызащитывкомпьютернойсистемесмобильнымсегментомБыласоставленаформальнаяспецификациясучетомугрозвоздействующихнасистемусредствзащитыинформациивыполненанализразличныхвариантовсистемызащитыипроизведенаоценкарисковнарушениябезопасностииврезультатевыбрансоставсистемызащиты