**Мартьянов Евгений Александрович Исследование и разработка методик оценки защищенности информационных объектов от потенциальных нарушителей**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

кандидат наук Мартьянов Евгений Александрович

Введение

Глава 1. Методики и методологии выявления инсайдера в информационных системах

1.1. Понятие инсайдера и задача его выявления

1.2. Программа CERT - анализ и изучение инцидентов в сфере информационной безопасности

1.3. Программа DARPA - поиск аномалий как средство выявления инсайдера

1.4. Верификация методов обнаружения инсайдера в информационной системе

1.5. Выводы к первой главе

Глава 2. Выявление инсайдера статистическими методами

2.1. Задача выявления инсайдера и способы её решения

2.2. Описание формальной модели информационной системы организации и ее пользователей

2.3. Алгоритм поиска инсайдера в информационной системе организации

2.4. Исследование свойств построенного алгоритма выявления инсайдера

2.5. Обобщение теории для большого количества пользователей

2.6. Дополнительные ограничения на доступ к содержанию определенных данных

2.7. Выводы ко второй главе

Глава 3. Имитационная модель поиска инсайдера в информационной системе

3.1. Применение имитационного моделирования в задачах выявления инсайдера

3.2. Задачи имитационного моделирования

3.3. Программная реализация средства для обнаружения инсайдера

с возможностью моделирования поведения пользователя

3.4. Задача 1. Работа пользователей с выборками большого объема

3.5. Задача 2. Закон Ципфа распределения вероятностей

3.6. Задача 3. Имитационное моделирование выборки атрибутов из хранилища данных по закону Ципфа

3.7. Задача 4. Сокрытие накопления избыточной информации инсайдером

3.8. Задача 5. Исследование времени работы алгоритма обнаружения инсайдера

3.9. Использование разработанного программного обеспечения на практике

3.10. Выводы к третьей главе

Заключение

Словарь терминов

Список литературы

Приложение А. Граничные значения для ожидаемой вероятности попадания атрибута в выборку аналитика