

Интеллектуальные сервисы защиты

информации в критических инфраструктурах

Сбор, преобразование и хранение информации о событиях безопасности

Аналитическое моделирование атак и поведения системы защиты на основе графов атак

Имитационное моделирование атак и поведения системы защиты

Анализ защищенности и оценка рисков

Верификация политик безопасности

Логический вывод на основе информации о событиях безопасности

Визуализация информации о событиях безопасности

Оглавление

Список сокращений и условных обозначений **9**

От рецензентов **12**

Введение **16**

ЧАСТЬ I. КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ПОСТРОЕНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СЕРВИСОВ ЗАЩИТЫ ИНФОРМАЦИИ **21**

Глава 1. Анализ современной литературы в области интеллектуализации сервисов защиты информации **23**

1.1. Научно-техническая литература по интеллектуальным средствам и методам защиты информации 23

1.2. Обзор литературы по аналитическому моделированию атак 26

1.2.1. Описание сценариев атак 26

1.2.2. Спецификация злоумышленников 28

1.2.3. Спецификация графов атак 28

1.3. Обзор литературы по механизмам защиты от бот-сетей и имитационному моделированию атак и механизмов защиты 30

Глава 2. Проблема защиты информации в критически важных инфраструктурах и требования к сервисам защиты **36**

2.1. Характеристика КВИ как объектов защиты информации 36

2.2. Проблема защиты информации в КВИ 39

2.3. Определение основных требований к сервисам защиты информации в КВИ 41

Глава 3. Принципы построения интеллектуальных сервисов защиты распределенных защищенных компьютерных сетей и систем **47**

3.1. Общая характеристика системы интеллектуальных сервисов защиты 47

3.2. Сервисы сбора, преобразования и хранения информации о событиях безопасности 49

3.3. Сервисы моделирования атак и поведения системы защиты 56

3.4. Сервисы поддержки принятия решений в области обеспечения безопасности 61

3.5. Сервисы визуализации информации о событиях безопасности 62

3.5.1. Круговая диаграмма 64

3.5.2. Гистограмма 65

3.5.3. Линейный график 65

3.5.4. Круговая диаграмма с накоплением 66

3.5.5. Гистограмма с накоплением 67

3.5.6. Линейный график с накоплением 67

3.5.7. Схемы полигонов ... 68
3.5.8. Диаграмма рассеяния ... 69
3.5.9. Параллельные координаты ... 70
3.5.10. Граф связей ... 71
3.5.11. Карта ... 72
3.5.12. Карта деревьев ... 73

Глава 4. Концепция интеллектуализации защиты информации в компьютерных сетях и системах объектов критически важных инфраструктур ... 75
4.1. Общие положения ... 75
4.2. Основные определения ... 75
4.3. Принципы интеллектуализации защиты информации ... 77
4.4. Цели и задачи системы интеллектуализации защиты информации ... 78
4.5. Особенности компьютерных сетей и систем объектов КВИ как объектов интеллектуализации защиты информации ... 78
4.6. Механизмы интеллектуализации защиты информации ... 84
4.7. Архитектура системы интеллектуализации защиты информации ... 84
4.8. Требования к системе интеллектуализации защиты информации ... 86

ЧАСТЬ И. МЕТОДЫ, МОДЕЛИ И АЛГОРИТМЫ ИНТЕЛЛЕКТУАЛЬНЫХ СЕРВИСОВ ЗАЩИТЫ ИНФОРМАЦИИ ... 89

Глава 5. Методы, модели и алгоритмы аналитического моделирования атак и механизмы защиты на основе многоуровневых графов атак ... 91
5.1. Модель анализируемой компьютерной сети ... 92
5.2. Модели компьютерных атак и нарушителя ... 99
5.3. Модель формирования дерева атак ... 108
5.3.1. Объекты дерева атак ... 108
5.3.2. Алгоритм формирования дерева атак ... 112

Глава 6. Методы, модели и алгоритмы динамического моделирования атак и механизмы защиты с использованием моделирования, основанного на имитации сетевых пакетов ... 116
6.1. Модели вредоносного программного обеспечения и механизмов защиты ... 116
6.1.1. Узлы вычислительной сети ... 117
6.1.2. Связи между узлами вычислительной сети ... 117
6.1.3. Компонент описания сценариев ... 119
6.1.3.1. Сценарии функционирования бот-сети ... 120
6.1.3.2. Сценарии защиты ... 131
6.1.3.3. Сценарии легитимной деятельности сети ... 133
6.2. Модели среды динамического моделирования, основанного на имитации сетевых пакетов ... 133
6.2.1. Общая модель среды моделирования ... 133
6.2.2. Модель сетевой структуры ... 135
6.2.3. Модель сценариев поведения ... 138
6.2.4. Модель взаимодействия с пользователем ... 140
6.3. Представление среды моделирования ... 140

Глава 7. Методы, модели и алгоритмы анализа защищенности и оценка рисков в компьютерных системах и сетях объектов критически важных инфраструктур 146
7.1. Подход к анализу защищенности и оценке риска 146
7.2. Методы и модели расчета общих показателей защищенности и риска 148
7.3. Методы и модели интегрированной оценки уровня защищенности на основе графа атак 151
7.4. Методы и модели расчета показателей навыков нарушителя, влияния и потенциала атаки, эффективности реагирования на атаку и косвенных потерь 165

Глава 8. Методы, модели и алгоритмы верификации политик безопасности в компьютерных системах и сетях объектов критически важных инфраструктур 169
8.1. Постановка задачи верификации политик безопасности 169
8.1.1. Основные понятия и определения политики безопасности 170
8.1.2. Характеристика и классификация конфликтов и аномалий в политике безопасности 172
8.2. Построение моделей политик безопасности для верификации на основе Common Information Model 176
8.2.1. Описание модели политики на основе CIM 176
8.2.2. Политика фильтрации 178
8.2.3. Политика аутентификации 184
8.2.4. Политика конфиденциальности 191
8.2.5. Политика авторизации 197
8.2.6. Политика операционных правил 203
8.3. Описание подходов к верификации политик безопасности 209
8.3.1. Метод "проверки на модели" 209
8.3.2. Методы доказательства теорем 212
8.3.3. Метод, основанный на гибридном подходе 212
8.3.4. Другие методы 213
8.4. Методика верификации методом "проверки на модели" 214
8.4.1. Модель защищенной компьютерной сети у межсетевого экрана 214
8.4.2. Модели аномалий фильтрации 217
8.4.3. Алгоритмы верификации правил политики безопасности и разрешения конфликтов 220
8.5. Методика верификации методом исчисления событий 221
8.5.1. Базовая аксиоматика для построения модели защищаемой сети 221
8.5.2. Алгоритм верификации 223

Глава 9. Механизмы логического вывода на основе информации в репозитории событий и информации безопасности 227
9.1. Релевантные работы 227
9.2. Описание языков и понятий для систем логического вывода 230
9.2.1. Язык RDFS 230
9.2.2. Язык Web Ontology Language 231
9.2.3. Язык Semantic Web Rule Language 233
9.2.4. Язык Protocol and RDF Query Language 235

9.3. Описание существующих систем логического вывода 236
9.4. Архитектура системы логического вывода для событий и информации безопасности, хранящейся в репозитории 237
9.5. Использование системы логического вывода для событий и информации безопасности для сервиса моделирования атак и поведения системы защиты 238

Глава 10. Модели визуализации информации и событий безопасности 242
10.1. Модели визуализации для мониторинга периметра сети 242
10.2. Модели визуализации информации о защищенности сети 249

ЧАСТЬ III. РЕАЛИЗАЦИЯ, ПРИМЕНЕНИЕ И ОЦЕНКА ИНТЕЛЛЕКТУАЛЬНЫХ СЕРВИСОВ ЗАЩИТЫ ИНФОРМАЦИИ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ 255

Глава 11. Архитектура системы интеллектуальных сервисов защиты информации 257
11.1. Общая архитектура 257
11.2. Архитектура сервисов уровня данных 261
11.3. Архитектура сервисов уровня передачи событий 264
11.4. Архитектура сервисов прикладного уровня 266
11.4.1. Обработка событий 267
11.4.2. Управление моделированием 268
11.4.3. Поддержка и принятие решений 271
11.4.4. Визуализация 273
11.4.5. Репозиторий 276

Глава 12. Разработка программных прототипов компонентов интеллектуальных сервисов защиты информации 277
12.1. Описание архитектуры и программного прототипа компонента построения и анализа графов атак 277
12.1.1. Описание архитектуры 277
12.1.2. Описание программного прототипа 279
12.2. Описание архитектуры и программного прототипа компонента хранения данных (репозитория) и механизмов логического вывода 282
12.2.1. Описание архитектуры 282
12.2.1. Описание программного прототипа 283
12.3. Описание архитектуры и программного прототипа компонента визуализации информации безопасности и событий 288
12.3.1. Подходы к построению систем визуализации 288
12.3.2. Описание архитектуры 288
12.3.3. Описание программного прототипа 290
12.4. Описание архитектуры и программного прототипа компонента верификации политик безопасности 293
12.4.1. Описание архитектуры 293
12.4.2. Описание программного прототипа 295

Глава 13. Теоретическая и экспериментальная оценка интеллектуальных сервисов защиты информации и сравнение предложенных технологий на соответствие мировому уровню 304
13.1. Общий подход к теоретической и экспериментальной оценке интеллектуальных сервисов защиты информации 304
13.1.1. Основные понятия 304
13.1.2. Определение номенклатуры показателей качества 305
13.1.3. Модель процесса оценивания качества программного средства 310
13.1.4. Общая методика оценивания качества программного средства 312
13.1.5. Методика экспертного анкетирования 315
13.2. Теоретическая и экспериментальная оценка компонента построения и анализа графов атак 319
13.2.1. Выбор показателей для оценки 319
13.2.1.1. Функциональные показатели 319
13.2.1.2. Показатели эффективности 321
13.2.1.3. Сопровождаемость 321
13.2.1.4. Мобильность 322
13.2.2. Проведение оценки 322
13.3. Теоретическая и экспериментальная оценка компонента хранения данных (репозитория) и механизмов логического вывода 325
13.3.1. Выбор показателей для оценки 325
13.3.1.1. Функциональные показатели 325
13.3.1.2. Показатели эффективности 327
13.3.1.3. Сопровождаемость 328
13.3.1.4. Мобильность 329
13.3.2. Проведение оценки 329
13.4. Теоретическая и экспериментальная оценка компонента верификации политик безопасности 333
13.4.1. Выбор показателей для оценки 333
13.4.2. Проведение оценки 336
13.5. Теоретическая и экспериментальная оценка компонента визуализации 342
13.5.1. Критерии оценивания 343
13.5.1.1. Функциональные показатели 343
13.5.1.2. Показатели визуализации 343
13.5.1.3. Показатели методики взаимодействия 344
13.5.2. Результаты оценивания 345
13.5.3. Количественный анализ интерфейса 346
13.5.3.1. Количественная оценка интерфейса для редактирования свойств сетевых объектов 348
13.5.3.2. Количественная оценка интерфейса для расчета метрик безопасности 351
13.5.4. Сопровождаемость 351
13.5.5. Мобильность 352
13.6. Обобщение и оценка полученных результатов 353

Заключение 357

Список литературы 360

Сведения об авторах 395

Предметный указатель 398