



Подсистемы идентификации и аутентификации относятся к разряду самых сложных интеллектуальных информационных систем, которые еще не изучены до конца и практически не регулируются на федеральном уровне. Тем не менее, согласно нормативным документам, выбор методов, механизмов и средств аутентификации возложен на владельца информационной системы.

В данном пособии предпринята одна из первых попыток системного изложения теоретических основ, моделей и методов исследования процессов идентификации и аутентификации. Выполнен анализ зарубежной и отечественной нормативной базы, рассмотрены методы и подходы исследования процессов аутентификации. Выполнена классификация систем идентификации и аутентификации, механизмов и средств аутентификации. Приводятся примеры построения простейших моделей процессов идентификации и аутентификации, проанализирована применимость основных методов анализа рисков и исследования надежности выполнения этих процессов. Рассмотрен ряд прикладных задач, связанных с применением аутентификации и электронной подписи.

Пособие предназначено для системных администраторов, администраторов безопасности, руководителей ИТ-служб как небольших организаций, так и крупных компаний, специалистов служб технической поддержки и инженеров предприятий и организаций, планирующих внедрение двухфакторной аутентификации, а также внедрение и обслуживание системы SafeNet Authentication Manager (SAM).

Введение

Глава 1. Анализ современного состояния нормативно-правовой базы и методологического обеспечения безопасности процессов аутентификации

1.1. Обзор зарубежной нормативной базы

1.2. Краткий анализ зарубежной нормативной базы

1.3. Анализ отечественной нормативной базы

- Федеральные законы
- Постановления Правительства
- Распоряжения Правительства
- Руководящие документы ФСБ России
- Руководящие документы ФСТЭК (Гостехкомиссии) России
- Нормативные акты Министерства связи и общественных коммуникаций
- Стандарты

1.4. Краткий обзор научных работ по анализу ИА

1.5. Обзор работ по анализу рисков

1.6. Анализ методов оценки надежности идентификации и аутентификации

1.7. Взаимосвязь понятий безопасности и надежности

1.8. Качество сервисов ИА

Глава 2. Методы исследования систем и процессов аутентификации

2.1. Основные определения

2.2. Процессы аутентификации. Участники взаимодействия и аутентификационная информация

2.3. Процедуры, составляющие процессы идентификации и аутентификации

2.4. Классификация СИА по требованиям ИБ

2.5. Классификация процессов аутентификации

2.6. Классификация средств идентификации и аутентификации

2.7. Анализ применимости методов оценки рисков

Глава 3. Методы многоуровневого анализа рисков нарушения информационной безопасности ИА при УЭВ

3.1. Общая методика оценки рисков

3.2. Методика предварительной оценки рисков ИА в ГИС

3.3. Анализ рисков СИА как отдельной подсистемы

- Многоуровневая модель пространства угроз
- Первый уровень детализации СИА. Угрозы информации в системе аутентификации как элементе системы управления доступом пользователей в ИС
- Второй уровень детализации СИА. Угрозы информации в процессах аутентификации, состоящих из цепи последовательных процедур
- Третий уровень детализации СИА. Угрозы информации в процессах аутентификации, детализированных до устройств и ПО
- Четвертый уровень детализации СИА. Угрозы информации в процессах аутентификации, детализированных до чипа устройств

3.4. Идентификация опасности и предварительная оценка последствий

- Модель дерева событий
- Оценка частоты возникновения опасных событий
- Анализ последствий

3.5. Методика оценки рисков процессов ИА

3.6. Пример оценки рисков. ЕСИА

- Объект исследования. Описание типовой схемы аутентификации
- Краткий анализ атак
- Оценка рисков аутентификации
- Пример предварительных оценок рисков процедур аутентификации

3.7. Особенности удаленной сетевой аутентификации

Глава 4. Об анализе надежности идентификации и аутентификации

4.1. Методика и модели исследования надежности идентификации

4.2. Оценка надежности аутентификации

Заключение

Приложения

Приложение 1. Уровни достоверности аутентификации

Приложение 2. Рекомендации по использованию типов (технологий) аутентификации в зависимости от применяемых видов электронной подписи

Приложение 3. Рекомендации по применению ключевых носителей

Приложение 4. Модели оценки надежности идентификации

Приложение 5. Рекомендации по изменению нормативной базы в части идентификации и аутентификации

Приложение 6. Перспективы развития доверенных АИС

Приложение 7. Решение задач аутентификации и защиты персональных данных при переходе к облачным вычислениям

Список литературы

Вспомогательная информация

- **Словарь терминов**
- **Список сокращений**
- **Иностранные аббревиатуры**
- **Глоссарий**