

Бабенко Л. К., Басан А. С., Журкин И. Г., Макаревич О. Б.

Защита данных геоинформационных систем: учеб. пособие для студенте]
вузов / Под ред. *И. Г. Журкина*. — М.: Гелиос АРВ, 2010. — 336 с, ил.

ВВЕДЕНИЕ.....

Глава 1. ОСНОВЫ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ ГИС

- 1.1. Понятие геоинформационной системы
- 1.2. Структура построения и функциональная схема ГИС
- 1.3. Оценка эффективности ГИС
- 1.4. Системы сбора геопространственных данных
- 1.5. Системы представления картографических данных
- 1.6. Типы геопространственных данных
- 1.7. Обзор инструментально-программных средств ГИС
- 1.7.1. ГИС «ПАНОРАМА»
- 1.7.2. ГИС «ArcGIS».....
- 1.7.3. «MapInfo», «Intergraph», «AUTOCAD»
- 1.8. Классификация ГИС по признаку доступности данных.....
- 1.8.1. Сетевые ГИС
- 1.8.2. Персональные ГИС
- 1.8.3. Интернет ГИС

Глава 2. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ГИС.....

- 2.1. Анализ данных, подлежащих защите в ГИС
- 2.2. Классификация угроз по их источнику
- 2.2.1. Антропогенные угрозы.....
- 2.2.2. Техногенные угрозы.....
- 2.2.3. Форс-мажорные обстоятельства
- 2.3. Характеристика наиболее часто проявляющихся угроз
- 2.4. Выявление угроз для конкретных компонентов ГИС.....

Глава 3. ОСНОВНЫЕ ПОНЯТИЯ И МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ГИС.

- 3.1. Методы шифрования
- 3.1.1. Симметричные криптосистемы
- 3.1.2. Асимметричные криптосистемы.....
- 3.2. Методы аутентификации
- 3.2.1. Парольная аутентификация
- 3.2.2. Симметричные методы аутентификации. Схема Kerberos
- 3.2.3. Асимметричные методы аутентификации. Удостоверяющие центры и цифровые сертификаты

3.3. Модели разграничения доступа	
3.3.1. Дискреционная модель доступа.....	
3.3.2. Мандатная модель доступа.....	

Глава 4. ПРИМЕНЕНИЕ SWOT-АНАЛИЗА ДЛЯ ВЫРАБОТКИ СТРАТЕГИИ ЗАЩИТЫ ИНФОРМАЦИИ В ГИС

Глава 5. СТРАТЕГИИ ЗАЩИТЫ ИНФОРМАЦИИ В ПЕРСОНАЛЬНЫХ ГИС

5.1. Защита информации в персональной ГИС массового использования.....	
5.2. Защита информации в персональной настольной ГИС	
5.3. Криптографическая защита хранимых и обрабатываемых данных в персональных настольных ГИС	
5.3.1. Выбор криптографического алгоритма для защиты персональных ГИС	
5.3.2. Особенности реализации модуля криптографической защиты файлов данных в информационных системах. Разработка модуля перехвата данных с помощью промежуточного драйвера файловой системы	

Глава 6. ЗАЩИТА ИНФОРМАЦИИ В ГИС НА СЕТЕВОМ УРОВНЕ.....

6.1. Стратегии защиты информации в Интернет ГИС.....	
6.2. Защита Интернет сервера.....	
6.3. Обеспечение безопасности WEB-серверов	
6.4. Особенности использования и настройки стандартных картографических серверов	
6.5. Анализ вариантов реализации картографического Интернет сервера.....	
6.6. Вопросы реализации Интернет ГИС с помощью базовой геоинформационной системы.	
6.6.1. Вопросы разработки подсистемы взаимодействия клиента и серверного сценария....	
6.6.2. Вопросы разработки подсистемы взаимодействия серверного сценария и базовой геоинформационной системы	
6.7. Вопросы реализации элементов ГИС в Интернет сервере	
6.7.1. Вопросы подготовки и использования картографического материала.....	
6.7.2. Вопросы подготовки и использования семантических данных.....	
6.7.3. Связь между пространственными и семантическими данными	
6.7.4. Вопросы реализации навигации	
6.7.5. Указание местоположения пространственных объектов на карте	
6.7.6. Использование многослойных карт	
6.8. Методы защиты Интернет ГИС, используемой для решения корпоративных задач	
6.9. Вопросы разработки технических средств по защите данных в сетевой геоинформационной системе.....	
6.9.1. Сетевая архитектура сетевой ГИС.....	
6.9.2. Архитектурные решения по защите сетевых данных.....	

6.9.3. Возможности шифрования пакетов на различных сетевых уровнях

- 6.9.4. Использование протоколов IPSec для защиты данных ГИС на сетевом уровне.....
- 6.10. Обоснование перечня организационных мероприятий по защите данных в сетевой геоинформационной системе.....

Глава 7. РАЗРАБОТКА И ВНЕДРЕНИЕ МАНДАТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА В СОВРЕМЕННЫЕ ГИС И СУБД.....

- 7.1. Механизм добавочной защиты. Понятия и основные принципы построения диспетчера доступа.....
- 7.2. Разработка модели мандатного доступа в современных реляционных СУБД.....
 - 7.2.1. Формальное описание и требования к модели мандатного разграничения доступа...
 - 7.2.2. Анализ модели мандатного разграничения доступа в СУБД Oracle.....
 - 7.2.3. Общие вопросы разработки модели мандатного доступа в реляционных СУБД.....
 - 7.2.4. Классификация объектов доступа.....
 - 7.2.5. Определение собственника, владельца и пользователя информации.....
 - 7.2.6. Разработка формальной модели мандатного доступа в реляционных СУБД.....
 - 7.2.7. Проблема взаимодействия мандатного и дискреционного доступа в СУБД.....
- 7.3. Разработка системы мандатного доступа в реляционных СУБД.....
 - 7.3.1. Разработка архитектуры СУБД с мандатным доступом.....
 - 7.3.2. Разработка структуры цифрового сертификата как средства хранения мандатных прав доступа.....
 - 7.3.3. Внесение классификационных меток в объекты доступа.....
 - 7.3.4. Алгоритмы обработки запросов диспетчером доступа.....
- 7.4. Реализация мандатного доступа в современных ГИС на примере «Карта 2005».....
 - 7.4.1. Протокол взаимодействия ГИС с прикладными программами и открытый формат цифровой информации о местности.....
 - 7.4.2. Хранение меток конфиденциальности для различных уровней представления картографической информации.....
 - 7.4.3. Вопросы реализации мандатного доступа на уровне объектов на картах.....
 - 7.4.4. Вопросы реализации мандатного доступа на уровне районов работ, пользовательских карт, классификаторов и слоев.....

Глава 8. ИСПОЛЬЗОВАНИЕ СТЕГАНОГРАФИИ В ГИС.....

- 8.1. Основные задачи, решаемые стеганографическими системами.....
- 8.2. Основные требования к стеганографическим методам.....
- 8.3. Основные способы стеганографирования.....
- 8.4. Возможность применения стеганографии в ГИС.....

Глава 9. ПОКАЗАТЕЛИ И МЕТОДИКИ ОЦЕНКИ СРЕДСТВ БЕЗОПАСНОСТИ ГИС.....

- 9.1. Оценка стоимости системы безопасности ГИС.....
 - 9.1.1. Оценка стоимости защиты информации на основе минимизации затрат и потерь.....

9.1.2.	Оценка стоимости защиты информации на основе априорных данных о хакерах...	
9.2.	Показатели подсистемы криптографической защиты ГИС	
9.2.1.	Криптостойкость средств симметричного шифрования	
9.2.2.	Быстродействие средств симметричного шифрования.....	
9.2.3.	Криптостойкость средств расчета хэш-значения	
9.2.4.	Быстродействие средств расчета хэш-значения.....	
9.2.5.	Криптостойкость электронной цифровой подписи	
9.2.6.	Быстродействие средств выработки и проверки электронной цифровой подписи...	
9.3.	Подсистема обеспечения целостности информации БД ГИС	
9.3.1.	Надежность функционирования подсистемы обеспечения целостности информации ГИС	
9.3.2.	Глубина отката ошибочных действий оператора	
9.3.3.	Интервал обновления контрольных точек	
9.3.4.	Степень достоверности средств контроля целостности БД ГИС и исполняемых модулей СПО	
9.3.5.	Надежность средств архивации, кодирования и сжатия информации ГИС	
9.4.	Подсистема мониторинга защищенности ГИС	
9.4.1.	Степень достоверности анализа вычислительных ресурсов ГИС	
9.4.2.	Быстродействие подсистемы мониторинга.....	
9.4.3.	Быстродействие встроенных средств оповещения	
9.4.4.	Объем протоколируемых событий.....	
9.4.5.	Степень защищенности системных регистрационных журналов от несанкционированного ознакомления и модификации.....	
9.5.	Показатели подсистемы аутентификации	
9.5.1.	Эффективность средств защиты при использовании детерминированных средств доступа.....	
9.5.2.	Оценка эффективности средств защиты от НСД к ресурсам рабочих станций с использованием биометрической аутентификации пользователя.....	
9.6.	Разработка проекта типовой методики оценки слабоформализуемых показателей безопасности ГИС	
9.6.1.	Разработка методики синтеза экспертных оценок.....	
9.6.2.	Разработка проекта типовой методики экспертной оценки показателей безопасности ГИС	
	Глава 10. СХЕМА КОМПЛЕКСНОЙ ЗАЩИТЫ ДАННЫХ ГИС	
	Глава 11. НОРМАТИВНАЯ ДОКУМЕНТАЦИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ГЕОИНФОРМАТИКЕ	
	ЗАКЛЮЧЕНИЕ.....	
	СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	