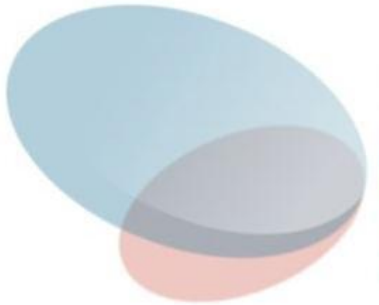

ОПЗБД
Лекция 1
Введение
1.Постановка задачи обеспечения информационной безопасности баз данных

Введение. Стр. 1

Ядром любой **системы автоматизированного управления** является **информационная система (ИС).**

Одной из важнейших **характеристик качества** ИС служит **уровень обеспечения ее информационной безопасности**.

9 сентября 2000 г. указом Президента РФ утверждена **Доктрина информационной безопасности Российской Федерации**.

В ней определена важность поиска эффективных методов решения проблемы обеспечения информационной безопасности (ИБ) автоматизированных систем информационного обеспечения управления.

Указ Президента РФ от 5 декабря 2016 г. № 646
“Об утверждении Доктрины информационной безопасности Российской Федерации”

Доктрина информационной безопасности Российской Федерации
(утв. Указом Президента РФ от 5 декабря 2016 г. № 646)

Введение. Стр. 2

Вопросы информационной безопасности баз данных рассматривают **с двух взаимодополняющих позиций**:

— **оценочные стандарты.**

Осуществляют **классификацию** информационных систем и средств их защиты в соответствии с требованиями безопасности.

Играют роль архитектурных спецификаций;

— **технические спецификации.**

Регламентируют различные аспекты **реализации средств защиты**.

Определяют, каким образом строить информационную систему конкретной архитектуры.

Введение. Стр. 3

Комплексная система обеспечения информационной безопасности должна строиться с учетом средств и методов, характерных **для всех ее уровней.**

Различают четыре уровня информационной системы:

— уровень **прикладного программного обеспечения**, отвечающий за взаимодействие с пользователем;

— уровень **системы управления базами данных (СУБД)**, обеспечивающий хранение и обработку данных информационной системы;

— уровень **операционной системы**, отвечающий за функционирование СУБД и иного прикладного программного обеспечения;

— уровень **среды доставки**, отвечающий за взаимодействие информационных серверов и потребителей информации.

Введение. Стр. 4

Проблема обеспечения безопасности автоматизированных информационных систем (АИС) может быть определена **как решение трех взаимосвязанных задач,** реализующих требуемый уровень:

— ***конфиденциальность*** — обеспечение пользователям доступа только к тем данным, для которых пользователь имеет явное или неявное разрешение на доступ (синонимы — **секретность, защищенность**);

— ***целостность*** — обеспечение защиты от преднамеренного или непреднамеренного *изменения* информации или процессов ее обработки;

— ***доступность*** — обеспечения *возможности* авторизованным в системе пользователям *доступа* к информации в соответствии с принятой технологией (синоним — **готовность**).

Введение. Стр. 5

- **Задача обеспечения конфиденциальности** предусматривает комплекс мер по **предотвращению несанкционированного доступа** к информации ограниченного пользования.
- **Задача обеспечения целостности** предусматривает комплекс мер по **предотвращению** умышленного или случайного **изменения или уничтожения** информации, используемой системой принятия решений.
- **Задача обеспечения доступности информации** предусматривает систему мер по поддержке всем уполномоченным пользователям **доступа** к ресурсам системы в соответствии с принятой технологией (например, круглосуточно).

Введение. Стр. 6

Анализ безопасности архитектурных решений и их программных реализаций в СУБД должен включать исследование следующих проблем:

- **идентификация и аутентификация** субъектов системы;
- **технологии реализации модели доступа** к ресурсам системы
  - **дискреционной,**
  - **мандатной и**
  - **ролевой**;
- **реализация аудита** действий пользователей.

Введение. Стр. 7

Дискреционная модель доступа

Обращается внимание на особенности **реализации системных привилегий и привилегий доступа к объектам системы**, механизмы предоставления и отзыва привилегий.

Основой системы разграничения доступа в большинстве СУБД промышленного уровня является реализация **принципа минимальных привилегий**.

- Суть **принципа минимальных привилегий:** пользователю должно быть явно (а не по умолчанию) разрешено выполнение каждого действия в системе.

То есть **возможность выполнения какого-либо действия в системе** (начиная с регистрации пользователя) **по умолчанию должна быть отключена или определена в минимально возможном объеме**, определяемом объективными условиями эксплуатации системы.

Мандатная модель управления доступом

Важнейший вопрос — технология присваивания и изменения **меток для объектов и субъектов**.

Разграничение доступа реализуется **на уровне кортежей и** предполагает наличие **специального столбца с меткой доступа.** Технология изменения данных в таком специальном столбце должна отличаться от традиционной.

Ролевая модель доступа

Широко распространена в мировой практике обеспечения защищенных технологий обработки баз данных.

Понятие **роли** вошло составной частью в стандарт SQL (SQL:2008) и стандарт Common Criteria для коммерческого профиля безопасности.

Введение. Стр. 9

- **Роль** — это **поименованный набор привилегий, который может быть предоставлен пользователю или другой роли.**

По сути, это языковое средство **для автоматизации работы администратора** по разграничению доступа. (Большое число пользователей, статус которых требует различных привилегий для доступа к ресурсам базы данных, создает значительный объем рутинной работы администратору.)

- ✔ Описание привилегий, характерных для той или иной роли, готовится заранее.
- ✔ При регистрации нового пользователя в системе администратор выполняет только предоставление пользователю привилегий конкретной роли.
- ✔ При необходимости изменить привилегии конкретному приложению достаточно изменить только привилегии соответствующей роли. Все пользователи, отображенные на эту роль, автоматически получат измененные привилегии.

Введение. Стр. 10

Представления. Использование **представлений** — широко применяемый, простой и эффективный способ реализации разграничения доступа.

- **Представление (view) — поименованная динамически поддерживаемая сервером выборка из одной или нескольких таблиц**.
- Оператор SELECT, определяющий выборку, **ограничивает *видимые*** пользователем данные.
- Представление также позволяет эффективно **ограничить данные**, **которые пользователь может *модифицировать***.
- Сервер гарантирует **актуальность представления**, то есть формирование представления (материализация соответствующего запроса) производится каждый раз при использовании представления.

Используя представления, администратор безопасности ограничивает доступную пользователю часть базы данных только теми данными, которые реально необходимы для выполнения работы этого пользователя.

Введение. Стр. 11

Триггеры. Специфическое для СУБД средство обеспечения информационной безопасности — **триггеры**.

- **Триггер** — это **совокупность предложений языка SQL или некоторого иного процедурного языка, автоматически запускаемая сервером при регистрации определенных событий в системе**.

Триггеры выполняются системой автоматически **до** или **после** возникновения предопределенных событий, таких, как выполнения операций INSERT, UPDATE, DELETE в некоторой таблице.

Обычно рассматривают два способа **использования триггеров для повышения защищенности системы**:

- дополнительный **контроль допустимости действий пользователя;**
- **ведение** специализированного (нестандартного) **аудита** действий пользователя.

Введение. Стр. 12

Особенность триггеров — автоматически реализуемая возможность выполнить необходимые проверки полномочий перед выполнением операций над таблицами.

На одном множестве таблиц может быть определено несколько триггеров. Комбинации триггеров, выполняемых до и после операций, позволяют создавать сложные механизмы проверки допустимости тех или иных действий в базе данных и фиксации (или откате) их результатов.

- Современные **СУБД промышленного уровня** поддерживают триггеры, запускаемые **для определенных *системных* событий**, в частности:
  - начала и завершения сессии взаимодействия пользователя с системой,
  - запуска и останова экземпляра сервера баз данных,
  - создания и уничтожения объектов и т. п.

Введение. Стр. 13

Шифрование. Еще одним направлением для СУБД является **наличие *встроенных механизмов шифрования* на уровне столбцов таблиц**, в основном на базе алгоритмов DES и AES.

- **Представлены встроенные генераторы псевдослучайных последовательностей и алгоритмы вычисления хеш-функций.**
- **Реализовано явное и неявное управление ключами**.

Риски. Исследование безопасности СУБД должно включать и **изучение инсайдерских рисков**: возможностей пользователей СУБД несанкционированно осуществлять чтение и запись в файлы и устройства операционной системы, включая возможность модификации записей аудита, осуществляемых во внешние файлы.

Введение. Стр. 14

Аудит. Полноценная система обеспечения безопасности должна обладать развитыми **средствами аудита**, то есть **автоматического ведения протоколов действий пользователей системы**.

В СУБД средство ведения аудита может быть реализовано

- в виде набора возможностей, управляемых языковыми средствами системы,
- или независимой утилиты (пакета).

Введение. Стр. 15

Аудит — функция регистрации различных событий (действий) в системе.

Гарантированно защищенных серверов баз данных нет.

Нет абсолютно надежных средств защиты среды передачи данных, механизмов аутентификации пользователей и технологий разграничения доступа.

Нельзя исключить возникновения обстоятельств, приводящих к разрушению данных конкретной системы.

Важным фактором, определяющим вероятностную сущность задачи обеспечения информационной безопасности, является высокая динамика изменений самих баз данных.

Аудит обеспечивает **непрерывный контроль событий**, происходящих с базами данных, и является эффективным средством повышения качества обеспечения их информационной безопасности.

Введение. Стр. 16

На основе анализа данных мониторинга состояния системы соответствующие алгоритмы должны определить *потенциально опасные* для безопасности информации *действия пользователей или события* и обеспечить *запуск процедур*, реализующих необходимые *меры противодействия*.

Первым этапом анализа уровня информационной безопасности баз данных должен быть этап выявления угроз.

Угрозы информационной безопасности всегда объективно существуют при использовании информационных технологий. **Источники угроз** определяются **средой**, в которой происходит работа с базами данных, и субъектами, осуществляющими обработку информации.

Определение субъектов информационных отношений на уровне предметной области и **выявление интересов** этих субъектов — необходимые предпосылки для профессионального проведения анализа безопасности баз данных.

Введение. Стр. 17

Средства аудита выполняют фиксацию информации об активности пользователей системы в **словаре данных** или в файле операционной системы — **журнале аудита**.

Информация о настройках системы аудита хранится в специальном **конфигурационном файле**.

Файл настройки или параметры команды активизации аудита **определяют перечень событий, которые фиксируются системой аудита**.

Исследование средств аудита должно включать:

- вопросы устойчивости системы аудита к несанкционированному изменению параметров системы и собственно данных аудита,
- избирательность средств аудита,
- возможность оптимизации параметров при заданных (стоимостных) критериях и ограничениях на объем используемых ресурсов системы.

Введение. Стр. 18

Исследование вопросов, связанных с программным обеспечением промежуточного уровня, должно включать:

- выявление портов взаимодействия с внешним программным обеспечением и механизмов их активизации и переназначения (внутренние и внешние);
- устойчивость к перегрузкам каналов шумовым трафиком и вставкам ложных пакетов;
- возможность внутреннего и внешнего управления активизацией и перенастройкой параметров протоколов ODBC (*Open Database Connectivity*) и JDBC (Java DataBase Connectivity — *соединение с базами данных на* Java) ;
- анализ алгоритмов и технологий линейного шифрования трафика межсерверного обмена и взаимодействия клиентского программного обеспечения с серверами баз данных.

1. Постановка задачи обеспечения информационной безопасности баз данных

1.1. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных. Стр. 1

Увеличение количества компьютеров и областей их применения расширило возможности модификации, хищения и уничтожения данных.

Выделяют следующие **этапы развития концепций обеспечения безопасности данных**.

Первый этап

Центральной идеей являлось намерение обеспечить безопасность данных **механизмами**, **функционирующими по строго формальным алгоритмам**.

- Программные **средства защиты включались в состав операционных систем и систем управления базами данных**.

1.1. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных. Стр. 2

Второй этап

- Главным достижением стала разработка концепции и реализации ***ядра безопасности*** — **специального программного компонента**, **управляющего программными и, частично, аппаратными средствами защиты данных.**

В составе операционных систем ядро безопасности реализовывалось как функционально самостоятельная подсистема управления механизмами защиты данных, которая включала

- технические,
- программные,
- и лингвистические средства.

Этап также характеризовался интенсивным развитием технических и криптографических средств защиты.

1.1. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных. Стр. 3

Третий этап

Основной отличительной особенностью стало использование научного уровня осмысления и применение ***принципа системности***.

- **Принцип системности** требует, чтобы обеспечение безопасности данных представляло собой **регулярный процесс**, осуществляемый **на всех этапах жизненного цикла АИС** при **комплексном использовании** всех средств и механизмов защиты.

При этом все средства и механизмы, используемые для защиты данных, объединяются в ***систему обеспечения безопасности данных***, которая должна обеспечивать **многоуровневую защиту данных**

- **от злоумышленников,**
- **от обслуживающего персонала АИС,**
- **от случайных ошибок пользователей.**

1.1. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных. Стр. 4

Основные документы, разработанные на третьем этапе:

Министерством обороны США в 1983 г. опубликован документ под названием «Критерии оценки надежных компьютерных систем», впоследствии по цвету обложки получившего название «Оранжевая книга».

В 1991 г. NCSC (National Computer Security Center) опубликован документ — Интерпретация «Критериев оценки надежных компьютерных систем» в применении к понятию надежной системы управления базой данных. Он конкретизирует и развивает положения «Оранжевой книги» для решения задачи создания и оценки защищенных СУБД; известен также как «Розовая книга».

В России Государственной технической комиссией при Президенте Российской Федерации (Гостехкомиссией) были разработаны и в 1992 г. опубликованы «Руководящие документы по защите от несанкционированного доступа к информации», определяющие требования, методику и стандарты построения защищенных средств вычислительной техники и автоматизированных систем.

1.1. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных. Стр. 5

Терминология, используемая в основных документах

Уровень безопасности

- **Уровень безопасности** средств вычислительной техники или программного обеспечения **характеризуется принадлежностью к одному из иерархически упорядоченных классов**.

Суть требований к оцениваемой системе может только усиливаться при переходе к более высоким классам защищенности. **Самый низкий класс — седьмой, самый высокий — первый**.

Показатель защищенности

- **Наличие или отсутствие конкретного средства защиты** от несанкционированного доступа к данным **является показателем защищенности** средства вычислительной техники.

Всего в руководящих документах **сформулирован 21 показатель**.

1.1. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных. Стр. 6

По защищенности процессов обработки информации все автоматизированные **системы делятся на три группы**.

- **Третья группа** включает в себя автоматизированные системы, в которых *работает один пользователь*. Предполагается, что он допущен до всей информации, и информация размещена на носителях одного уровня конфиденциальности.
- **Вторая и первая группы** включают *многопользовательские системы*, в которых информация обрабатывается и хранится на носителях *различного уровня конфиденциальности*.
  - Если **пользователь имеет одинаковые права доступа ко всей обрабатываемой и хранимой информации,** то автоматизированная система относится ко **второй группе**.
  - В тех же случаях, когда **не все пользователи имеют права доступа ко всей информации**, система относится к **первой группе**.

1.1. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных. Стр. 7

- **По степени защищенности** от несанкционированного доступа все автоматизированные системы подразделяются на **девять классов**.

  Внутри каждой группы соблюдается иерархия классов по требованиям к защите, с усилением требований в порядке перечисления классов.

- **Система защиты информации** реализуется как комплекс **программно-технических средств** и **организационных мер** по защите информации от несанкционированного доступа.

Система защиты информации должна быть рассмотрена как состоящая из **четырех подсистем**:

- подсистемы **управления доступом**;
- подсистемы **регистрации и учета**;
- **криптографической подсистемы**;
- подсистемы **обеспечения целостности**.

1.1. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных. Стр. 8

Четвертый этап

- Характеризуется **разработкой и внедрением стандартов** в области информационной безопасности.

Ставится и решается задача управления обеспечением информационной безопасности конкретного объекта, в частности, баз данных.

Цель управления — обеспечение **требуемого уровня защищенности информационных активов от объективно существующих угроз**.

Требуемый уровень защищенности определяется как **разумный баланс** между

- потенциальным **ущербом**, связанным с реализациями существующих угроз,
- и **затратами** на обеспечение процесса управления.

1.1. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных. Стр. 9

Основные документы, разработанные на четвертом этапе

1 декабря 1999 г. издан официальный текст международного стандарта ISO/IEC 15408, известного также как «Общие критерии».

Международная Организация по Стандартизации (ISO), Evaluation (оценка) criteria for IT security (IEC)

Принятие этого стандарта отразило изменения, происходящие в идеологии подхода к построению безопасных информационных технологий, в частности, защищенных информационных систем и их программного ядра — СУБД.

Основная идея «Общих критериев» состоит в **разделении всех требований безопасности на две категории**:

- **функциональные**, обеспечивающие безопасность информационных технологий,
- и **требования гарантии оценки**, оценивающие правильность и эффективность реализации функциональных требований.

1.1. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных. Стр. 10

В 2002 г. на основе аутентичного текста ISO/IEC 15408 был принят российский стандарт ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

Базис стандарта включает

- определение и оценку **уязвимых мест** в анализируемой информационной системе,
- оценку уровня существующих **угроз**
- и определение **комплекса мер**, позволяющего снизить **риски** до приемлемого для организации уровня.

1.1. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных. Стр. 11

- **Выбор комплекса мер по снижению рисков осуществляется на основе стоимостного анализа потенциальных потерь, связанных с реализацией конкретных угроз.**

Стандарт содержит практические правила обеспечения безопасности ИС для всех этапов жизненного цикла системы.

Правила интегрированы в комплексный метод и основаны на проверенных практикой приемах и технологиях.

Например, стандарт предписывает *использовать*

- определенные *средства идентификации и аутентификации* пользователей (или процессов),
- средства *резервного копирования*,
- *антивирусный контроль* и т. д.

1.2. Критерии качества баз данных. Стр. 1

При выполнении анализа безопасности систем баз данных рассматривают **два компонента**:

- **систему программ управления данными**
- и **совокупность данных**, упорядоченных по некоторым правилам.

Поэтому и **при анализе качества** системы баз данных выделяют **два основных компонента**:

- **программные средства системы управления базой данных** (СУБД), независимые от сферы их применения, структуры и смыслового содержания накапливаемых и обрабатываемых данных;
- **информацию базы данных**, доступную для накопления, упорядочивания, обработки и использования в конкретной проблемно-ориентированной сфере применения.

1.2. Критерии качества баз данных. Стр. 2

Первый компонент для системного анализа и требований к качеству — комплекс программ СУБД.

Важнейшие характеристики качества СУБД — требования к функциональной пригодности для процессов **формирования** и **изменения** информационного наполнения БД администраторами, а также **доступа к данным** и **представления результатов** пользователям БД.

В зависимости от конкретной проблемно-ориентированной области применения СУБД, **приоритет** при системном анализе требований к качеству может отдаваться различным конструктивным характеристикам:

- либо **надежности и защищенности** применения (финансовая сфера),
- либо **удобству использования** малоквалифицированными пользователями (социальная сфера),
- либо **эффективности использования ресурсов** (сфера материально-технического снабжения).

1.2. Критерии качества баз данных. Стр. 3

Второй компонент БД — собственно накапливаемая и обрабатываемая информация. В системах баз данных доминирующее значение приобретают сами данные, их хранение и технология обработки.

Характеристики качества систем баз данных можно разделить на

- **функциональные** и
- **конструктивные**.

- **Функциональная пригодность** баз данных при проектировании определяется на основании требований к реальным значениям необходимых показателей и критериев качества.
- **Мерой качества функциональной пригодности** может быть *степень соответствия* доступной пользователям *информации* целям создания, назначения и функциям системы баз данных.

1.2. Критерии качества баз данных. Стр. 4

Функциональная пригодность систем баз данных также отражается следующими характеристиками:

- **полнотой накопленных описаний объектов** — относительным числом объектов или документов, имеющихся в БД, к общему числу объектов по данной тематике или по отношению к числу объектов в аналогичных БД того же назначения;
- **идентичностью данных** — относительным числом описаний объектов, не содержащих дефекты и ошибки, к общему числу документов об объектах в систем баз данных;
- **актуальностью данных** — относительным числом устаревших данных об объектах в ИБД к общему числу накопленных и обрабатываемых данных.

1.2. Критерии качества баз данных. Стр. 5

Требования к информации баз данных должны содержать особенности обеспечения ее

- надежности,
- актуальности (достоверности),
- эффективности использования вычислительных ресурсов и
- приемлемого уровня сопровождения.

Особенно выделяются характеристики

- **актуальности (достоверности) данных** и
- **защищенности информации**.

- **Актуальность (достоверность) данных** — это степень соответствия информации об объектах в системе баз данных моделируемым реальным объектам в данный момент времени.

Причинами нарушения актуальности данных являются изменения самих объектов, которые могут несвоевременно или некорректно отображаться в их образах в базах данных.

1.2. Критерии качества баз данных. Стр. 6

Важными показателями качества баз данных являются **объемно-временные характеристики обрабатываемых данных**:

- **объем базы данных** — относительное число записей описаний объектов или документов в базе данных, доступных для хранения и обработки, по сравнению с полным числом реальных объектов во внешней среде;
- **оперативность** — степень соответствия динамики изменения описаний данных в процессе сбора и обработки состояниям реальных объектов или величина допустимого запаздывания между появлением или изменением характеристик реального объекта относительно его отражения в базе данных;
- **глубина ретроспективы** — максимальный интервал времени от даты выпуска и/или записи в базу данных самого раннего документа до настоящего времени;
- **динамичность** — относительное число изменяемых описаний объектов к общему числу записей в БД за некоторый интервал времени, определяемый периодичностью издания версий БД.

1.2. Критерии качества баз данных. Стр. 7

Защищенность информации БД реализуется, в основном, программными средствами СУБД.

Цели, назначение и функции защиты данных тесно связаны с особенностями функциональной пригодности ИБД.

Основное внимание сосредотачивается на **защите от**

- **злоумышленных разрушений,**
- **искажений и**
- **хищений информации баз данных**.

Основой такой защиты является

- **аудит доступа**, а также
- **контроль организации** и **эффективности ограничений доступа**.

1.2. Критерии качества баз данных. Стр. 8

В реальных системах баз данных должны *учитываться последствия реализации угроз*, **источниками** которых являются

- случайные,
- непредсказуемые,
- дестабилизирующие факторы или дефекты

и отсутствуют непосредственно заинтересованные лица в подобных нарушениях.

- **Качество защиты систем баз данных можно характеризовать величиной потенциального ущерба**, риск возникновения которого при проявлении дестабилизирующих факторов и реализации конкретных угроз безопасности **удается предотвратить или понизить**.
- **Характеристикой качества защиты** может выступать **среднее время** между возможными угрозами, преодолевающими защиту данных.

1.3. Сущность понятия безопасности баз данных. Стр. 1

В государственных документах сформулирована и законодательно оформлена **концепция национальной безопасности и концепция экономической безопасности России.**

Понятие безопасности связывается с защитой некоторых активов от угроз.

Угрозы классифицируются в зависимости от возможности нанесения ущерба защищаемым активам.

Основные угрозы связываются

- с **умышленными действиями людей,**
- **с непреднамеренными действиями людей,**
- **с объективными процессами, происходящими в природе**, такими, как стихийные бедствия, физические процессы, влияющие на распространение радиоволн, и т. п.

1.3. Сущность понятия безопасности баз данных. Стр. 2

Безопасность ИС

- **Безопасность ИС** можно определить как **состояние защищенности ИС от угроз ее нормальному функционированию**.
- Под **защищенностью** понимают *наличие средств ИС и методов* их применения, обеспечивающих *снижение или ликвидацию негативных последствий*, связанных с реализацией угроз.

Изложенный подход к определению понятия безопасность ИС предполагает, что **перечень и содержание угроз достаточно хорошо определены и достаточно стабильны во времени**.

1.3. Сущность понятия безопасности баз данных. Стр. 3

Некоторые сферы экономической деятельности, например электронный бизнес, характеризуются *высокой динамикой*. В этом случае возможен иной подход к определению безопасности.

- **Безопасность ИС** для сфер деятельности с высокой динамикой можно определить как **свойство системы адаптироваться к агрессивным проявлениям среды, в которой функционирует система**, **обеспечивающее поддержку на экономически оправданном уровне характеристики качества системы**.

Здесь основной акцент делается не на перечне и содержании угроз, нейтрализация которых обеспечивается, а на характеристике качества системы.

- При этом основной **критерий качества** ИС является *экономическим*, т. е. оценка средств и методов обеспечения безопасности осуществляется на основе **учета затрат** на реализацию механизмов безопасности **и потенциальных выгод** от недопущения ущерба, связанного с целенаправленным или случайным агрессивным проявлением среды.

1.4. Основные подходы к методам построения защищенных информационных систем. Стр. 1

Разработка теории построения защищенных систем обработки информации предполагает разработку **моделей строгого обоснования *надежности* систем обеспечения безопасности информации.**

В настоящее время наиболее широко реализуются **два подхода** построения оценки эффективности защиты любой автоматизированной системы:

- разработка и применение строгих **математических моделей**, позволяющих аналитически или на компьютере получить надлежащие оценки;
- **критериальный подход** к оценке надежности автоматизированных систем на всех этапах жизненного цикла.

1.4. Основные подходы к методам построения защищенных информационных систем. Стр. 2

Одна из самых насущных и сложных проблем информационной безопасности — проблема разработки и реализации **моделей разграничения доступа,** адекватных потребностям современных **распределенных автоматизированных систем**.

Управление доступом считается одним из основных **сервисов** программно-технического уровня систем обработки информации.

Он **осуществляется** соответствующими средствами **на трех основных уровнях**:

- ядро операционной системы;
- сервер баз данных;
- сервер приложений или прикладная система.

1.4. Основные подходы к методам построения защищенных информационных систем. Стр. 3

Ключевую роль в системе аппаратно-программных сервисов защиты автоматизированных систем играет **монитор безопасности**.

Основная функция монитора — реализация разграничения доступа различных **субъектов системы (пользователи, процессы и т. п.)** к **объектам системы (файлы, устройства, процессы, сегменты разделяемой памяти** и т. д.) в соответствии с принятой **политикой безопасности**.

Основные механизмы разграничения доступа реализуются в ядре защищенной операционной системы или сервера баз данных.

Модели математически строгого описания правил разграничения доступа реализуются, как правило, **на основе подхода «Субъект-объект»**. К таким наиболее часто употребляемым и реализуемым в операционных и автоматизированных информационных системах относятся **дискреционная** и **мандатная модели**.

1.4. Основные подходы к методам построения защищенных информационных систем. Стр. 4

Для построения защищенной автоматизированной системы используются **два принципиально отличных подхода.**

Первый основан на пересмотре традиционных механизмов автоматизированной системы и **создании системы с новой архитектурой**, предусматривающей использование более тонких схем разграничения доступа в таких ключевых подсистемах, как ядро операционной системы, способов работы с памятью, контроля атомарности вычисления файловых операций и более корректной работы с временными файлами.

Второй основан на подходах, направленных на устранение тех же проблем в системе, однако путем анализа и выявления уязвимых мест, исправления недостатков **модернизации уже существующих традиционных систем**. Второе направление лучше реализуется для систем с открытыми кодами. К таким системам относятся в первую очередь операционные системы Linux и Free BSD.

1.4. Основные подходы к методам построения защищенных информационных систем. Стр. 5

Тестирование

Получение уверенности в правильности проектных решений по построению системы защиты невозможно без применения методов **тестирования**.

Традиционно используются **два основных метода тестирования:**

- тестирование по методу «**черного ящика**»;
- тестирование по методу «**белого ящика**».

Тестирование по методу «черного ящика» предполагает отсутствие у тестирующей стороны каких-либо специальных знаний о конфигурации и внутренней структуре объекта испытаний.

1.4. Основные подходы к методам построения защищенных информационных систем. Стр. 6

При тестировании методом **«черного ящика»** против объекта испытаний реализуются все известные типы атак и проверяется устойчивость системы защиты в отношении этих атак.

Используемые методы тестирования эмулируют действия потенциальных злоумышленников, пытающихся взломать систему защиты.

Основным средством тестирования в данном случае **являются сетевые сканеры, располагающие базами данных известных уязвимостей.**

Метод «белого ящика» предполагает составление программы тестирования на основе знаний о структуре и конфигурации объекта испытаний. В ходе тестирования проверяются

- наличие и работоспособность механизмов безопасности,
- соответствие состава и конфигурации системы защиты требованиям безопасности и существующим рискам.

1.6. Структура свойства информационной безопасности баз данных. Стр. 7

Распределенная обработка данных характеризуется

- размещением логически единой информационной базы в распределенной сетевой среде,
- асинхронной многопользовательской обработкой данных
- и развитыми средствами разграничения доступа.

Реальная сложность организации управления доступом должна быть скрыта от пользователя. Логическое пространство баз данных должно выглядеть для пользователя единым, то есть как если бы вся база располагалась на его локальном компьютере.

Высокая степень безопасности данных должна быть обеспечена без снижения функциональности автоматизированных систем и практически без усложнения работы пользователя в системе. Механизм обеспечения безопасности данных должен обладать гибкостью и удобством администрирования системы.

1.6. Структура свойства информационной безопасности баз данных. Стр. 8

Сущность проблемы обеспечения информационной безопасности систем баз данных состоит в разработке методов и средств, обеспечивающих выполнение трех взаимосвязанных свойств системы:

- ***конфиденциальность**:* обеспечение пользователям доступа только к тем данным, для которых пользователь имеет явное или неявное разрешение на доступ;
- ***целостность**:* обеспечение защиты от преднамеренного или непреднамеренного изменения информации или процессов ее обработки;
- ***доступность**:* обеспечение возможности авторизованным в системе пользователям доступа к информации в соответствии с принятой технологией.

1.6. Структура свойства информационной безопасности баз данных. Стр. 9

Конфиденциальность

Задача обеспечения секретности предусматривает комплекс мер по предотвращению несанкционированного доступа к конфиденциальной информации каким-либо пользователям.

- **Разрешение на доступ к информации определяется внешними по отношению к системе факторами.**
- Система должна обладать **языковыми средствами**, достаточными для описания правил, определяющих возможность доступа к данным.
- Обычно предполагается, что используемые **правила обеспечивают однозначное решение о разрешении или запрещении доступа** к данным.

1.6. Структура свойства информационной безопасности баз данных. Стр. 10

Целостность

Задача обеспечения целостности предусматривает комплекс мер по **предотвращению непреднамеренного изменения или уничтожения информации**, используемой информационной системой управления или системой поддержки принятия решений.

Изменение или уничтожение данных может быть следствием

- неблагоприятного стечения обстоятельств и состояния внешней среды (стихийные бедствия, пожары и т. п.),
- неадекватных действий пользователей (ошибки при вводе данных, ошибки операторов и т. п.)
- и проблем, возникающих при многопользовательской обработке данных.

1.6. Структура свойства информационной безопасности баз данных. Стр. 11

При изучении данной дисциплины методы обеспечения информационной безопасности баз данных будут рассматриваться как совокупность методов и средств обеспечения **конфиденциальности, целостности и доступности**.

Рис. Структура свойства информационной безопасности